DOC 55 **2572/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

17 mars 2022

PROJET DE LOI

relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités

SOMMAIRE Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

17 maart 2022

WETSONTWERP

betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten

INHOUD Blz.

Le gouvernement a déposé ce projet de loi le 17 mars 2022.	*De regering heeft dit wetsontwerp op 17 maart 2022 ingediend.*
Le "bon à tirer" a été reçu à la Chambre le 24 mars 2022.	*De "goedkeuring tot drukken" werd op 24 maart 2022 door de Kamer ontvangen.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

RÉSUMÉ

La loi vise essentiellement à rétablir un cadre juridique conforme à la jurisprudence en matière de conservation des "métadonnées" ou "données de trafic et de localisation" par les opérateurs.

En effet, à la suite de l'arrêt "La Quadrature du Net" rendu par la Cour de justice de l'Union européenne le 6 octobre 2021, la Cour constitutionnelle belge a annulé les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (arrêt n° 57/2021 du 22 avril 2021), ce qui implique qu'une conservation généralisée et indifférenciée de ces métadonnées en tout temps n'est plus permise pour les opérateurs à des fins répressives.

Cependant, l'arrêt suggère certaines pistes alternatives à la conservation généralisée et indifférenciée en tout temps , telles que la conservation ciblée sur base géographique.

Ces pistes ont été suivies et développées par la présente loi.

Enfin, ce projet de loi vise également à répondre aux attentes sociétales légitimes d'un monde de plus en plus digitalisé. Force est de constater que les transactions électroniques (e-commerce) deviennent dans beaucoup de secteurs la norme. De la sorte, afin de lutter contre certaines formes d'infractions se commettant exclusivement en ligne, il est nécessaire que les autorités chargées de la prévention, de la détection et de la poursuite de ces infractions puissent obtenir des opérateurs les données dont ils disposent, dans la mesure nécessaire à l'accomplissement de leurs missions respectives.

SAMENVATTING

De wet is er voornamelijk op gericht weer een juridisch kader in te stellen dat voldoet aan de rechtspraak inzake bewaring van de "metagegevens" of "verkeers- en locatiegegevens door operatoren.

Naar aanleiding van het arrest"La Quadrature du Net", gewezen door het Hof van Justitie van de Europese Unie op 6 oktober 2021 heeft het Belgische Grondwettelijk Hof immers de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie nietig verklaard (arrest nr. 57/2021 van 22 april 2021), wat impliceert dat een veralgemeende en ongedifferentieerde bewaring van deze matadata te allen tijde niet meer is toegestaan voor operatoren voor rechtshandhavingsdoeleinden.

In het arrest worden echter enkele alternatieven voorgesteld voor een algemene en ongedifferentieerde databewaring te allen tijde, zoals een gerichte dataretentie op geografische basis.

Deze pistes zijn gevolgd en ontwikkeld door de onderhavige wet.

Ten slotte beoogt dit wetsontwerp inderdaad ook te beantwoorden aan de legitieme maatschappelijke verwachtingen van een wereld die steeds digitaler wordt. Het is duidelijk dat in vele sectoren de elektronische transacties (e-commerce) de norm worden. Om bepaalde vormen van overtredingen die uitsluitend online worden gepleegd, te bestrijden, is het derhalve noodzakelijk dat de autoriteiten die zijn belast met de preventie, opsporing en vervolging van deze overtredingen, van de operatoren de gegevens kunnen verkrijgen die ze in hun bezit hebben, in de mate die nodig is om hun respectieve opdrachten te vervullen.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

1. Arrêt de la Cour constitutionnelle du 22 avril 2021

Cet avant-projet de loi vise essentiellement à répondre à l'annulation par la Cour constitutionnelle dans son arrêt n° 57/2021 du 22 avril 2021 des articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.

Cette loi prévoyait l'obligation pour les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet et de courrier électronique par Internet (qu'ils soient opérateurs notifiés à l'IBPT ou non) de conserver certaines catégories de données de localisation et de trafic pendant une durée de 12 mois essentiellement afin que ces données soient disponibles pour des finalités répressives et en particulier pour les enquêtes pénales. Ces données ne concernent pas le contenu des communications.

L'argumentaire de la Cour constitutionnelle renvoie à l'arrêt "Quadrature du Net" de la Cour de Justice de l'Union européenne rendu le 6 octobre 2020 (affaires C-511/18, C-512/18 et C-520/18: La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone), lequel détaille les limites à la conservation des données et suggère certaines pistes, à savoir:

1) La conservation généralisée et indifférenciée des données de trafic et de localisation (autres que les données d'identité civile et les adresses IP à la source de la connexion) peut uniquement être imposée aux opérateurs en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale;

2) Pour la lutte contre la criminalité grave ou la prévention de menaces graves contre la sécurité publique, seules sont permises la conservation ciblée de données, dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers, et la conservation rapide des données ("quick-freeze"), à savoir une demande de gel

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

1. Arrest van het Grondwettelijk Hof van 22 april 2021

Dit voorontwerp van wet beoogt in wezen tegemoet te komen aan arrest nr. 57/2021 van 22 april 2021 waarin het Grondwettelijk Hof heeft beslist om de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie te vernietigen.

Deze wet voorzag in de verplichting voor aanbieders van openbare telefoniediensten, waaronder ook via het internet, van internettoegang, van e-mail via het internet (ongeacht of ze bij het BIPT een kennisgeving hadden gedaan of niet) om bepaalde categorieën locatie- en verkeersgegevens gedurende een periode van 12 maanden te bewaren, in hoofdzaak zodat deze gegevens beschikbaar zijn voor rechtshandhavingsdoeleinden en met name voor strafrechtelijk onderzoek. Deze gegevens hebben geen betrekking op de inhoud van de communicatie.

Het betoog van het Grondwettelijk Hof verwijst naar het arrest "Quadrature du Net" van het Hof van Justitie van de Europese Unie van 6 oktober 2020 (zaken C-511/18, C-512/18 en C-520/18: *La Quadrature du Net*, French Data Network et Ordre des barreaux francophones et germanophone), waarin de grenzen van de bewaring van gegevens nader worden toegelicht en bepaalde pistes worden voorgesteld, namelijk:

1) Het algemeen en ongedifferentieerd bewaren van verkeers- en locatiegegevens (met uitzondering van gegevens met betrekking tot de burgerlijke identiteit en de IP-adressen aan de bron van de verbinding) kan alleen aan operatoren worden opgelegd in geval van een werkelijke en actuele of voorzienbare ernstige bedreiging van de nationale veiligheid;

2) Met het oog op het bestrijden van zware criminaliteit of de voorkoming van ernstige bedreigingen voor de openbare veiligheid zijn alleen gerichte gegevensbewaring, in bepaalde zones of voor bepaalde categorieën personen waarvan vooraf is vastgesteld dat zij een bijzonder risico vormen, en snelle gegevensbewaring ("*quick freeze*"), d.w.z. een verzoek om verkeers- en

des données de trafic et de localisation relatives à une personne sur une courte période;

3) La conservation des données d'identité civile est permise pour d'autres motifs que ceux visés aux points 1) et 2), et donc notamment pour la recherche des infractions ne relevant pas de la criminalité grave;

4) Seule la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale sont de nature à justifier la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion.

Dans son arrêt du 22 avril 2021, la Cour constitutionnelle indique ce qui suit: "B.18. L'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué: l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours "répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi" (points 132 et 133).".

Il y a aussi lieu de rappeler que les métadonnées ne sont pas confidentielles par rapport aux opérateurs, dès lors que ces derniers ne doivent les conserver que pour autant qu'ils les traitent ou les génèrent. Cependant, la législation limite les traitements que font les opérateurs de ces données, vu qu'il peut s'agir de données à caractère personnel. Par contre, les métadonnées traitées ou générées par les opérateurs sont confidentielles par rapport aux autorités. Il est donc essentiel que la fourniture aux autorités de ces données, qui constitue une exception au principe de confidentialité des données de communications, reste l'exception, ce qui correspond au système mis en place en Belgique.

locatiegegevens van een persoon gedurende een korte periode te bevriezen, toegestaan;

3) Het bewaren van burgerlijke-identiteitsgegevens is toegestaan om andere dan de in de punten 1) en 2) genoemde redenen, en dus met name voor het onderzoek naar strafbare feiten die niet onder de noemer ernstige criminaliteit vallen;

4) Enkel de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid kunnen een algemene en ongedifferentieerde bewaring rechtvaardigen van enkel de IP-adressen die zijn toegewezen aan de bron van een verbinding.

In zijn arrest van 22 april 2021 zegt het Grondwettelijk Hof het volgende: "B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt: de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds "beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel" (punten 132 en 133).".

Er dient ook te worden herinnerd aan het feit dat de metagegevens niet vertrouwelijk zijn ten opzichte van de operatoren, aangezien deze laatste ze slechts moeten bewaren voor zover zij die verwerken of genereren. De wetgeving beperkt evenwel de verwerkingen die de operatoren van deze gegevens doen, aangezien het om persoonsgebonden gegevens kan gaan. Metagegevens die verwerkt of gegenereerd worden door de operatoren zijn daarentegen wel vertrouwelijk ten opzichte van de autoriteiten. Het is dus van fundamenteel belang dat het verstrekken van die gegevens aan de autoriteiten, wat een uitzondering vormt op het principe van de vertrouwelijkheid van de communicatiegegevens, de uitzondering blijft, hetgeen overeenstemt met het stelsel dat in België is ingesteld.

2. Solutions mises en place dans la loi programme dans le cadre des possibilités laissées par la jurisprudence

2.1. Conservation généralisée et indifférenciée des métadonnées en cas de menace grave pour la sécurité nationale et des données d'identification

Même si la Cour de Justice de l'Union européenne limite les possibilités de conservation généralisée et indifférenciée de données d'identification et des métadonnées, cette dernière demeure possible dans certains cas de figure.

Ainsi, les articles 126 et 127 de la loi relative aux communications électroniques, tels que modifiés par le présent projet de loi, reprennent des données d'identification des utilisateurs finaux, des équipements terminaux et des services de communications électroniques (en ce compris l'adresse IP) sans viser les données de communication.

Il convient de souligner, à cet égard, que pour se conformer à la jurisprudence précitée, les données qui doivent être conservées par les opérateurs sur la base de la nouvelle version de l'article 126 sont désormais limitées aux données d'identification. Les autres métadonnées ne doivent donc plus être conservées sur cette base.

Une conservation généralisée et indifférenciée des données est également prévue en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, conformément à ce que la Cour de Justice de l'Union européenne permet. Cette menace est établie par les services de renseignement ou après l'évaluation de la menace par l'OCAM, en cas de menace de niveau 3 ou 4 sur l'ensemble du territoire. De même, si l'OCAM, à la suite de l'évaluation de la menace, détermine que le niveau de menace est de 3 ou 4 pour l'ensemble du territoire, cela peut entraîner une conservation généralisée et indifférenciée des données tant que la menace reste au même niveau.

2.2. Quick et future freeze (gel des données)

Une mesure de conservation rapide ("*quick freeze*") constitue une mesure utile, dès lors qu'elle permet de prolonger la durée de conservation de certaines données.

Cependant, une telle mesure, à elle seule, ne permet pas de lutter contre la criminalité grave et les menaces réelles et actuelles en matière de sécurité. Très concrètement, ordonner une mesure de *quick freeze* au moment

2. Oplossingen ingesteld in de programmawet in het kader van de mogelijkheden die door de rechtspraak worden gelaten

2.1. Algemene en ongedifferentieerde bewaring van de verkeersgegevens in geval van ernstige bedreiging voor de nationale veiligheid en van de identificatiegegevens

Hoewel het Hof van Justitie van de Europese Unie de mogelijkheden inzake algemene en ongedifferentieerde bewaring van identificatie gegevens en van metagegevens beperkt, blijft zo'n bewaring mogelijk in een aantal specifieke gevallen.

Zo nemen de artikelen 126 en 127 van de wet betreffende de elektronische communicatie, zoals gewijzigd door het voorliggende wetsontwerp, identificatiegegevens van de eindgebruikers, van de eindapparatuur en van de elektronische-communicatiediensten (waaronder ook het IP-adres) op, zonder de communicatiegegevens te beogen.

Daarbij dient te worden onderstreept dat om zich naar de voormelde rechtspraak te schikken, de gegevens die de operatoren moeten bewaren op basis van de nieuwe versie van artikel 126 voortaan beperkt zijn tot de identificatiegegevens. De overige metagegevens moeten dus niet meer op die basis worden bewaard.

Er wordt eveneens voorzien in de algemene en ongedifferentieerde bewaring van gegevens in geval van een ernstige, werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid overeenkomstig hetgeen het Hof van Justitie van de Europese Unie toestaat. Deze dreiging wordt vastgesteld door de inlichtingendiensten of na de evaluatie van de dreiging door het OCAD, in geval van dreigingsniveau 3 of 4 op het gehele grondgebied. Ook wanneer OCAD, na de evaluatie van de dreiging, vaststelt dat het dreigingsniveau 3 of 4 is voor het gehele grondgebied, kan dit als gevolg hebben dat een algemene en ongedifferentieerde gegevensbewaring wordt ingevoerd zolang de dreiging op hetzelfde niveau blijft.

2.2. Quick en future freeze (bevriezing van de gegevens)

Een maatregel van snelle bewaring ("*quick freeze*") is een nuttige maatregel, aangezien aan de hand daarvan de duur van bewaring van bepaalde gegevens verlengd kan worden.

Zo'n maatregel kan evenwel op zichzelf geen antwoord bieden in de strijd tegen de zware criminaliteit en de reële en actuele dreigingen op vlak van veiligheid. In wezen is het meestal al te laat als men, op het moment dat de

de la détection des faits, par exemple en cas de plainte pour enlèvement ou de découverte d'un cadavre ou d'une explosion à la suite d'un attentat est dans l'immense majorité des cas trop tard. Ce sont notamment par excellence les contacts antérieurs d'une personne qui permettent de démarrer une enquête ou plus encore l'interrogation des appareillages présents dans cette zone au moment des faits. Cette mesure seule ne respecterait aucunement les droits des victimes dans la recherche de la vérité.

Le Conseil d'État français, qui a été amené à examiner la législation française en matière de conservation de données de trafic pour les autorités (arrêt du 21/04/2021 n^{os} 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), l'explique dans les termes suivants: "56. La conservation rapide des données de connexion est ainsi de nature à faire obstacle à la disparition des informations nécessaires à la recherche, à la constatation et à la poursuite des auteurs d'infractions pénales à compter de la date et de l'heure à laquelle il est enjoint à un opérateur d'y procéder, à la suite de la commission d'une infraction ou du recueil d'éléments donnant à penser qu'une telle infraction est projetée, ainsi qu'à l'effacement ou à l'anonymisation des données relatives à des communications antérieures lorsqu'elles ont été conservées par les opérateurs. Cependant, sur ce dernier point, l'efficacité du dispositif est subordonnée à la condition que les données aient été effectivement conservées. À défaut, la conservation rapide ne permet pas aux services d'enquête et à l'autorité judiciaire d'exploiter des données relatives aux communications effectuées avant qu'elle soit ordonnée.".

Le législateur a opté pour créer un gel des données en temps réel ("*future freeze*") dans le cadre d'une enquête, que ce soit au niveau judiciaire (nouvel article 39*quinquies* du Code d'instruction criminelle) ou au niveau des services de renseignement et de sécurité (nouvel article 13/6 de la loi organique des services de renseignement et de sécurité). La mesure peut être ordonnée à l'égard d'une personne ou d'un groupe de personnes, d'un lieu ou d'un moyen de communication, et concerne les données de trafic et de localisation générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés. Il pourrait également s'agir de données que les opérateurs conserveraient pour leurs propres besoins. Ces mesures de conservation rapide de données sont accompagnées de garanties procédurales importantes. Elles ne peuvent s'opérer que sur demande du procureur du Roi ou du juge d'instruction ou, pour les services de renseignement et de sécurité, d'un chef de service. De plus, les principes essentiels en matière d'information et d'instruction sont d'office d'application (e.a. droit de

feiten vastgesteld worden, bijvoorbeeld een ontvoering of de ontdekking van een lijk of bomexplosie bij een aanslag, een *quick freeze* beveelt. Het zijn namelijk bij uitstek de eerdere contacten van een persoon die toelaten om een onderzoek uit te diepen of nog om een bevraging te doen van de toestellen die op het moment van de feiten in deze zone aanwezig waren. De maatregel alleen is onvoldoende om de rechten van het slachtoffer te eerbiedigen in de zoektocht naar de waarheid.

De Franse Conseil d'État, die de Franse wetgeving betreffende bewaring van verkeersgegevens voor de autoriteiten moest onderzoeken (arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), legt dit uit in de volgende bewoording: "56. De snelle bewaring van de connectiegegevens is aldus van die aard dat die in de weg staat van de verdwijning van de informatie die nodig is voor de opsporing, de vaststelling en de vervolging van de plegers van strafbare feiten te rekenen vanaf de datum en vanaf het tijdstip waarop een operator gelast wordt om daartoe over te gaan, na het plegen van een inbreuk of na het bundelen van elementen die doen vermoeden dat een dergelijke inbreuk gepland is, alsook van het wissen of de anonimisering van de gegevens met betrekking tot vroegere communicatie wanneer die door de operatoren zijn bewaard. Wat dat laatste punt betreft is de efficiëntie van de beschikking evenwel afhankelijk van de voorwaarde dat de gegevens daadwerkelijk zijn bewaard. Als dat niet zo is, biedt de snelle bewaring de onderzoeksdiensten en de gerechtelijke autoriteit niet de mogelijkheid om gebruik te maken van gegevens in verband met communicatie die plaatsgevonden heeft voordat die snelle bewaring bevolen is.". (vrij vertaald).

De wetgever heeft gekozen voor het bevriezen van gegevens in real time ("*future freeze*") in het kader van een onderzoek, hetzij op het niveau van justitie (nieuwe artikel 39*quinquies* van het Wetboek van Strafvordering), hetzij op het niveau van de inlichtingen- en veiligheidsdiensten (nieuwe artikel 13/6 van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten). De maatregel kan bevolen worden ten opzichte van een persoon of groep van personen, een plaats of een communicatiemiddel en betreft verkeers- en locatiegegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten. Het zou daarbij ook kunnen gaan om gegevens die de operatoren zouden bijhouden voor hun eigen behoeften. Deze maatregelen van snelle bewaring worden vergezeld van belangrijke procedurele garanties. Ze kunnen alleen worden uitgevoerd op verzoek van de procureur des Konings of de onderzoeksrechter of, in het geval van de inlichtingen- en veiligheidsdiensten, een dienshoofd. Bovendien worden de essentiële beginselen van

consultation du dossier, d'en prendre copie, possibilité de contester la régularité de la procédure, degré d'appel). Quant aux services de renseignement, un contrôle par le Comité R est prévu.

Dans un souci d'exhaustivité, on peut ajouter que le "*quick freeze*", qui consiste à demander une conservation rapide de données déjà existantes, existe déjà dans la procédure pénale belge. C'est ce que prévoit l'article 39*ter* du Code d'instruction criminelle, introduit par la loi du 25 décembre 2016 portant diverses modifications du code d'instruction criminelle et du code pénal, en vue d'améliorer les méthodes d'enquête spéciales et certaines méthodes d'enquête relatives à Internet et aux médias électroniques et de télécommunications, et de créer une base de données d'empreintes vocales. Le présent projet de loi ne fait donc qu'introduire le "future freeze" comme une nouvelle mesure dans le Code d'instruction criminelle. Pour les services de renseignement, les deux formes de conservation rapide sont nouvelles: le "*quick freeze*" et le "future freeze" sont tous deux introduits par le projet de loi actuel.

En outre, un "*quick freeze*" est également lancé pour l'auditeur de la FSMA. À cette fin, l'auditeur de la FSMA reçoit la possibilité, pour permettre la détection et la poursuite d'abus de marché et les enquêtes en la matière, de "geler" temporairement les données de trafic et de localisation. Cette mesure porte uniquement sur les données existantes qui sont encore conservées mais risquent d'être supprimées ou rendues anonymes en attente de l'autorisation du juge d'instruction. Pour avoir accès à ces données, l'auditeur de la FSMA a en effet toujours besoin de l'autorisation préalable d'un juge d'instruction. Les garanties matérielles et procédurales nécessaires sont d'application à cet égard.

Ce mécanisme de "*quick*" ou de "*future freeze*" à lui seul est cependant insuffisant pour lutter contre la criminalité grave puisqu'il concerne le gel des données de personnes qui font déjà l'objet d'une enquête, par exemple, des personnes déjà identifiées comme suspects potentiels. Or, il n'est pas exceptionnel que les autorités judiciaires et policières doivent ouvrir un dossier en s'appuyant principalement sur les données de trafic. Par exemple, en cas de meurtre ou de viol, les premiers actes d'enquête visent précisément à établir dans le laps de temps de la commission probable de l'infraction, via les données de trafic, quelles personnes pouvaient être présentes sur les lieux du crime. Ces données sont donc nécessaires pour démarrer une enquête et aider, le cas échéant, à établir une liste de suspects potentiels. En matière d'enquête, la prise de mesure de conservation rapide des données en "temps réel", par exemple lors

het opsporings- en gerechtelijk onderzoek automatisch toegepast (o.a. recht op inzage van het dossier, recht om een kopie te nemen, mogelijkheid om de regelmatigheid van de procedure aan te vechten, mate van beroep). Voor wat betreft de inlichtingendiensten is de controle door het Vast Comité I voorzien.

Voor de volledigheid kan nog toegevoegd worden dat de "*quick freeze*", waarbij een snelle bewaring gevraagd wordt van reeds bestaande gegevens, al bestaat in de Belgische strafprocedure. Deze is voorzien in artikel 39*ter* van het Wetboek van strafvordering, ingevoerd door de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische media en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken. Huidig wetsontwerp voert dus enkel de "future freeze" in als nieuwe maatregel in het Wetboek van strafvordering. Voor de inlichtingendiensten zijn beide vormen van snelle bewaring nieuw: zowel de "*quick freeze*" als de "future freeze" worden ingevoerd door huidig wetsontwerp.

Daarnaast wordt ook een "*quick freeze*" ingevoerd ten behoeve van de auditeur van de FSMA. Te dien einde krijgt de auditeur van de FSMA voor doeleinden van het opsporen, onderzoeken en vervolgen van marktmisbruik de mogelijkheid om verkeers- en locatiegegevens tijdelijk te laten "bevriezen". Deze maatregel heeft enkel betrekking op bestaande gegevens, die nog bewaard worden maar riskeren te worden verwijderd of anoniem gemaakt in afwachting van de toestemming van de onderzoeksrechter. Om toegang te krijgen tot deze gegevens heeft de auditeur van de FSMA immers steeds de voorafgaande toestemming van een onderzoeksrechter nodig. Terzake gelden de nodige materiële en procedurele waarborgen.

Dit mechanisme van "*quick*" of "*future freeze*" alleen is echter onvoldoende om de ernstige criminaliteit te bestrijden, aangezien het gaat om het bevriezen van gegevens van personen tegen wie reeds een onderzoek loopt, bijvoorbeeld personen die reeds als mogelijke verdachten zijn geïdentificeerd. Het is echter niet uitzonderlijk dat gerechtelijke en politionele autoriteiten een zaak moeten openen voornamelijk op basis van verkeersgegevens. In het geval van moord of verkrachting bijvoorbeeld zijn de eerste onderzoeksdaden er juist op gericht om in het tijdsbestek waarin het misdrijf vermoedelijk is gepleegd, aan de hand van verkeersgegevens vast te stellen welke personen op de plaats van het misdrijf aanwezig kunnen zijn geweest. Deze gegevens zijn dus nodig om een onderzoek te starten en eventueel een lijst van mogelijke verdachten te helpen opstellen. In veel gevallen is het nemen van maatregelen voor de snelle bewaring van

de la découverte du cadavre ou de la plainte pour viols, s'avère, dans un nombre important de cas, inopérante car trop tardive. C'est la raison pour laquelle cette mesure, qui est utile dans le cadre d'une information ou d'une instruction en cours, doit être accompagnée par d'autres mesures de conservation de données.

2.3. Conservation ciblée sur base des personnes

Comme déjà mentionné au point 2.2., il est prévu à l'article 39*quinquies* du Code d'instruction criminelle et à l'article 13/6 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité que les autorités judiciaires et les services de renseignement et de sécurité puissent requérir des opérateurs une conservation de données de communication ciblée sur une personne ou un groupement de personnes. Cette conservation est ponctuelle, pour une durée limitée, et axée sur la cible d'une information, d'une instruction ou d'une enquête de renseignement. Il s'agit de la conservation rapide et ciblée des données de trafic et de localisation des personnes dans le cadre d'une affaire spécifique. C'est aussi actuellement la seule possibilité de conservation ciblée sur une base personnelle. La possibilité de demander un "future freeze" est expliquée dans le commentaire des deux articles.

2.4. Conservation ciblée sur base géographique

Vu l'insuffisance des données de trafic et de localisation disponibles auprès des opérateurs pour répondre aux besoins des autorités, la conservation ciblée sur base géographique est mise en œuvre, en tenant compte des éléments suivants.

Premièrement, la Cour de Justice de l'Union européenne a suggéré cette possibilité comme méthode de conservation admissible au regard du droit au respect de la vie privée, moyennant le recours à des critères objectifs et non discriminatoires (point 150 de l'arrêt "La Quadrature du Net").

Deuxièmement, il est tenu compte du fait qu'il n'est pas possible de prédire avec une certitude absolue où des faits criminels vont être commis, ni par qui.

Dans une vision purement théorique, la conciliation parfaite des principes de vie privée et de lutte contre la criminalité grave ou de prévention de menaces graves contre la sécurité publique implique que seules les données d'identification, de localisation et de trafic des personnes dont on a la certitude absolue qu'elles sont coupables ou victimes d'infraction pénale ou qu'elles ont besoin d'une aide ou d'une assistance pourraient être conservées. Il s'agirait de ne conserver que les seules données relatives aux auteurs d'infractions pénales qui

gegevens in "real time", bijvoorbeeld wanneer een lijk wordt gevonden of wanneer een klacht wordt ingediend over een verkrachting, ondoeltreffend omdat deze te laat komt. Daarom moet deze maatregel, die nuttig is in het kader van een lopend onderzoek, gepaard gaan met andere maatregelen inzake gegevensbewaring.

2.3. Gerichte bewaring op basis van de personen

Zoals al vermeld onder punt 2.2., wordt in artikel 39*quinquies* van het Wetboek van Strafvordering en in artikel 13/6 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten bepaald dat de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten de operatoren mogen opvorderen tot het bewaren van communicatiegegevens gericht op een persoon of een groep personen. Deze bewaring is specifiek, voor een beperkte duur en gericht op het doel van een opsporingsonderzoek, een gerechtelijk onderzoek of een inlichtingenonderzoek. Het gaat hier om een snelle en gerichte bewaring van verkeers- en locatiegegevens van personen in het kader van een concreet dossier. Dit is op dit moment ook de enige mogelijkheid tot gerichte bewaring op basis van personen. De mogelijkheid tot een "future freeze" wordt uitgelegd in de commentaar bij de twee artikelen.

2.4. Gerichte bewaring op geografische basis

Gelet op de ontoereikendheid van de verkeers- en locatiegegevens die beschikbaar zijn bij de operatoren om te voldoen aan de behoeften van de autoriteiten, wordt de gerichte bewaring op geografische basis toegepast, rekening houdende met de volgende elementen.

Ten eerste heeft het Hof van Justitie van de Europese Unie deze mogelijkheid gesuggereerd als bewaringsmethode die toelaatbaar is ten aanzien van het recht op eerbiediging van de privacy, mits gebruik wordt gemaakt van objectieve en niet-discriminerende criteria (punt 150 van het arrest "*La Quadrature du Net*").

Ten tweede is er rekening gehouden met het feit dat het onmogelijk is om met absolute zekerheid te voorspellen waar criminele feiten zullen plaatsvinden of door wie.

Zuiver theoretisch gezien impliceert de perfecte verzoening van de beginselen van de eerbiediging van de persoonlijke levenssfeer met de bestrijding van zware criminaliteit of de voorkoming van ernstige bedreigingen van de openbare veiligheid dat alleen de identificatie-, locatie- en verkeersgegevens van personen van wie met absolute zekerheid bekend is dat zij schuldig zijn aan of slachtoffer zijn van strafbare feiten dan wel hulp of bijstand behoeven, mogen worden bewaard. Alleen van plegers van strafbare feiten zouden die gegevens

servent à sceller la preuve de leur culpabilité et que les seules données relatives à des lieux où l'on sait avec la même assurance absolue qu'une infraction grave va être commise. Dans cette même optique purement théorique, on ne conserverait alors que les données des personnes dont on sait par avance qu'elles deviendront des victimes et ce, uniquement lors de la survenance de l'infraction. Tout un chacun sait cependant qu'il n'est bien évidemment pas possible de prédéterminer d'office les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu très précis où elle sera commise.

Le législateur est pleinement conscient que la conservation ciblée sur base géographique entraîne inévitablement une manière totalement nouvelle pour les opérateurs de concevoir et de gérer la conservation de données de localisation et de trafic et la fourniture de ces données aux autorités.

Le législateur a également pris connaissance des difficultés techniques et opérationnelles rencontrées par les opérateurs pour mettre en œuvre la conservation ciblée sur base géographique.

À cet égard, le ciblage géographique des différentes zones identifiées dans le présent projet de loi doit tenir compte du matériel déjà placé par les opérateurs d'une part et de l'obligation positive pour certains opérateurs d'offrir un réseau de communication sur la quasi-totalité du territoire. Tel que mentionné dans le RGPD, entre autres aux articles 25 et 32, l'obligation de mise en place de mesures techniques et organisationnelles afin de garantir un niveau de protection des données adéquat constitue une obligation de moyens prenant en compte tant "l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement" que "les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques".

Il convient d'appliquer en l'espèce cette balance d'intérêt "interne au RGPD" afin d'assurer une mise en balance proportionnée entre les capacités techniques des opérateurs, le respect de la vie privée et les finalités de protection de l'État et de ses citoyens. En effet, le fait d'accepter que certains opérateurs ne conservent, sur la base des obligations de conservation ciblée sur base géographique, aucune donnée de trafic et de localisation en raison de l'impossibilité technique de couvrir de manière précise et strictement limitée la zone géographie ciblée créerait un traitement inégal entre les victimes des faits graves de criminalités en fonction de la technique et des moyens disponibles par chaque opérateur. Le législateur estime qu'une telle application

mogen worden bewaard die strekken tot bewijs van hun schuld, en alleen de gegevens met betrekking tot locaties waarvan met dezelfde absolute zekerheid bekend is dat er een ernstig misdrijf zal worden gepleegd. In dezelfde zuiver theoretische zin worden alleen gegevens bewaard over personen van wie van tevoren bekend is dat zij slachtoffer zijn, en alleen wanneer het misdrijf plaatsvindt. Iedereen weet echter dat het uiteraard niet mogelijk is vooraf te bepalen wie betrokken zal zijn bij een strafbaar feit dat nog niet is gepleegd of waar het precies zal worden gepleegd.

De wetgever is er zich ten volle van bewust dat de gerichte bewaring op geografische basis onvermijdelijk leidt tot het ontwikkelen van een totaal nieuwe manier voor de operatoren om de bewaring van locatie- en verkeersgegevens op te vatten en te beheren, alsook de verstrekking van deze gegevens aan de autoriteiten.

De wetgever heeft ook kennis genomen van de technische en operationele moeilijkheden die de operatoren ondervonden om de gerichte bewaring op geografische basis te verrichten.

In dit verband moet bij de geografische afbakening van de verschillende gebieden die in dit wetsontwerp worden aangewezen, rekening worden gehouden met enerzijds de reeds door de operatoren geplaatste apparatuur en anderzijds met de positieve verplichting voor bepaalde operatoren om over bijna het hele grondgebied een communicatienetwerk aan te bieden. Zoals vermeld in de AVG, onder meer in de artikelen 25 en 32, is de verplichting om technische en organisatorische maatregelen te nemen om een passend niveau van gegevensbescherming te waarborgen, een middelenverbintenis waarbij rekening wordt gehouden met zowel "de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking" als "de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen".

Deze "interne AVG"-belangenafweging moet in casu worden toegepast om te zorgen voor een evenredig evenwicht tussen de technische capaciteiten van de operatoren, de eerbiediging van de persoonlijke levenssfeer en de doeleinden van de bescherming van de Staat en zijn burgers. Indien zou worden aanvaard dat sommige operatoren geen verkeers- en locatiegegevens bewaren op basis van de verplichtingen inzake gerichte bewaring op geografische basis, omdat het technisch onmogelijk is de beoogde geografische zone nauwkeurig en strikt begrensd af te dekken, zou dit leiden tot een ongelijke behandeling van slachtoffers van ernstige criminaliteit, afhankelijk van de techniek en de middelen waarover elke operator beschikt. De wetgever is van mening dat

stricte du principe de minimisation des données constituerait en ce sens une discrimination entre les citoyens en termes d'exercice de leurs droits et libertés et serait dès lors contraire au principe d'égalité de traitement entre les citoyens.

Par conséquent, le législateur a opté pour une obligation de moyen permettant, de manière strictement nécessaire, proportionnée et limitée, aux opérateurs de pouvoir conserver les données au-delà des zones géographiques strictement délimitées.

Il va de soi que cette obligation de moyen imposée aux opérateurs sera contrôlée par l'IBPT qui veillera à ce que les opérateurs fournissent tous les efforts requis, en fonction de l'état des techniques utilisées et des coûts y relatifs, pour cibler le plus précisément possible les zones géographiques.

Il existe également un risque que les auteurs d'infraction s'organisent pour commettre des infractions dans des zones non soumises à conservation de données.

Le législateur a en effet décidé d'opérer de la conservation de données sur des zones où il y a une menace grave pour la sécurité publique vu le taux important par 1 000 habitants d'infractions graves qui y ont été commises au cours des 3 années précédentes. Si ce taux est un marqueur indéniable d'une activité criminelle foisonnante, il serait bien entendu absurde de ne viser que les rues, coordonnées GPS où ces infractions graves se sont tenues car cela impliquerait que les schémas criminels sont parfaitement prévisibles et se déroulent forcément aux mêmes endroits. Ici aussi, il est cependant possible de ne pas d'office cibler tout le territoire mais de regarder l'importance de la menace pour la sécurité publique arrondissement judiciaire par arrondissement judiciaire ou zone de police par zone de police.

Le nombre de faits commis sur un territoire donné est un indicateur fiable de divers phénomènes. D'abord, il indique la récurrence à laquelle une zone déterminée a été soumise à un fait délictueux d'une certaine ampleur, ce qui a de manière indéniable un impact sur le sentiment d'insécurité de la population. Deuxièmement, il est également un indicateur fiable de la sensibilité de la zone à des phénomènes criminels. De fait, pour une certaine catégorie de faits, il est incontestable que des facteurs criminologiques tels que la structure sociale et économique de l'endroit, la présence d'axes routiers facilitateurs, la distance des postes de police, etc. jouent un rôle important dans certains phénomènes criminels. Ces facteurs ayant une certaine pérennité, ils influencent la répétition de faits criminels similaires.

een dergelijke strikte toepassing van het minimaliseringsbeginsel van de gegevens zou neerkomen op een discriminatie tussen de burgers wat de uitoefening van hun rechten en vrijheden betreft, en dus in strijd zou zijn met het beginsel van gelijke behandeling van burgers.

Bijgevolg heeft de wetgever gekozen voor een middelenverbintenis die de operatoren de mogelijkheid biedt om, op strikt noodzakelijke, evenredige en beperkte wijze, gegevens te bewaren buiten de strikt afgebakende geografische gebieden.

Het spreekt vanzelf dat deze aan de operatoren opgelegde middelenverbintenis gecontroleerd zal worden door het BIPT, dat erop zal toezien dat de operatoren, afhankelijk van de stand van de gebruikte technieken en de daaraan verbonden kosten, alles in het werk stellen om de geografische zones zo nauwkeurig mogelijk af te bakenen.

Er bestaat ook een risico dat daders van inbreuken zich organiseren om inbreuken te plegen in gebieden waar de gegevensbewaring niet van toepassing is.

De wetgever heeft besloten gegevens te bewaren over gebieden waar de openbare veiligheid ernstig wordt bedreigd, gezien het hoge aantal ernstige misdrijven per 1 000 inwoners dat daar de afgelopen 3 jaren is gepleegd. Hoewel dit percentage een onbetwistbare indicator is van hoge niveaus van criminele activiteit, zou het voor een goed begrip absurd zijn alleen de straten en GPS-coördinaten waar deze ernstige misdrijven hebben plaatsgevonden, in het vizier te nemen, omdat dit zou impliceren dat criminele patronen volkomen voorspelbaar zijn en noodzakelijkerwijs op dezelfde plaatsen plaatsvinden. Ook hier is het echter mogelijk om niet het gehele grondgebied te bestrijken, maar de omvang van de bedreiging voor de openbare veiligheid per gerechtelijk arrondissement of per politiezone te bekijken.

Het aantal misdrijven dat in een bepaald gebied wordt gepleegd, is een betrouwbare indicator van diverse verschijnselen. In de eerste plaats geeft het aan hoe vaak een bepaald gebied het slachtoffer is geweest van een misdrijf van een bepaalde omvang, hetgeen ontegenzeggelijk van invloed is op het gevoel van onveiligheid van de bevolking. Ten tweede is het ook een betrouwbare indicator voor de gevoeligheid van het gebied voor criminele verschijnselen. Voor een bepaalde categorie van feiten valt namelijk niet te ontkennen dat criminologische factoren zoals de sociale en economische structuur van het gebied, de aanwezigheid van faciliterende wegen, de afstand tot politiebureaus, enz. een belangrijke rol spelen bij bepaalde criminele verschijnselen. Aangezien deze factoren een zekere duurzaamheid hebben, beïnvloeden zij de herhaling van soortgelijke strafbare feiten.

De ce fait, le nombre de faits passés est dans une certaine mesure un indicateur du nombre de faits futurs. Ex: les home-jacking se concentrent dans les quartiers où le niveau économique est plus élevé et dans des quartiers à proximité d'axes routiers, les vols avec violence dans des boutiques de nuit, l'importation de stupéfiants dans les ports, etc.

La conjonction du sentiment d'insécurité (liée à l'obligation de l'état d'apporter une assistance, certainement aux victimes primaires) et la répétition de certains phénomènes criminels dans des zones déterminées donne au critère "Nombre de faits par rapport aux nombre d'habitants" tout son sens et sa pertinence.

C'est également ce sentiment d'insécurité qui justifie que le nombre de faits est mis en relation avec un nombre d'habitants et non une superficie donnée. Ce sentiment d'insécurité est influencé par divers facteurs, dont notamment le risque d'être exposé à un fait, à sa gravité et à la connaissance de l'existence de faits similaires et de leur répétition: 3 faits graves qui se déroulent sur une année sur un territoire d'une commune de 20 km^2 auront généralement plus d'impact dans la population si cette commune ne compte que peu d'habitants, par rapport aux mêmes faits, que dans une commune pourtant plus petite en superficie mais qui compte 150 000 habitants.

Les attentes de la population vis-à-vis de la police pour résoudre les faits passés et prévenir des faits futurs seront plus présentes dans ce premier cas que dans la deuxième situation. Ceci démontre l'impact relatif et réduit de la notion de superficie, en faveur du nombre d'habitants.

Aux termes de cet examen minutieux, validé par un organe indépendant, des statistiques de criminalité grave, arrondissement judiciaire par arrondissement judicaire, lesquelles objectivent le nombre élevé d'actes de criminalité grave, le gouvernement estime qu'il n'est pas impossible que l'entièreté du territoire national soit visé par une conservation des données. Autrement formulé, une approche ciblée de la conservation des données à l'aide du critère de statistique n'exclut pas d'avoir comme conséquence possible, que l'entièreté du territoire national soit couvert. Si cette hypothèse est rencontrée, il s'agira alors d'une conservation ciblée dans son approche mais généralisée dans ses conséquences.

Une conservation ciblée géographique des données est également prévue en cas de menace grave, réelle et actuelle pour la sécurité nationale. Cette menace est établie par l'OCAM en cas de niveau de la menace 3 ou 4.

Bijgevolg is het aantal feiten in het verleden tot op zekere hoogte een indicator voor het aantal toekomstige feiten. Bv.: homejacking is geconcentreerd in buurten met een hoger economisch niveau en in buurten dicht bij wegen, berovingen met geweld in nachtwinkels, drugsinvoer in havens, enz.

De combinatie van het onveiligheidsgevoel (dat verband houdt met de verplichting van de Staat om bijstand te verlenen, zeker aan de eerste slachtoffers) en de herhaling van bepaalde criminele verschijnselen in bepaalde gebieden geeft het criterium "Aantal incidenten in verhouding tot het aantal inwoners" zijn volledige betekenis en relevantie.

Het is ook dit onveiligheidsgevoel dat rechtvaardigt dat het aantal feiten wordt gerelateerd aan een aantal inwoners en niet aan een bepaalde oppervlakte. Dit onveiligheidsgevoel wordt door verschillende factoren beïnvloed, waaronder met name het risico om aan een incident te worden blootgesteld, de ernst ervan en de kennis van het bestaan van soortgelijke incidenten en de herhaling ervan: 3 ernstige feiten die zich in de loop van een jaar in een gemeente van 20 km^2 voordoen, zullen over het algemeen een grotere impact hebben op de bevolking indien deze gemeente slechts weinig inwoners telt, dan dezelfde incidenten in een gemeente die qua oppervlakte kleiner is, maar 150 000 inwoners telt.

De verwachtingen van de bevolking ten opzichte van de politie om feiten uit het verleden op te lossen en feiten in de toekomst te voorkomen, zullen in het eerste geval meer aanwezig zijn dan in het tweede. Hieruit blijkt de relatieve en beperkte invloed van het begrip oppervlakte, ten gunste van het aantal inwoners.

Op grond van dit zorgvuldige, door een onafhankelijk orgaan gevalideerde onderzoek van de statistieken van ernstige criminaliteit, gerechtelijk arrondissement per gerechtelijk arrondissement, waaruit het hoge aantal zware misdrijven objectief valt af te leiden, is de regering van mening dat het niet onmogelijk is dat het gehele nationale grondgebied onder de gegevensbewaring valt. Met andere woorden, een gerichte benadering van gegevensbewaring op basis van het statistische criterium sluit niet uit dat het gehele nationale grondgebied wordt bestreken. Indien aan deze hypothese wordt voldaan, dan is er sprake van bewaring die doelgericht is in haar aanpak maar veralgemeend in haar gevolgen.

Er wordt ook in een gerichte geografische bewaring van de gegevens voorzien in geval van ernstige, reële en actuele bedreiging voor de nationale veiligheid. Deze bedreiging wordt vastgesteld door het OCAD in geval van dreigingsniveau 3 of 4.

Le législateur a également, comme le permet la Cour, prévu la conservation des données dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave, dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population et dans les zones où il y a une menace grave potentielle pour les intérêts des institutions internationales.

2.5. Garanties auprès des opérateurs concernant la fourniture des données

Il est bien entendu important de rappeler qu'outre les nouveaux critères et les garanties apportées au niveau de la conservation des données, les principes de demande de données auprès des différents opérateurs (demande uniquement sur la base du besoin d'en connaître et d'une autorisation judiciaire) restent entièrement d'application. Un croisement en masse et une vue constante et générique de l'ensemble des données d'identification et des métadonnées de l'ensemble de la population tant dans le chef des autorités répressives que des opérateurs constituaient et constituent dès lors des craintes absolument non fondées.

Par ailleurs, la Cour de Justice de l'Union européenne insiste aussi sur la nécessité de prendre des mesures afin de prévenir les risques d'abus des données conservées. Ici aussi, il faut rappeler les mesures déjà mises en place en Belgique:

— il y a, au sein des opérateurs, une cellule dédiée uniquement aux demandes des autorités judiciaires ou des services de renseignement;

— les membres de cette cellule font l'objet d'une vérification de sécurité avant de rejoindre cette cellule;

— ces membres sont soumis au secret professionnel.

Afin de rencontrer les critiques de la Cour de Justice de l'Union européenne, ces mesures ont été renforcées. Concernant l'obligation pour les opérateurs de tenir un journal, la loi précise dorénavant que le journal doit être complété pour l'ensemble des traitements réalisés au profit des autorités pendant 10 ans et que ce journal, également accessible à l'IBPT et à l'Autorité de protection des données, doit être automatisé afin d'éviter les risques de falsification.

De wetgever heeft ook, zoals toegestaan door het Hof, voorzien in de bewaring van gegevens in de zones die in het bijzonder zijn blootgesteld aan dreigingen voor de nationale veiligheid of grote risico's van zware criminaliteit, in de zones waar een mogelijke ernstige bedreiging bestaat voor de vitale belangen van de natie of voor de essentiële behoeften van de bevolking en in de zones waarin een mogelijke ernstige bedreiging bestaat voor de belangen van de internationale instellingen.

2.5. Waarborgen bij de operatoren betreffende de toegang tot de gegevens

Er zij uiteraard aan herinnerd dat, naast de nieuwe criteria en de geboden garanties voor de bewaring van gegevens, de beginselen van toegang tot gegevens bij de operatoren (toegang uitsluitend op basis van het "need-to-know"-beginsel en met toestemming van de rechter) volledig van toepassing blijven. Massale kruiscontroles en een voortdurend en algemeen overzicht van alle identificatie-, verkeers- en locatiegegevens van de gehele bevolking zowel in hoofde van de gerechtelijke autoriteiten als van de operatoren waren en zijn derhalve volkomen ongegronde angsten.

Bovendien wijst het Hof van Justitie van de Europese Unie ook op de noodzaak om maatregelen te nemen om de risico's van misbruik van de bewaarde gegevens te voorkomen. Ook hier moet worden herinnerd aan de maatregelen die reeds in België van kracht zijn:

— er is bij de operatoren een cel die zich uitsluitend bezighoudt met de verzoeken van de gerechtelijke autoriteiten of de inlichtingendiensten;

— de leden van deze cel worden onderworpen aan een veiligheidscontrole voordat zij tot de cel toetreden;

— deze leden zijn onderworpen aan het beroepsgeheim.

Om tegemoet te komen aan de kritiek van het Hof van Justitie van de Europese Unie zijn deze maatregelen aangescherpt. Betreffende de verplichting voor de operatoren om een logboek bij te houden, schrijft de wet voortaan voor dat het logboek moet worden ingevuld voor alle verwerkingen uitgevoerd voor de autoriteiten gedurende 10 jaar en dat dit logboek, ook toegankelijk voor het BIPT en de Gegevensbeschermingsautoriteit, in belangrijke mate moet geautomatiseerd zijn om het risico van vervalsing te voorkomen.

2.6. La fourniture aux autorités des données conservées

Le projet de loi aborde également la fourniture aux autorités compétentes des données conservées. L'article 127/1 de la loi sur les communications électroniques contient une liste des catégories d'autorités qui peuvent demander des données d'identification ou des métadonnées conservées par les opérateurs en vertu de ces articles au profit des autorités, des utilisateurs finaux ou pour leurs propres besoins, dans les conditions déterminées par les lois organiques de ces autorités.

Ce projet de loi vise également à répondre aux attentes sociétales légitimes d'un monde de plus en plus digitalisé. En effet, force est de constater que l'e-commerce devient dans beaucoup de secteurs la norme. De la sorte, afin de lutter contre certaines formes d'infractions se commettant via le commerce en ligne, il est nécessaire que certains services d'inspection avec des pouvoirs d'enquêtes puissent disposer des données d'identification conservées par les opérateurs, afin de pouvoir démarrer une enquête. C'est dans cette optique que le service d'Inspection Produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement a, au chapitre 8, reçu la possibilité d'identifier des personnes morales ou physiques sur la base d'un numéro de téléphone ou d'une adresse IP. Il ne s'agit en d'autres termes que de données qui ne donnent pas d'information précise sur la vie privée des personnes concernées puisqu'elles concernent des données d'identification. Dans ces hypothèses, le critère de proportionnalité est par ailleurs immédiatement rencontré vu que, sans la fourniture de ces données, il y a une impossibilité matérielle pour ce service de remplir sa mission légale et que les enquêtes resteraient immuablement à charge de X. Le déni de cet élément factuel reviendrait conséquemment à créer dans l'internet un espace de non droit.

Afin d'exercer efficacement leurs tâches les personnes habilitées au sein du CSIRT national (rôle assuré par le Centre pour la Cybersécurité Belgique, ci-après CCB) reçoivent la possibilité de demander des données d'identification et des métadonnées aux opérateurs dans le cadre de la prévention et de la détection des infractions en matière de cybercriminalité, de la prévention de menaces contre la sécurité publique liées à la cybersécurité ainsi que de l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques.

Pour clôturer, ce projet de loi prévoit aussi quelques modifications au statut de l'IBPT. Ces modifications

2.6. De toegang van de autoriteiten tot de bewaarde gegevens

Het ontwerp van wet heeft ook betrekking op de toegang tot de bewaarde gegevens door de bevoegde autoriteiten. Deze autoriteiten worden opgesomd in het artikel 127/1 van de wet betreffende de elektronische communicatie, dat de lijst bevat van de categorieën van autoriteiten die toegang kunnen vragen tot de identificatie-, verkeers- en locatiegegevens, bewaard bij de operatoren krachtens deze artikelen ten behoeve van de autoriteiten, de eindgebruikers of voor hun eigen behoeften, onder de voorwaarden die bepaald worden door de organieke wetten van deze autoriteiten.

Met dit wetsontwerp wordt tevens beoogd tegemoet te komen aan de legitieme maatschappelijke verwachtingen van een steeds meer gedigitaliseerde wereld. Het is inderdaad duidelijk dat elektronische handel in vele sectoren de norm aan het worden is. Zo is het voor de bestrijding van bepaalde vormen van strafbare feiten die via de onlinehandel worden gepleegd, noodzakelijk dat bepaalde inspectiediensten met opsporingsbevoegdheid toegang hebben tot de door de operatoren bijgehouden identificatiegegevens, zodat zij een onderzoek kunnen instellen. Met het oog hierop heeft de inspectiedienst consumentenproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, in de hoofdstuk 8, de mogelijkheid gekregen om rechtspersonen of natuurlijke personen te identificeren op basis van een telefoonnummer of IP-adres. Met andere woorden, de gegevens zijn niet gevoelig omdat zij identificatiegegevens betreffen. In deze gevallen is ook onmiddellijk voldaan aan het evenredigheidscriterium, aangezien het zonder deze toegang materieel onmogelijk zou zijn voor deze dienst om zijn wettelijke taak te vervullen en de onderzoeken altijd ten laste van X zouden blijven vallen. De ontkenning van dit feitelijke element zou bijgevolg neerkomen op het creëren van een rechteloze ruimte op het internet.

Om hun taken efficiënt te kunnen uitvoeren krijgen het nationale CSIRT (rol vervuld door het Centrum voor Cybersecurity België, hierna het CCB) gemachtigde personen krijgen de mogelijkheid om identificatie-, verkeers- en locatiegegevens op te vragen bij operatoren in het kader van het voorkomen en opsporen van misdrijven inzake cybercriminaliteit, het voorkomen van bedreigingen voor de openbare veiligheid in verband met cyberbeveiliging en het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten.

Tot slot voorziet dit ontwerp van wet ook in een aantal wijzigingen in het statuut van het BIPT. Dankzij deze

permettent de confirmer que l'IBPT peut demander aux opérateurs des données d'identification et des métadonnées, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions. La pratique montre en effet qu'il est parfois nécessaire que l'IBPT prenne connaissance de ces données dans le cadre de la mise en œuvre de cette loi du 13 juin 2005 ou dans le cadre du contrôle des opérateurs télécoms.

Bien entendu, dans l'ensemble de ces hypothèses, les demandes faites aux opérateurs se déroulent via la Cellule de coordination de l'opérateur, ce qui implique que ces demandes font partie du journal tenu par les opérateurs et que celles-ci doivent être motivées et ciblées.

wijzigingen kan bevestigd worden dat het BIPT van de operatoren identificatie-, verkeers- of locatiegegevens kan vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten. De praktijk toont immers aan dat het soms noodzakelijk is dat het BIPT kennis neemt van deze gegevens in het kader van de uitvoering van deze wet van 13 juni 2005 of in het kader van de controle van de telecomoperatoren.

Uiteraard worden in al deze gevallen de verzoeken aan de operatoren via de Coördinatiecel van de operator gedaan, hetgeen impliceert dat deze vragen om toegang deel uitmaken van het logboek dat door de operatoren wordt bijgehouden en dat zij gemotiveerd en doelgericht moeten zijn.

COMMENTAIRE DES ARTICLES

TOELICHTING BIJ DE ARTIKELEN

CHAPITRE 1ER

HOOFDSTUK 1

Disposition générale

Algemene bepaling

Article 1er

Artikel 1

Conformément à l'article 83 de la Constitution, l'article premier précise que ce projet de loi règle des matières visées à l'article 74 de la Constitution.

Overeenkomstig artikel 83 van de Grondwet bepaalt artikel 1 dat het wetsontwerp aangelegenheden regelt als bedoeld in artikel 74 van de Grondwet.

CHAPITRE 2

HOOFDSTUK 2

Modifications à la loi du 13 juin 2005 relative aux communications électroniques

Wijzigingen aan de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 2 (modifications à l'article 2)

Art. 2 (wijzigingen aan artikel 2)

L'article 2 définit dorénavant la notion de fraude et d'utilisation malveillante du réseau ou du service.

L'auteur de la fraude peut être l'utilisateur final et la victime l'opérateur (par exemple, l'utilisateur final ne respecte pas les conditions générales qui le lient à l'opérateur).

L'auteur de la fraude peut aussi être un tiers, et la victime l'utilisateur final. Par exemple, un tiers fait usage d'un service de communications électroniques au nom de l'abonné à son insu, le harponnage par SMS ("*smishing*"), le harponnage par Internet ("*phishing*") ou encore un appel entrant induisant l'utilisateur final en erreur sur l'origine de cet appel et lui causant un préjudice ("*spoofing*").

Artikel 2 definieert voortaan het begrip van fraude en kwaadwillig gebruik van het netwerk of de dienst.

De fraudepleger kan de eindgebruiker zijn en het slachtoffer de operator (bijvoorbeeld, de eindgebruiker leeft de algemene voorwaarden niet na die hem aan de operator binden).

De fraudepleger kan ook een derde zijn, en het slachtoffer de eindgebruiker. Bijvoorbeeld, een derde maakt gebruik van een elektronische-communicatiedienst op naam van de abonnee buiten zijn medeweten, phishing via sms ("*smishing*"), *phishing* of een binnenkomende oproep die de eindgebruiker misleidt wat de oorsprong van deze oproep betreft en hem daarbij nadeel berokkent ("*spoofing*").

L'utilisation malveillante du réseau ou du service couvre par exemple le harcèlement par téléphone.

La définition d'appels infructueux, annulée par la Cour constitutionnelle dans son arrêt du 22 avril 2021 (arrêt n° 57/2021), est réintroduite dans l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques. Il convient cependant de noter que l'article 126 de cette même loi (conservation généralisée et indifférenciée de données d'identification) ne fait plus référence à la notion d'appels infructueux, qui est uniquement utilisée dans l'article 126/1 (conservation ciblée sur base géographique).

Le présent article reprend les définitions de "données de communications électroniques", "contenu de communications électroniques" et "métadonnées de communications électroniques" qui se trouvent dans la proposition de la Commission européenne de janvier 2017 de règlement "ePrivacy" (proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement "vie privée et communications électroniques")). Cette proposition de règlement est destinée à remplacer la directive 2002/58/CE, qui est la directive "vie privée et communications électroniques" (également connue comme la directive "ePrivacy").

Lors de la consultation des opérateurs par rapport au présent avant-projet de loi, de nombreux opérateurs ont indiqué que la définition de données de trafic ne correspond plus aux développements technologiques et économiques et ont proposé d'introduire dans la loi télécom la notion de métadonnées comme définie dans la proposition de règlement ePrivacy et de faire une distinction claire avec les informations collectées dans un but de facturation.

La notion de métadonnées doit être entendue au sens large, et inclut les données de trafic qui sont traitées en vue de l'acheminement d'une communication mais pas les données de trafic traitées uniquement en vue de la facturation du service, mais aussi les données de connexion qui ne seraient pas des données de trafic. Ces données de connexion comprennent toute donnée échangée entre un équipement terminal et le réseau de communications électroniques ou le service de communications électroniques en vue de la gestion de ce réseau ou de ce service. Ces données comprennent par exemple la localisation par le réseau des équipements terminaux à intervalles réguliers, de manière à permettre la gestion du réseau.

Kwaadwillig gebruik van het netwerk of de dienst dekt bijvoorbeeld pesterijen via de telefoon.

De definitie van oproeppogingen zonder resultaat die het Grondwettelijk Hof had vernietigd in zijn arrest van 22 april 2021 (arrest nr. 57/2021), wordt opnieuw ingevoegd in artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Er moet evenwel worden opgemerkt dat artikel 126 van diezelfde wet (algemene en ongedifferentieerde bewaring van identificatiegegevens) niet langer verwijst naar het begrip van oproeppogingen zonder resultaat, dat enkel in artikel 126/1 wordt gebruikt (gerichte bewaring op geografische basis).

Het onderhavige artikel neemt de definities over van "elektronische-communicatiegegevens", "elektronische-communicatie-inhoud" en "elektronische-communicatiemetagegevens" die vermeld zijn in het voorstel van de Europese Commissie van januari 2017 voor een "ePrivacy-verordening" (voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)). Het onderhavige voorstel voor een verordening is bestemd om Richtlijn 2002/58/EG, de "richtlijn betreffende privacy en elektronische communicatie" (ook bekend als de "ePrivacy-verordening"), te vervangen.

Tijdens de raadpleging van de operatoren over het onderhavige voorontwerp van wet hebben talrijke operatoren laten weten dat de definitie van verkeersgegevens niet langer overeenstemt met de technologische en economische ontwikkelingen en hebben zij voorgesteld om in de telecomwet het begrip metagegevens in te voeren, zoals dit gedefinieerd is in het voorstel voor een ePrivacy-verordening, en om een duidelijk onderscheid te maken met de informatie die wordt verzameld met het oog op facturering.

Het begrip metagegevens moet worden opgevat in de ruime betekenis en omvat de verkeersgegevens die worden verwerkt met het oog op het routeren van communicatie, maar niet de verkeersgegevens die uitsluitend worden verwerkt met het oog op de facturering van de dienst, maar ook de verbindingsgegevens die geen verkeersgegevens zouden zijn. Deze verbindingsgegevens omvatten alle gegevens die worden uitgewisseld tussen een eindtoestel en het elektronische-communicatienetwerk of de elektronische-communicatiedienst met het oog op het beheer van dat netwerk of van die dienst. Die gegevens omvatten bijvoorbeeld de regelmatige plaatsbepaling door het netwerk van de eindtoestellen, zodat het netwerk kan worden beheerd.

Art. 3 (remplacement de l'article 107/5)

Les systèmes d'encryptage se révèlent être des outils efficaces pour garantir un niveau élevé de sécurité des communications. Par principe, ils doivent donc être encouragés, en ce compris ceux mis en place par les opérateurs.

L'encryptage (le chiffrement) constitue l'une des méthodes efficaces utilisées notamment pour sécuriser les transactions financières ou empêcher des personnes non autorisées de prendre connaissance du contenu de communications privées. L'encryptage est nécessaire, non seulement pour la protection de la vie privée, mais également pour préserver notre potentiel scientifique et économique, pour maintenir la compétitivité de nos entreprises, pour protéger le secret médical et les secrets des affaires.

L'article proposé veut réaffirmer de manière très claire et incontestable dans son paragraphe 1er que l'encryptage doit être favorisé. Bien entendu comme tout objectif, il n'est pas absolu et il appartient au législateur de fixer les limites dans lesquelles l'encryptage doit être favorisé.

L'article 107/5 de la loi (l'article 48 avant la transposition dans la loi télécom du Code des communications électroniques européen) précise en effet que "L'emploi de la cryptographie est libre". Cet article avait initialement été inséré dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (à l'article 109*ter* F) suite à la libéralisation du secteur des télécommunications. L'exposé des motifs de la loi du 19 décembre 1997 précisait la nécessité de cette insertion comme suit: "Ceci est nécessaire afin de montrer l'évolution par rapport à la législation précédente qui entendait soumettre la cryptographie à des procédures de dépôt de clés. En effet, l'état de l'art ne permet pas la mise en œuvre d'un tel système à l'heure actuelle. Dès lors, étant entendu que la cryptographie est nécessaire au développement du commerce sur les autoroutes de l'information et à une meilleure protection des données à caractère personnel, il est apparu nécessaire de faciliter l'usage de ces techniques. Ceci ne signifie pas que le législateur ait complètement abandonné toute volonté de pouvoir à l'avenir avoir accès aux messages en clair lorsque des écoutes judiciaires ont été autorisées. Cette problématique sera revue plus tard au vu de l'évolution de la technologie ou d'un usage abusif de la cryptographie par des structures mafieuses ou terroristes." (Parl. Chambre, 49-1265/1, p. 55).

Art. 3 (vervanging van artikel 107/5)

Encryptiesystemen blijken doeltreffende tools te zijn om een hoog niveau van veiligheid van de communicatie te garanderen. Ze moeten dus principieel worden aangemoedigd, ook deze ingevoerd door de operatoren.

Encryptie (versleuteling) is een doeltreffende (maar niet de enige) methode om bijvoorbeeld betalingsverkeer te beveiligen, of om te verhinderen dat onbevoegden kennis kunnen nemen van de inhoud van privécommunicatie. Encryptie is noodzakelijk, niet enkel voor het privéleven, maar ook voor de vrijwaring van ons wetenschappelijk en economisch potentieel, het handhaven van de competitiviteit van onze bedrijven, het beschermen van het medisch geheim en bedrijfsgeheimen.

Het voorgestelde artikel wil in paragraaf 1 nogmaals heel duidelijk en zeker bevestigen dat de voorkeur moet worden gegeven aan versleuteling. Net als elke doelstelling is die natuurlijk niet absoluut en komt het aan de wetgever toe om de limieten vast te stellen waarbinnen de voorkeur moet uitgaan naar versleuteling.

Artikel 107/5 van de wet (artikel 48 vóór de omzetting van het Europees wetboek voor elektronische communicatie in de telecomwet) bepaalt immers: "Het gebruik van versleuteling is vrij". Dat artikel was aanvankelijk ingevoegd in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (in artikel 109*ter* F) na de liberalisering van de telecommunicatiesector. De memorie van toelichting bij de wet van 19 december 1997 verduidelijkte de noodzaak tot deze invoeging als volgt: "Dit is nodig om de ontwikkeling aan te tonen ten opzichte van de voorgaande wetgeving die de versleuteling aan procedures wilde onderwerpen in verband met de neerlegging van sleutels. Technisch is de verwezenlijking van een dergelijk systeem momenteel in feite onmogelijk. Vandaar dat het noodzakelijk is gebleken om het gebruik van die technieken te vergemakkelijken aangezien versleuteling nodig is voor de ontwikkeling van de handel op de informatiesnelwegen en voor een betere bescherming van de persoonsgebonden gegevens. Dit betekent niet dat de wetgever volledig alle wil heeft laten varen om in de toekomst toegang te hebben tot ongecodeerde berichten, wanneer toestemming is verleend voor afluistering door het gerecht. Die problematiek zal later worden herzien gelet op de ontwikkeling van de technologie of van misbruik van de versleuteling door maffiaorganisaties of terroristen." (Parl. Kamer, 49-1265/1, blz. 55).

Plus de 20 ans après cette disposition initiale, les paragraphes 2 à 4 de l'article 107/5 fixent une série de restrictions à la liberté d'encryptage.

Ces restrictions peuvent être résumées comme suit:

i) l'utilisation de l'encryptage ne doit pas empêcher un utilisateur d'appeler les services de secours, ni les services de secours d'identifier et de localiser l'appelant;

ii) l'utilisation de l'encryptage, qu'il soit ou non de bout en bout, ne peut pas empêcher un opérateur de remplir ses obligations en matière de conservation des données (données concernant les communications qui ont eu lieu dans un laps de temps déterminé dans le passé – métadonnées des communications);

iii) l'utilisation de l'encryptage par un opérateur étranger ne peut avoir pour conséquence que les opérateurs, dans le cas des personnes qui utilisent une carte SIM étrangère dans leur appareil (inroamers) sur notre territoire, du fait de cet encryptage, ne puissent plus respecter les dispositions légales en matière de conservation des données et d'interception du contenu de la communication.

Le Roi fixe les modalités exactes selon lesquelles les opérateurs, dans le cadre de ces principes, doivent coopérer.

Ces restrictions sont expliquées en détail ci-dessous:

Paragraphe 2

1e restriction: l'utilisation de l'encryptage ne doit pas empêcher un utilisateur d'appeler les services de secours ou d'identifier et de localiser l'appelant.

Tout d'abord, les systèmes d'encryptage ne peuvent pas avoir pour effet d'empêcher les communications d'urgence (paragraphe 2). Cette restriction porte tant sur le chiffrement des appareils, que des réseaux ou des communications. Elle n'appelle pas en soi beaucoup de commentaires.

Meer dan 20 jaar later, stellen de paragrafen 2 tot 4 van artikel 107/5 specifiek 4 beperkingen aan de vrijheid van versleuteling.

Deze beperkingen kunnen als volgt kort samengevat worden:

i) het gebruik van versleuteling mag niet beletten dat een gebruiker de hulpdiensten kan bellen, noch dat de hulpdiensten de oproeper kunnen identificeren en localiseren;

ii) het gebruik van versleuteling, of de versleuteling nu end-to-end is of niet, mag niet tot gevolg hebben dat een operator niet kan voldoen aan haar verplichtingen inzake dataretentie (gegevens over de communicatie die binnen een bepaalde tijd in het verleden gebeurd zijn – metadata van de communicatie);

iii) het gebruik van versleuteling door een buitenlandse operator mag niet tot gevolg hebben dat de operatoren, bij personen die een buitenlandse SIM kaart in hun toestel gebruiken (inroamers) op ons grondegebied, als gevolg van deze versleuteling, niet meer kunnen voldoen aan de wettelijke bepalingen rond dataretentie en het onderscheppen van de inhoud van de communicatie.

De koning bepaalt de precieze modaliteiten waaronder de operatoren, binnen deze principes, moeten meewerken.

Hieronder worden deze beperkingen in detail toegelicht:

Paragraaf 2

1e beperking: het gebruik van versleuteling mag niet verhinderen dat een gebruiker de hulpdiensten kan bellen, noch dat de oproeper geïdentificeerd en gelokaliseerd kan worden.

Allereerst mogen de versleutelingssystemen niet tot gevolg hebben dat noodcommunicatie wordt verhinderd (paragraaf 1, eerste lid, 1°). Deze beperking geldt zowel voor de versleuteling van het toestel, de netwerken als de communicatie zelf. Deze bepaling behoeft als dusdanig weinig commentaar.

Paragraphe 3

2e restriction: l'utilisation de l'encryptage des communications ne doit pas empêcher un opérateur de remplir ses obligations en matière de conservation des données.

En d'autres termes, l'encryptage ne doit pas empêcher l'opérateur de fournir des données d'identification ou de trafic aux autorités.

Les systèmes d'encryptage/de sécurité, ne peuvent pas avoir comme corollaire qu'un opérateur ne soit plus en mesure de conserver les données d'identification, de trafic ou de localisation pour les autorités comme c'est prévu par la loi (notamment la loi télécoms, le Code d'instruction criminelle, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers). Les métadonnées de communication ne peuvent donc jamais être encapsulées dans un chiffrement end to end.

Les communications privées comprennent également les communications dites de machine à machine, qui peuvent s'avérer particulièrement utiles dans le cadre d'une instruction, par exemple lorsque le juge d'instruction souhaite avoir un aperçu des signaux émis par un véhicule, de plus en plus souvent équipé de cartes SIM qui transmettent les signaux de capteurs.

Au point 162 de son avis, l'Autorité de protection des données considère que "l'interdiction d'utiliser des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que la conservation des données d'identification, de trafic ou de localisation constitue une ingérence disproportionnée dans le droit au respect de la vie privée des personnes concernées et qui excède dès lors ce qui est nécessaire dans une société démocratique."

Toutefois, si on doit considérer que la remarque de l'Autorité de protection des données porte sur des systèmes d'encryptage, il convient de rappeler que l'article 107/5 en projet interdit un système d'encryptage qui rend impossible la conservation par les opérateurs des données d'identification, de trafic ou de localisation. En effet, quelle serait l'utilité d'imposer, d'une part, aux opérateurs une obligation de conserver ces données, mais, d'autre part, de ne pas faire respecter cette obligation dans la pratique en raison de l'utilisation d' un système d'encryptage? En outre, cela signifierait que la restriction visée au paragraphe 1er ne serait pas non plus respectée.

Paragraaf 3

2e beperking: het gebruik van versleuteling mag niet tot gevolg hebben dat een operator niet kan voldoen aan zijn verplichtingen inzake dataretentie.

Versleuteling mag met andere woorden niet verhinderen dat de operator identificatie- of verkeersgegevens aan de autoriteiten kan verstrekken.

Deze versleutelings-/beveiligingssystemen mogen niet tot gevolg hebben dat een operator niet langer in staat is om de identificatie-, verkeers- of locatiegegevens te bewaren voor de autoriteiten zoals voorgeschreven door de wet (met name de telecomwet, het Wetboek van Strafvordering, de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten). De metagegevens van communicatie mogen dus nooit ingekapseld zitten in end-to-end encryptie.

Met privécommunicatie wordt ook zogenaamde machine-to-machine communicatie bedoeld die bijzonder nuttig kan zijn voor een strafonderzoek, bijvoorbeeld wanneer de onderzoeksrechter zicht wil krijgen op de signalen van een voertuig, die steeds vaker uitgerust zijn met simkaarten die signalen van sensoren doorsturen.

In punt 162 van haar advies maakt de Gegevensbeschermingsautoriteit de bedenking dat "het verbod op het gebruik van systemen die de identificatie van de eindgebruiker kunnen verhinderen, het traceren en lokaliseren van niet openbaar beschikbare communicatie en het bewaren van identificatie-, verkeers- of locatiegegevens een onevenredige aantasting [vormt] van het recht op eerbiediging van het privéleven van de betrokkenen, en […] dus verder [gaat] dan wat in een democratische samenleving noodzakelijk is."

Echter, als ervan moet worden uitgegaan dat de opmerking van de Gegevensbeschermingsautoriteit betrekking heeft op versleutelingssystemen, moet eraan worden herinnerd dat het ontworpen artikel 107/5 een versleutelingssysteem dat het voor de operatoren onmogelijk maakt om identificatie-, verkeers- of locatiegegevens te bewaren, wel degelijk verbiedt. Welk nut zou het immers hebben om de operatoren enerzijds te verplichten tot het bewaren van deze gegevens, maar anderzijds deze verplichting in de praktijk niet af te dwingen door het gebruik van een versleutelingssysteem? Bovendien zou dit betekenen dat ook niet voldaan zou worden aan de in paragraaf 1 omschreven beperking.

Le législateur reconnaît l'atteinte considérable à la vie privée que représente l'interception du contenu des communications. En ce qui concerne les données d'identification des utilisateurs, dont la Cour de justice de l'Union européenne indique elle-même qu'elles peuvent être considérées comme non sensibles dans certains cas, et les données de trafic et de localisation, qui sont effectivement sensibles mais moins sensibles que leur contenu, le législateur estime approprié et proportionné d'imposer cette obligation, dans les conditions prévues aux articles 126 et 126/1 du présent projet.

En effet, comme l'a indiqué la Cour de justice de l'Union européenne dans l'arrêt quadrature du Net, les "États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est "nécessaire, appropriée et proportionnée au sein d'une société démocratique" au regard des objectifs que cette disposition énonce.".

Paragraphe 3

3e restriction: l'utilisation de l'encryptage par un opérateur étranger ne peut avoir pour conséquence que les opérateurs, dans le cas des personnes qui utilisent une carte SIM étrangère dans leur appareil (inroamers) sur notre territoire, du fait de cet encryptage, ne puissent plus respecter les dispositions légales en matière de conservation des données et d'interception du contenu de la communication.

L'introduction de la 5G et de la VoLTE affecte les relations entre les différents opérateurs.

Ces normes modifient radicalement la manière dont la communication vocale est traitée sur le plan technique.

La possibilité pour un opérateur belge de répondre à une requête des autorités belges visant à prendre connaissance du contenu de la communication de ce que l'on appelle les "inroamers" (cartes SIM étrangères actives sur notre réseau) n'est pas prévue dans les normes de la 5G. (Cette possibilité s'appelait le "local break-out").

Avec la disparition de cette possibilité dans les normes techniques des communications, les contrats d'itinérance des opérateurs belges avec les opérateurs étrangers sur la 5G deviennent extrêmement importants (par exemple, déjà avec AT&T en 2022). En d'autres termes, ce paragraphe doit permettre aux opérateurs belges d'imposer dans leurs accords avec les opérateurs étrangers qu'ils

De wetgever erkent de grote inbreuk op het privéleven wat betreft het onderscheppen van de inhoud van de communicatie. Wat betreft de identificatiegegevens van een gebruiker, waarvan de rechtspraak van het Europees Hof van Justitie zelf aangeeft dat ze in bepaalde gevallen als niet-gevoelig kunnen worden beschouwd, en de verkeers- en lokalisatiegegevens, die wel degelijk gevoelig zijn maar dan weer minder gevoelig dan de inhoud, oordeelt de wetgever dat het redelijk en proportioneel is om, binnen de voorwaarden bepaald in artikels 126 en 126/1 van dit ontwerp, deze verplichting op te leggen.

Immers, zoals het Europees Hof van Justitie in arrest-Quadrature du Net stelt, "[kunnen] de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens […] treffen wanneer een dergelijke maatregel „in een democratische samenleving noodzakelijk, redelijk en proportioneel is" in het licht van de in die bepaling genoemde doelstellingen.".

Paragraaf 3

3e beperking: het gebruik van versleuteling door een buitenlandse operator mag niet tot gevolg hebben dat de operatoren, bij personen die een buitenlandse SIM kaart in hun toestel gebruiken (inromaers) op ons grondegebied, als gevolg van deze versleuteling, niet meer kunnen voldoen aan de wettelijke bepalingen rond dataretentie en het onderscheppen van de inhoud van de communicatie.

De introductie van 5G en VoLTE heeft gevolgen voor de verhouding tussen verschillende operatoren.

Deze normen brengen een drastische verandering aan aan de manier waarop gesproken communicatie op technisch vlak wordt behandeld.

De mogelijkheid voor een Belgische operator om te voldoen aan een verzoekschrift van de Belgische autoriteiten om kennis te nemen van de inhoud van de communicatie van zogenaamde "inroamers" (buitenlandse sim-kaarten actief op ons netwerk), zijn niet voorzien in de standaarden voor 5G. (Deze mogelijkheid heette "local break-out").

Met het verdwijnen van deze mogelijkheid binnen de technische standaarden van de communicatie, worden de roamingcontracten van Belgische operatoren met buitenlandse operatoren over 5G uitermate belangrijk (bijvoorbeeld al met AT&T in 2022). Deze paragraaf moet met andere woorden toelaten aan Belgische operatoren om af te dwingen in haar overeenkomsten met buitenlandse

puissent se conformer aux mêmes dispositions légales que pour leurs propres utilisateurs. L'absence de cette disposition signifierait en effet que, dans certains cas, seul l'opérateur étranger ou une puissance étrangère serait en mesure d'intercepter un utilisateur étranger dans notre pays. Cette situation porterait gravement atteinte à notre souveraineté.

En pratique, en cas d'itinérance et d'utilisation de la technologie VoLTE, les opérateurs devront analyser les flux de données (données de trafic) afin de conserver les données, comme l'exige la loi télécoms. Pour que l'opérateur belge puisse analyser ces données, elles ne doivent pas pouvoir être cryptées par l'opérateur étranger. La technologie VoLTE est une technologie de transport de voix qui tire son nom de "*Voice over LTE*", parfois appelée voix LTE (*Long-Term Evolution*). VoLTE est utilisée sur les réseaux mobiles 4G LTE.

Concrètement, lors de la conclusion de contrat d'itinérance avec les opérateurs étrangers, les opérateurs belges doivent s'appuyer sur le droit belge pour exiger que l'interception des communications reste possible.

Afin de garantir l'effectivité de cette disposition, il est prévu que toute clause contractuelle y faisant obstacle est interdite et nulle.

Cet alinéa répond par ailleurs à une demande formulée par les opérateurs belges lors de la consultation publique, qui estiment qu'il est important que les dispositions concernant les systèmes de cryptage se trouvent dans la loi, de sorte qu'ils puissent les imposer à leurs partenaires de roaming.

Il est également nécessaire d'inclure cette disposition pour empêcher les criminels et autres personnes mal intentionnées d'échapper simplement aux autorités judiciaires ou aux services de renseignement belges en utilisant des cartes SIM étrangères qui ne peuvent être interceptées.

Art. 4 (insertion de l'article 121/8)

Face à l'augmentation et à la diversification des cas de fraude commises par le biais des services de communications électroniques et d'utilisation malveillante des réseaux et services de communications électroniques, le cadre juridique existant est apparu insuffisant pour assurer une réaction rapide et efficace de la part des opérateurs et du régulateur.

operatoren, dat ze kunnen voldoen aan dezelfde wettelijke bepalingen als voor haar eigen gebruikers. Het ontbreken van deze bepaling zou immers betekenen dat in sommige gevallen enkel de buitenlandse operator of een buitenlandse mogendheid in staat zou zijn om het onderscheppen van een buitenlandse gebruiker in ons land mogelijk te maken. Deze situatie zou onze soevereiniteit danig aantasten.

In de praktijk zullen de operatoren in geval van roaming en gebruik van de VoLTE-technologie de datastromen (verkeersgegevens) moeten analyseren om de gegevens te kunnen bewaren, zoals de telecomwet dat oplegt. Opdat de Belgische operator deze gegevens kan analyseren mogen deze niet kunnen worden versleuteld door de buitenlandse operator. De VoLTE-technologie is een technologie voor spraakoverdracht, waarvan de naam komt van "*Voice over LTE*", soms spraak-LTE genoemd (*Long-Term Evolution*). VoLTE wordt toegepast op mobiele 4G-LTE-netwerken.

Concreet betekent dit dus dat Belgische operatoren zich bij het sluiten van roamingovereenkomsten met buitenlandse operatoren moeten beroepen op de Belgische wetgeving om te eisen dat het onderscheppen van communicatie mogelijk blijft.

Om de doeltreffendheid van deze bepaling te waarborgen, is bepaald dat elk contractueel beding dat eraan in de weg staat, verboden en nietig is.

Deze paragraaf beantwoordt overigens aan een vraag die tijdens de openbare raadpleging geformuleerd is door de Belgische operatoren, die van oordeel zijn dat het belangrijk is dat de bepalingen betreffende de versleutelingssystemen zich in de wet bevinden, zodat zij die kunnen opleggen aan hun roamingpartners.

Het inschrijven van deze bepaling is ook noodzakelijk om te verhinderen dat criminelen en andere personen met slechte bedoelingen simpelweg aan het Belgische gerecht of de inlichtingendiensten kunnen ontsnappen door gebruik te maken van buitenlandse SIM-kaarten die niet onderschept kunnen worden.

Art. 4 (invoeging van artikel 121/8)

In het licht van de toename en de diversifiëring van de gevallen van fraude gepleegd aan de hand van elektronische-communicatiediensten en kwaadwillig gebruik van de elektronische-communicatienetwerken en -diensten, is het huidige juridische kader ontoereikend gebleken om een snelle en doeltreffende reactie vanwege de operatoren en de regulator te kunnen garanderen.

Il apparait, en outre, que c'est de plus en plus souvent l'utilisateur final et non plus l'opérateur lui-même qui est victime de la fraude. Dès lors, l'incitation naturelle à agir contre ces pratiques pour l'opérateur est moins importante qu'en matière de sécurité des réseaux où les attaques portent directement atteinte aux réseaux et services de l'opérateur. Or, en matière de sécurité, les opérateurs sont d'ores-et-déjà soumis à des obligations étendues en vertu des articles 114 et 114/1 de la loi télécom.

Le nouvel article 121/8 qui est inséré a pour objectif de pallier ce manque.

Le premier paragraphe du nouvel article 121/8 prévoit une obligation générale pour les opérateurs de prendre les mesures appropriées, proportionnées, préventives (telles que, par exemple, des filtres de type "anti-spam" permettant de notifier au destinataire le caractère potentiellement frauduleux ou malveillant de certaines communications entrantes) et curatives (telles que, par exemple, des mesures de blocage de certaines communications identifiées comme manifestement frauduleuses ou malveillantes), compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés.

De façon similaire à ce que prévoit l'article 114 de la loi télécom en matière de sécurité des réseaux, ce premier paragraphe place les opérateurs en position de premier juge des mesures appropriées et proportionnées à adopter, compte tenu des possibilités techniques les plus récentes.

En cas de défaillance de l'opérateur, l'Institut dispose du pouvoir de lui donner des instructions contraignantes, de la même manière que le prévoit l'article 114/2 en matière de sécurité des réseaux.

En outre, le Roi est habilité à préciser les mesures à prendre par les opérateurs par voie réglementaire.

Afin d'apporter une plus grande sécurité juridique aux opérateurs lorsqu'ils sont confrontés à des cas graves de fraude ou d'utilisation malveillante qui justifient des mesures fortes, le second paragraphe du nouvel article 121/8 énonce certains exemples de mesures pouvant être prises sur le pied du paragraphe 1er, à savoir:

— des mesures au niveau du réseau, tels que le blocage des numéros, de services, des URLs, de noms

Bovendien blijkt dat het steeds vaker de eindgebruiker is en niet de operator zelf, die slachtoffer wordt van de fraude. De operator wordt dan ook van nature minder aangespoord om op te treden tegen deze praktijken dan wanneer het gaat om de netwerkveiligheid waarbij de aanvallen rechtstreeks de netwerken en diensten van de operator treffen. Wat veiligheid betreft, zijn de operatoren overigens reeds onderworpen aan uitgebreide verplichtingen krachtens de artikelen 114 en 114/1 van de telecomwet.

Het nieuwe artikel 121/8 dat wordt ingevoegd heeft tot doel die leemte te vullen.

De eerste paragraaf van het nieuwe artikel 121/8 voorziet in een algemene verplichting voor de operatoren om de gepaste, evenredige, preventieve maatregelen (bijvoorbeeld, filters van het type "antispam" die het mogelijk maken om de bestemmeling kennis te geven van de potentieel frauduleuze of kwaadwillige aard van sommige binnenkomende berichten) en curatieve maatregelen (bijvoorbeeld maatregelen om bepaalde berichten te blokkeren die geïdentificeerd worden als duidelijk frauduleus of kwaadwillig) te nemen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en te vermijden dat de eindgebruikers nadeel ondervinden of lastiggevallen worden.

Op gelijkaardige wijze als de bepalingen van artikel 114 van de telecomwet inzake netwerkveiligheid, maakt deze eerste paragraaf van de operatoren de eerstgeplaatsten om te oordelen over de te treffen gepaste en evenredige maatregelen, rekening houdende met de meest recente technische mogelijkheden.

In geval van tekortkoming van de operator, beschikt het Instituut over het recht om hem dwingende instructies op te leggen, op dezelfde manier als waarin artikel 114/2 voorziet op het stuk van netwerkveiligheid.

Bovendien is de Koning gemachtigd om de door de operatoren te nemen maatregelen reglementair te preciseren.

Om de operatoren meer rechtszekerheid te geven wanneer ze worden geconfronteerd met ernstige gevallen van fraude of kwaadwillig gebruik die krachtige maatregelen vergen, lijst de tweede paragraaf van het nieuwe artikel 121/8 bepaalde voorbeeldmaatregelen op die kunnen worden getroffen in uitvoering van paragraaf 1, met name:

— maatregelen op netwerkniveau, zoals de blokkering van nummers, diensten, URL's, domeinnamen,

de domaine, d'adresses IP ou de tout autre élément d'identification de la communication électronique;

— des mesures au niveau de l'utilisateur final, telles que la désactivation complète ou partielle de certains services ou équipements.

L'article 51, § 5 existant de la loi télécom, qui est apparu inadapté dans la mesure notamment où il ne prévoit que la possibilité pour l'IBPT de prendre une mesure coercitive de blocage de numéros ou de services, ce qui ne permet pas de répondre de manière adéquate à l'ensemble des situations rencontrées, est supprimé en conséquence de l'adoption de ce nouvel article 121/8.

Art. 5 (modifications à l'article 122)

Le paragraphe 1er de l'article 122

L'article 122, qui transpose l'article 6 de la directive "vie privée et communications électroniques" (directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques), vise les données de trafic telles que définies à l'article 2, 6°, en ce compris les données de localisation, définies à l'article 2, 7°, sauf lorsque ces données de localisation ne sont pas traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication. Dans ce cas, l'article 123 leur est applicable.

Dans son avis, l'Autorité de protection des données souligne que la conservation des données de trafic ne doit pas contenir ou permettre de déduire l'URL spécifique des pages web visitées par les personnes concernées. Or, cette règle découle de l'interdiction de principe de prendre connaissance du contenu des communications électroniques visée à l'article 124 de la loi télécom et aux articles 259*bis* et 314*bis* du Code pénal, de sorte qu'il n'est pas requis de modifier l'article 122 à cet égard.

La version antérieure de l'article 122, § 1er, alinéa 2, prévoyait que l'alinéa 1er (l'obligation pour les opérateurs de supprimer les données de trafic ou de les rendre anonymes lorsqu'elles ne sont plus nécessaires pour la transmission de la communication) s'appliquait sans préjudice du respect des obligations de coopération prévues avec certaines autorités.

IP-adressen of elk ander element ter identificatie van de elektronische communicatie;

— maatregelen op het niveau van de eindgebruiker, zoals de volledige of gedeeltelijke deactivering van bepaalde diensten of apparatuur.

Het bestaande artikel 51, § 5, van de telecomwet dat onaangepast is gebleken, met name in de zin dat het niet voorzag in de mogelijkheid voor het BIPT om een dwangmaatregel te nemen bestaande in de blokkering van nummers of diensten, waardoor niet op gepaste wijze kan worden beantwoord aan alle situaties die zich voordoen, wordt geschrapt naar aanleiding van de aanneming van dit nieuwe artikel 121/8.

Art. 5 (wijzigingen aan artikel 122)

Paragraaf 1 van artikel 122

Artikel 122, dat artikel 6 van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie) omzet, doelt op de verkeersgegevens zoals gedefinieerd in artikel 2, 6°, inclusief de locatiegegevens, gedefinieerd in artikel 2, 7°, behalve wanneer deze locatiegegevens niet verwerkt worden met het oog op het overbrengen van communicatie via een elektronische-communicatienetwerk of de facturering van dergelijke communicatie. In dat geval is artikel 123 daarop van toepassing.

In haar advies benadrukt de Gegevensbeschermingsautoriteit dat de bewaring van de verkeersgegevens geen specifieke URL van de door de betrokken personen bezochte websites mogen bevatten, of het niet mogelijk mogen maken om dergelijke URL's af te leiden. Welnu, die regel vloeit voort uit het principsverbod om kennis te nemen van de inhoud van elektronische communicatie, bedoeld in artikel 124 van de telecomwet en in de artikelen 259*bis* en 314*bis* van het Strafwetboek, zodat het niet vereist is om artikel 122 in dat opzicht te wijzigen.

De vorige versie van artikel 122, § 1, tweede lid, bepaalde dat het eerste lid (de verplichting voor de operatoren om de verkeersgegevens te verwijderen of ze te anonimiseren wanneer ze niet langer nodig waren voor de transmissie van de communicatie) gold onverminderd de naleving van de vastgelegde verplichtingen tot samenwerking met bepaalde autoriteiten.

Dans un souci de clarté, la liste des autorités pouvant demander accès aux données est reprise de façon centralisée et adaptée à l'article 127/1.

Les paragraphes 2 et suivants de l'article 122 constituent des dérogations par rapport au paragraphe 1er. Il convient bien entendu de rappeler qu'un opérateur ne doit conserver que les données qu'il traite ou qu'il génère.

Le paragraphe 2 de l'article 122

Alors que l'ancien article 122, § 2, prévoyait une obligation pour les opérateurs de conserver des données de trafic dans le but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, cet article prévoit dorénavant une possibilité pour les opérateurs de le faire, et ce pour les raisons suivantes.

D'une part, une obligation n'est pas nécessaire, étant donné que les opérateurs ont tout intérêt à conserver ces données pour ces finalités et qu'il découle de l'article 110 de la présente loi, à tout le moins indirectement, que ces données doivent être disponibles. D'autre part, cette modification permet de se rapprocher de l'article 6, § 2, de la directive "vie privée et communications électroniques" (directive 2002/58/CE) que l'article 122, § 2 transpose. Cet article 6, § 2, prévoit que, par dérogation au principe de suppression ou d'anonymisation, les données de trafic peuvent être traitées à des fins de facturation.

La liste des données de trafic que les opérateurs devaient traiter selon l'article 122, § 2, est supprimée, étant donné que cette liste n'est plus adaptée aux différents services de communications électroniques offerts par les opérateurs.

Cette liste était surtout pertinente pour le service de téléphonie fixe et visait les données suivantes:

1° l'identification de la ligne appelante;

2° les adresses relatives à l'abonné et au lieu de raccordement, ainsi que le type d'équipement terminal;

3° le nombre total d'unités à facturer pour la période de facturation;

4° l'identification de la ligne appelée;

5° le type d'appel, l'heure à laquelle l'appel a commencé, la durée de l'appel ou la quantité de données transmises;

6° la date de la communication ou du service;

Omwille van de duidelijkheid wordt de lijst van de autoriteiten die toegang tot de gegevens kunnen vragen gecentraliseerd en aangepast in artikel 127/1.

De paragrafen 2 en volgende van artikel 122 vormen afwijkingen ten aanzien van paragraaf 1. Er dient evenwel aan te worden herinnerd dat een operator enkel de gegevens moet bewaren die hij behandelt of genereert.

Paragraaf 2 van artikel 122

Terwijl het oude artikel 122, § 2, een verplichting oplegde aan de operatoren om verkeersgegevens te bewaren teneinde de abonnees te factureren of de interconnectiebetalingen uit te voeren, voorziet dit artikel voortaan in een mogelijkheid voor de operatoren om dat te doen, om de volgende redenen.

Enerzijds is een verplichting niet nodig aangezien de operatoren er alle belang bij hebben om deze gegevens te bewaren voor die doeleinden en vloeit uit artikel 110 van deze wet al minstens onrechtstreeks voort dat deze gegevens beschikbaar moeten zijn. Anderzijds maakt deze wijziging het mogelijk om beter aan te sluiten bij artikel 6, § 2, van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) dat artikel 122, § 2, omzet. Dat artikel 6, § 2, bepaalt dat, in afwijking op het principe van verwijdering of anonimisering, de verkeersgegevens voor factureringsdoeleinden mogen worden gebruikt.

De lijst met verkeersgegevens die de operatoren dienden te behandelen volgens artikel 122, § 2, wordt geschrapt aangezien die lijst niet langer is afgestemd op de verschillende elektronische-communicatiediensten die worden aangeboden door de operatoren.

Die lijst was vooral relevant voor de vaste-telefoniedienst en beoogde de volgende gegevens:

1° de identificatie van de oproeplijn;

2° het adres van de abonnee en van de plaats van de aansluiting, alsook het soort eindapparatuur;

3° het totale aantal voor de factureringsperiode aan te rekenen eenheden;

4° de identificatie van de opgeroepen lijn;

5° het type, het tijdstip van aanvang en de duur van de oproep of de verzonden hoeveelheid gegevens;

6° de datum van de verbinding of van de dienst;

7° d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.

Le paragraphe 3 de l'article 122

L'article 122, § 3, qui transpose l'article 6, § 3 de la directive "vie privée et communications électroniques" (directive 2002/58/CE), ne subit pas de modification faisant suite à l'arrêt Quadrature du Net du 6/10/2020 de la CJUE (affaires C-511/18, C-512/18 et C-520/18: La Quadrature du Net, *French Data Network* et Ordre des barreaux francophones et germanophone).

Des modifications d'ordre légistique sont cependant opérées de manière à actualiser la référence à la réglementation en matière de protection des données à caractère personnel et à uniformiser la terminologie employée au sein des articles 122 et 123.

L'article 122, § 3, 2° et 3°, est modifié pour s'aligner sur la notion de consentement au sens du RGDP.

Les paragraphes 4 et 4/1 de l'article 122

Remarques générales de l'Autorité de protection des données

Dans son avis, l'Autorité de protection des données indique ce qui suit:

L'article 122, § 4, de la loi télécom impose aux opérateurs de conserver de manière systématique des données de localisation et d'autres données de trafic de l'ensemble des utilisateurs des moyens de communications électroniques, ce qui constitue ainsi une ingérence particulièrement grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel;

Le principe de proportionnalité exige que l'objectif d'intérêt général poursuivi par la mesure de conservation obligatoire soit en relation avec la gravité de l'ingérence qu'elle cause;

L'Autorité doute de la proportionnalité de l'obligation de conservation prévue au regard des objectifs qu'elle poursuit alors que ces objectifs, s'ils sont légitimes, ne semblent pas, à première vue, présenter le même degré d'importance que la lutte contre la criminalité grave.

Elle fait des remarques similaires pour ce qui concerne la sécurité des réseaux.

7° andere gegevens betreffende de betalingen, zoals vooruitbetaling, betaling in termijnen, afsluitingen en aanmaningen.

Paragraaf 3 van artikel 122

Artikel 122, § 3, die artikel 6, § 3, van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) omzet, ondergaat geen wijzigingen naar aanleiding van het arrest-Quadrature du Net van 6/10/2020 van het HvJ-EU (zaken C-511/18, C-512/18 en C-520/18: *La Quadrature du Net*, *French Data Network* et *Ordre des barreaux francophones et germanophone*).

Wijzigingen van wetgevingstechnische aard worden evenwel doorgevoerd teneinde de verwijzing naar de reglementering inzake bescherming van persoonsgegevens bij te werken en de terminologie gebruikt in de artikelen 122 en 123 te uniformiseren.

Artikel 122, § 3, 2° en 3°, wordt gewijzigd om zich af te stemmen op het begrip van toestemming in de zin van de AVG.

De paragrafen 4 en 4/1 van artikel 122

Algemene opmerkingen van de Gegevensbeschermingsautoriteit

In haar advies geeft de Gegevensbeschermingsautoriteit het volgende aan:

Artikel 122, § 4, van de telecomwet verplicht de operatoren om systematisch locatie- en andere verkeersgegevens te bewaren van alle elektronische-communicatiegebruikers, wat een bijzonder ernstige inmenging vormt in de rechten betreffende de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens;

Het evenredigheidsbeginsel eist dat de doelstelling van algemeen belang nagestreefd door de maatregel van verplichte bewaring in overeenstemming is met de ernst van de inmenging die ze teweegbrengt;

De Autoriteit stelt zich vragen bij de evenredigheid van de opgelegde bewaringsplicht in het licht van de doelstellingen die ze nastreeft terwijl deze doelstellingen, ook al zijn ze wettig, op het eerste zicht niet dezelfde graad van belang als de bestrijding van de zware criminaliteit lijken te vertegenwoordigen.

Ze uit gelijkaardige opmerkingen wat betreft de netwerkveiligheid.

Selon le législateur, la CJUE ne s'est pas encore prononcée à ce jour sur une obligation pour les opérateurs de conserver certaines données de trafic ou de localisation dans le cadre de la lutte contre les fraudes ou dans le cadre de la sécurité des réseaux.

Le législateur est d'avis qu'une ingérence d'une conservation de données de trafic ou de localisation dans les droits au respect de la vie privée et à la protection des données à caractère personnel est assez théorique. Cette ingérence ne se concrétise vraiment que lorsque l'opérateur fait usage des données ou lors de l'accès aux données par un tiers. À cet égard, la conservation de données de facturation constitue une conservation généralisée et indifférenciée de certaines données de trafic. Si on suit le raisonnement de l'Autorité de protection des données, une telle conservation de données constituerait une ingérence particulièrement grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel. Or les données qui sont conservées dans le cadre de la lutte contre la fraude, contre l'utilisation malveillante du réseau et pour assurer la sécurité des réseaux le sont dans l'intérêt des utilisateurs finaux des services de l'opérateur.

Par ailleurs, le législateur estime qu'il n'est pas opportun de comparer les objectifs de lutte contre la fraude commise à l'aide d'un service de communications électroniques, de lutte contre l'utilisation malveillante des réseaux et la sécurité des réseaux avec l'objectif de la lutte contre la criminalité grave.

D'abord, car si une telle comparaison devait avoir lieu, elle devrait se faire avec une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, car c'est cette dernière et non la criminalité grave qui, selon la CJUE, peut justifier une conservation généralisée et indifférenciée de données de trafic et de localisation.

Ensuite, ces objectifs ont une portée fondamentalement différente. La lutte contre la fraude commise à l'aide d'un service de communications, la lutte contre l'utilisation malveillante du réseau et la sécurité des réseaux sont des objectifs qui sont intrinsèquement liés à la fourniture du service de communications électroniques. La criminalité grave ou la sauvegarde de la sécurité nationale ne le sont pas, sauf lorsque l'infraction pénale grave ou l'acte qui porte atteinte à la sécurité nationale est commis au moyen d'un service de communications électroniques (ex. infraction pénale en ligne).

Or, tout comme les données de facturation sont indispensables pour la facturation des services de

Volgens de wetgever heeft het HvJ-EU zich tot op heden nog niet uitgesproken over een verplichting voor de operatoren om bepaalde verkeers- of locatiegegevens te bewaren in het kader van de bestrijding van fraude of in het kader van netwerkveiligheid.

De wetgever meent dat een inmenging door bewaring van verkeers- of locatiegegevens in de rechten op eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens nogal theoretisch is. Deze inmenging komt pas echt tot uiting wanneer de operator gebruik maakt van de gegevens of bij de inzage in de gegevens door een derde. In dat opzicht vormt de bewaring van factureringsgegevens een algemene en ongedifferentieerde bewaring van bepaalde verkeersgegevens. Als we de redenering van de Gegevensbeschermingsautoriteit volgen, zou een dergelijke gegevensbewaring een bijzonder ernstige inmenging vormen in de rechten op de eerbiediging van de persoonlijke levenssfeer en de bescherming van de persoonsgegevens. Overigens worden de gegevens bewaard in het kader van de bestrijding van fraude, kwaadwillig gebruik van het netwerk en om de veiligheid van de netwerken te garanderen, bewaard in het belang van de eindgebruikers van de diensten van de operator.

Verder meent de wetgever dat het niet gepast is om de doelstellingen van de bestrijding van fraude gepleegd door middel van een elektronische-communicatiedienst te vergelijken met de strijd tegen het kwaadwillig gebruik van de netwerken en de veiligheid van de netwerken met als doel de bestrijding van de zware criminaliteit.

Indien een dergelijke vergelijking zou moeten gemaakt worden, zou ze in de eerste plaats moeten gemaakt worden ten aanzien van een ernstige bedreiging voor de staatsveiligheid die reëel en actueel is, want het is dat laatste en niet de zware criminaliteit dat, volgens het HvJ-EU, een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens kan rechtvaardigen.

Die doelstellingen hebben verder ook een fundamenteel andere scope. De strijd tegen de fraude gepleegd door middel van een communicatiedienst, de strijd tegen het kwaadwillig gebruik van een netwerk en de netwerkveiligheid zijn doelstellingen die intrinsiek verband houden met de verstrekking van de elektronische-communicatiedienst. De zware criminaliteit of het vrijwaren van de staatsveiligheid zijn dat niet, tenzij wanneer de ernstige strafbare inbreuk of daad die een aanslag vormt op de staatsveiligheid wordt begaan door middel van een elektronische-communicatiedienst (bijv. online strafbaar feit).

Net zoals factureringsgegevens overigens onmisbaar zijn voor de facturering van de communicatiediensten,

communications, certaines données de trafic sont indispensables pour une lutte efficace contre les fraudes commises à l'aide d'un moyen de communications électroniques, une lutte contre les utilisations malveillantes du réseau ou la sécurité des réseaux.

Par ailleurs, au point 68 de son avis, l'Autorité de protection des données indique ce qui suit: "l'Autorité s'interroge également sur la nécessité de l'obligation de conservation préventive et systématique des données qui est imposée par le nouvel article 122, § 4, de la loi télécom à des fins de détection et d'analyse d'une fraude présumée ou d'une utilisation malveillante présumée du réseau de communications électroniques. Ces objectifs ne pourraient-ils pas être atteints par des mesures moins intrusives dans les droits et libertés des personnes concernées? Ne serait-il pas possible, par exemple, de prévoir que l'obligation de conservation des données à des fins de lutte contre la fraude et l'utilisation malveillante du réseau peut être "activée" lorsqu'il existe des indices de fraude ou d'utilisation malveillante du réseau, auquel cas la conservation serait ciblée sur les personnes susceptibles d'être mêlées d'une manière ou d'une autre à la fraude ou à l'utilisation malveillante du réseau ou qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave? Cette option rencontrerait l'exigence du "changement de perspective" mise en évidence par l'arrêt de la Cour constitutionnelle: on passerait d'une conservation préventive et généralisée à une conservation réactive et ciblée. L'Autorité rappelle qu'il incombe au législateur de justifier que l'option qu'il choisit constitue la voie la moins attentatoire aux droits et libertés des personnes concernées pour atteindre l'objectif qu'il poursuit."

Le législateur comprend et partage la préoccupation de l'APD exprimée au point 68 de son avis: la conservation des données doit être limitée à ce qui est nécessaire à la poursuite des objectifs.

Le législateur estime cependant qu'il n'est pas possible d'atteindre l'objectif poursuivi par une conservation réactive et ciblée dès le départ.

En effet, une approche réactive impliquerait que si l'opérateur prend connaissance à un moment donné, par exemple à la suite d'une information de l'abonné ou de l'interaction avec une autorité, telle que le service de médiation pour les télécommunications, d'une fraude commise antérieurement à l'aide d'un service de communications électroniques ou d'une utilisation malveillante et passée du réseau, l'opérateur ne disposera pas de données "historiques" par rapport à ce fait, car ces données n'ont pas été conservées. Or, en

zijn bepaalde verkeersgegevens onontbeerlijk voor een doeltreffende bestrijding van fraude gepleegd door middel van elektronische communicatie, de strijd tegen kwaadwillig gebruik van een netwerk of netwerkveiligheid.

In punt 68 van haar advies geeft de Gegevensbeschermingsautoriteit bovendien het volgende aan: "De Autoriteit vraagt zich ook af of een verplichting tot preventieve en systematische gegevensbewaring, zoals is voorzien in het nieuwe artikel 122, § 4, van de telecomwet, noodzakelijk is om een vermoed geval van fraude of een vermoed geval van kwaadwillig gebruik van het elektronische communicatienetwerk op te sporen en te analyseren. Kunnen die doelstellingen niet worden bereikt met maatregelen die niet zo'n zware inmenging in de rechten en vrijheden van de betrokken personen vormen? Zou het bijvoorbeeld niet mogelijk zijn om tot de bewaring van de gegevens te verplichten voor het bestrijden van fraude en kwaadwillig gebruik als er aanwijzingen bestaan van die fraude of kwaadwillig gebruik van het netwerk? De bewaring zou dan kunnen worden gericht op de personen die op de een of andere manier bij de fraude of het kwaadwillig gebruik van het netwerk kunnen betrokken zijn of die om andere redenen zouden kunnen bijdragen, via de bewaring van hun gegevens, tot de bestrijding van zware criminaliteit. Een dergelijke keuze zou voldoen aan de eis van "verandering van gezichtspunt" waarnaar wordt verwezen in het arrest van het Grondwettelijk Hof: van een preventieve en algemene bewaring zou worden overgestapt op een reactieve en gerichte bewaring. De Autoriteit benadrukt dat de wetgever dient te rechtvaardigen dat de door hem gekozen maatregel om het beoogde doel te bereiken diegene is die de rechten en vrijheden van de betrokken personen het minst aantast."

De wetgever begrijpt en deelt de bekommernis van de GBA die ze uitdrukt in punt 68 van haar advies: de bewaring van de gegevens moet beperkt worden tot wat nodig is voor de nastreving van de doelstellingen.

De wetgever meent echter dat het niet mogelijk is om het doel te verwezenlijken dat wordt nagestreefd met een bewaring die reactief en doelgericht is van bij het begin.

Een reactieve benadering zou immers inhouden dat indien de operator op een gegeven ogenblik, bijvoorbeeld via informatie van de abonnee of de interactie met een autoriteit zoals de telecomombudsdienst, kennis neemt van fraude die eerder werd begaan door middel van een elektronische-communicatiedienst of eerder gepleegd kwaadwillig gebruik van het netwerk, hij niet zal beschikken over "historische" gegevens in verband met dat feit want die zullen niet bewaard zijn. In de praktijk verloopt er bovendien nog steeds (soms relatief veel) tijd tussen

pratique, il existe presque toujours un laps de temps (parfois relativement long) entre la commission du fait qui justifie la conservation des données et le moment où l'opérateur prend connaissance de ce fait. En d'autres termes, l'utilité d'une conservation préventive (ou de données historiques) est qu'elle permet de remonter dans le passé, ce que ne permet pas une conservation réactive. Comme il sera expliqué ci-après, la plupart du temps, l'opérateur n'est pas en mesure de détecter (et donc d'empêcher) la commission de la fraude ou de l'utilisation malveillante du réseau. Par conséquent, il ne pourra intervenir qu'après que celle-ci ait eu lieu (dans le cadre de l'analyse de cette dernière).

Pour l'abonné, qui est victime d'une fraude ou d'une utilisation malveillante du réseau, il n'est pas non plus acceptable qu'il apparaisse que l'opérateur n'a pas conservé de données par rapport à cette fraude ou cette utilisation malveillante, dès lors que l'abonné n'avait pas été repris dans une liste de personnes ciblées.

Un ciblage des données en amont n'est possible que si l'opérateur savait à l'avance qui serait victime (ou auteur) d'une fraude ou d'une utilisation malveillante du réseau ou qu'une certaine atteinte à la sécurité de son réseau aurait lieu à un moment donné. Mais bien entendu, ce n'est pas le cas dans la pratique (les opérateurs ne disposent pas d'une boule de cristal).

En revanche, la suggestion de l'Autorité de protection des données est suivie dans la mesure où des délais de conservation des données différenciés sont prévus dans le cadre de la lutte contre la fraude, l'utilisation malveillante du réseau et dans la cadre de la sécurité du réseau. Un premier délai concerne la conservation préventive et générale de certaines données de trafic. Un deuxième délai, qui concerne les données relatives à un cas particulier de fraude ou d'utilisation malveillante du réseau ou du service, ou d'atteinte à la sécurité du réseau, permet de conserver les données qui s'y rapportent pour une durée plus longue si nécessaire (principe de la conservation ciblée et réactive).

Le paragraphe 4 de l'article 122

Le cadre de l'Union européenne

Le traitement et la conservation des données de trafic pour protéger les intérêts de l'opérateur et de l'utilisateur final contre la fraude et l'utilisation malveillante du réseau entrent dans les limites permises par la directive "vie privée et communications électroniques" (directive 2002/58/CE).

het plegen van het feit dat aanleiding geeft tot de gegevensbewaring en het moment waarop de operator kennis neemt van dat feit. Met andere woorden, het nut van een preventieve bewaring (of van historische gegevens) is dat er kan worden teruggekeerd in het verleden, wat niet mogelijk is met een reactieve bewaring. Zoals hieronder zal worden toegelicht, is de operator meestal niet in staat om het plegen van fraude of het kwaadwillig gebruik van het netwerk op te sporen (en dus te verhinderen). Hij zal dus pas kunnen optreden nadat het feit gepleegd werd (in het kader van de analyse ervan).

Voor de abonnee, die slachtoffer is van fraude of van een kwaadwillig gebruik van het netwerk, is het evenmin aanvaardbaar dat blijkt dat de operator geen gegevens heeft bewaard in verband met deze fraude of dat kwaadwillig gebruik daar de abonnee immers niet was opgenomen in een lijst van doelen.

Zich richten op gegevens stroomopwaarts is pas mogelijk wanneer de operator op voorhand weet wie het slachtoffer (of de dader) van fraude of kwaadwillig gebruik van het netwerk zou zijn of dat er een zekere inbreuk op de veiligheid van zijn netwerk zou plaatsvinden op een gegeven ogenblik. Maar dat is natuurlijk niet zo in de praktijk (de operatoren hebben geen kristallen bol).

De suggestie van de Gegevensbeschermingsautoriteit wordt daarentegen wel gevolgd daar waar wordt voorzien in gedifferentieerde gegevensbewaringstermijnen in het kader van de bestrijding van fraude en kwaadwillig gebruik van het netwerk en in het kader van netwerkveiligheid. Een eerste termijn betreft de preventieve en algemene bewaring van bepaalde verkeersgegevens. Dankzij een tweede termijn, die betrekking heeft op de gegevens in verband met een specifiek geval van fraude of kwaadwillig gebruik van het netwerk of de dienst, of een inbreuk op de netwerkveiligheid, kunnen de gegevens die er betrekking op hebben langer worden bewaard indien nodig (principe van de doelgerichte en reactieve bewaring).

Paragraaf 4 van artikel 122

Het kader van de Europese Unie

De verwerking en de bewaring van verkeersgegevens om de belangen van de operator en de eindgebruiker te vrijwaren van fraude en kwaadwillig gebruik van het netwerk vallen binnen de door de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) toegestane limieten.

En effet, l'article 6, § 5, de la directive "vie privée et communications électroniques" énonce que "Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées […] de détecter les fraudes […]; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.".

En outre, l'article 15, § 1, de la même directive prévoit que les États membres peuvent déroger aux règles prévues par son article 6 lorsque cela constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour la poursuite de l'une des finalités énumérées à cet article 15, § 1.

Parmi ces finalités figurent la sauvegarde de la sécurité nationale, la protection de la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales, au sujet desquelles la Cour de Justice de l'Union européenne (CJUE) s'est prononcée dans le cadre de l'arrêt La Quadrature du Net (aff. jtes. C-511/18, C-512/18 et C-520/18, du 6 octobre 2020).

D'autres finalités, sur lesquelles la CJUE ne s'est pas prononcée à ce stade, sont également permises par l'article 15, § 1 de la directive. Il s'agit, en particulier, de la prévention, la recherche, la détection d'utilisations non autorisées du système de communications électroniques et des motifs d'exception prévus à l'article 13 de la directive 95/46, remplacé par l'article 23, § 1 du RGPD (cf. arrêt de la CJUE du 29 janvier 2008, Promusicae, C-275/06, pt. 53), parmi lesquels figurent les autres objectifs importants d'intérêt public général (art. 23, § 1, e) du RGPD) et la protection de la personne concernée ou des droits et libertés d'autrui (art. 23, § 1, g) du RGPD).

La protection de l'intérêt de l'utilisateur à disposer d'un service de communications électroniques de qualité, exempt de nuisances frauduleuses, entre également dans ce cadre.

Finalement, la lutte contre la fraude et l'utilisation malveillante du réseau figure parmi les objectifs expressément prévus par le projet européen de règlement ePrivacy, voué à remplacer la directive "vie privée et communications électroniques" (directive 2002/58/CE).

Une modernisation de la présente loi, tenant compte de l'importance croissante de cet objectif, est donc souhaitable.

Artikel 6, § 5, van de richtlijn betreffende privacy en elektronische communicatie stelt immers dat "De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor […] opsporing van fraude […], en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.".

Bovendien stelt artikel 15, § 1, van dezelfde richtlijn dat de lidstaten kunnen afwijken van de regels vastgelegd in haar artikel 6 wanneer dat een noodzakelijke, gepaste en evenredige maatregel betreft, binnen een democratische maatschappij, ter nastreving van een van de doeleinden opgelijst in dit artikel 15, § 1.

Deze doeleinden omvatten de vrijwaring van de nationale veiligheid, de bescherming van de openbare veiligheid, de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, waarover het Europees Hof van Justitie (HvJ-EU) zich heeft uitgesproken in het kader van het arrest-*La Quadrature du Net* (gevoegde zaken C-511/18, C-512/18 en C-520/18, van 6 oktober 2020).

Andere doeleinden, waarover het HvJ-EU zich in dit stadium niet heeft uitgesproken, worden eveneens toegestaan door artikel 15, § 1, van de richtlijn. Het gaat met name om de voorkoming, het onderzoek en de opsporing van niet-toegestaan gebruik van het elektronischecommunicatiesysteem en om de uitzonderingsredenen vastgelegd in artikel 13 van Richtlijn 95/46, vervangen door artikel 23, § 1, van de AVG (cf. arrest van het HvJ-EU van 29 januari 2008, Promusicae, C-275/06, pt. 53), waaronder de andere belangrijke doelstellingen van algemeen belang (art. 23, § 1, e) van de AVG) en de bescherming van de betrokken persoon of de rechten en vrijheden van anderen (art. 23, § 1, g) van de AVG).

Ook de bescherming van het belang van de gebruiker om te beschikken over een kwalitatieve elektronischecommunicatiedienst, vrij van frauduleuze hinder, valt binnen dat kader.

Ten slotte behoort de bestrijding van fraude en kwaadwillig gebruik van het netwerk tot de doelstellingen die uitdrukkelijk zijn geformuleerd in het ontwerp van de ePrivacy-verordening, dat bestemd is om de richtlijn betreffende privacy en elektronische communicatie te vervangen (Richtlijn 2002/58/EG).

Het is dus wenselijk om deze wet te updaten, rekening houdend met het toenemende belang van deze doelstelling.

L'obligation pour les opérateurs de conserver et traiter certaines données de trafic

Dans la version actuelle de l'article 122, § 4, les opérateurs disposent de la possibilité de traiter des données de trafic afin de déceler des fraudes éventuelles. Il convient d'obliger les opérateurs à déployer leurs meilleurs efforts pour le faire pour les raisons suivantes.

Une possibilité pour l'opérateur de traiter les données de trafic en matière de fraude implique qu'un opérateur pourrait décider de ne pas le faire (parce que la fraude ne lui cause pas de préjudice financier), ce qui pourrait porter atteinte aux intérêts de l'utilisateur final. Il convient à cet égard de veiller à ce que les opérateurs offrent un service de qualité à leurs abonnés, sans se contenter de simplement permettre une communication électronique.

Cette possibilité implique également que de grandes différences peuvent exister entre opérateurs, certains étant plus actifs que d'autres dans la protection des intérêts des utilisateurs finaux en matière de fraude.

Il convient aussi de prendre en compte la multiplication des fraudes, leur impact pour les utilisateurs finaux et le fait que c'est de plus en plus souvent l'utilisateur final et non plus l'opérateur qui est victime de la fraude.

Bien entendu, dans certains cas, il ne sera pas techniquement possible pour les opérateurs de détecter certaines fraudes ou certaines utilisations malveillantes du réseau ou de contribuer à en établir leur existence avec les seules données de trafic, par exemple si cette opération nécessite de prendre connaissance du contenu des communications (par exemple, le contenu d'un SMS), ce que l'article 122 ne permet pas. En revanche, une dérogation au principe de confidentialité est prévue à l'article 125, 7° lorsque les actes sont accomplis par les opérateurs dans le but exclusif de combattre la fraude commise au moyen de messages utilisant des numéros de téléphone, comme des messages SMS ou MMS, et moyennant le respect des conditions strictes prévues par cet article. Par ailleurs, dans certains cas, l'opérateur peut ne disposer que d'indices de fraude potentielle ou d'utilisation malveillante potentielle du réseau, sans pouvoir acquérir de certitude à cet égard. Dans bien des cas, l'opérateur ne pourra pas détecter la fraude ou l'utilisation malveillante du réseau car aucune anomalie n'est apparente. En ce qui concerne les SMS, les opérateurs peuvent appliquer certains filtres, mais en cas de phishing ils ne peuvent pas empêcher leurs clients de divulguer leurs données au fraudeur afin que ce dernier puisse accéder au profil du client. Dans ce

De verplichting voor de operatoren om bepaalde verkeersgegevens te bewaren en te verwerken

In de huidige versie van artikel 122, § 4, beschikken de operatoren over de mogelijkheid om verkeersgegevens te verwerken om eventuele fraude op te sporen. Het is zaak om de operatoren te verplichten om daartoe maximale inspanningen te leveren om de volgende redenen.

De mogelijkheid voor de operator om de verkeersgegevens te verwerken in het kader van fraude houdt in dat een operator zou kunnen beslissen om dat niet te doen (omdat de fraude hem geen financieel nadeel berokkent), hetgeen de belangen van de eindgebruiker zou kunnen schaden. In dat opzicht dient ervoor te worden gezorgd dat de operatoren een kwalitatieve dienst bieden aan hun abonnees, zonder genoegen te nemen met enkel het mogelijk maken van elektronische communicatie.

Deze mogelijkheid houdt ook in dat er grotere verschillen kunnen bestaan tussen operatoren, aangezien sommigen actiever zijn dan anderen wat betreft de bescherming van de belangen van de eindgebruikers op het stuk van fraude.

Er dient ook rekening te worden gehouden met het toenemende aantal fraudegevallen, de impact daarvan op de eindgebruikers en het feit dat het steeds vaker de eindgebruiker is en niet de operator die het slachtoffer is van de fraude.

In bepaalde gevallen zal het uiteraard technisch niet mogelijk zijn voor de operatoren om bepaalde gevallen van fraude of vormen van kwaadwillig gebruik van het netwerk op te sporen of bij te dragen tot de vaststelling daarvan aan de hand van enkel de verkeersgegevens, bijvoorbeeld wanneer voor deze handeling kennis moet worden genomen van de inhoud van de communicatie (bijvoorbeeld de inhoud van een sms), wat artikel 122 niet toestaat. Er wordt echter voorzien in een afwijking op het vertrouwelijkheidsbeginsel in artikel 125, 7°, wanneer de handelingen worden gesteld door de operatoren met als enige doel de fraude gepleegd door middel van berichten die telefoonnummers gebruiken, zoals sms'en of mms'en, te bestrijden, op voorwaarde dat de strikte voorwaarden die daartoe worden vastgelegd in dit artikel, worden nageleefd. In sommige gevallen kan de operator overigens enkel over aanwijzingen beschikken dat het gaat om mogelijke fraude of mogelijk kwaadwillig gebruik van het netwerk, zonder daar zeker van te zijn. In heel wat gevallen zal de operator de fraude of het kwaadwillig gebruik van het netwerk niet kunnen opsporen omdat er geen anomalie zichtbaar is. Inzake sms'en kunnen operatoren bepaalde filters toepassen, maar ze kunnen niet beletten dat klanten in geval van *phishing* hun gegevens vrijgeven aan de fraudeur zodat

cas, l'opérateur ne peut qu'effectuer une réinitialisation du mot de passe pour bloquer le fraudeur. Un opérateur peut prendre des mesures si une vulnérabilité du réseau est utilisée par le fraudeur.

Cependant, il est essentiel que les opérateurs développent les outils et l'expertise nécessaire en matière de détection de fraude, qu'ils analysent les fraudes et comprennent leur origine et qu'ils prennent les actions adéquates sur la base de cette analyse, dans les limites permises par la loi.

Le traitement et la conservation des données de trafic pour protéger les intérêts de l'opérateur et de l'utilisateur final contre la fraude et l'utilisation malveillante du réseau entrent dans les limites permises par la directive "vie privée et communications électroniques" (directive 2002/58/CE).

Les données nécessaires

D'autres données que les données de facturation peuvent être nécessaires pour détecter ou analyser la fraude ou l'utilisation malveillante du réseau, par exemple les données de localisation de l'appelant et les données liées aux communications entrantes, telles que les SMS et appels entrants.

La facturation ne permet pas, par exemple, de mettre en évidence un SMS entrant, qui constitue un smishing, et le gain obtenu par le fraudeur ne se reflètera pas nécessairement dans un appel sortant.

La facturation ne permet généralement pas de contribuer à établir le harcèlement par téléphone (les appels entrants ne sont pas facturés).

La facturation ne permet pas non plus de retracer la localisation de l'équipement terminal employé pour réaliser une fraude, alors que cette localisation peut être pertinente pour détecter la fraude (différentes localisations peuvent par exemple s'avérer être incohérentes ou suspectes) et pour l'analyser. Une association d'opérateurs a indiqué que les données de localisation ne sont pas utilisées par tous les opérateurs pour combattre la fraude. La volonté du législateur est de tirer vers le haut le niveau de protection des clients des opérateurs. Par ailleurs, lorsqu'un abonné victime d'une fraude commise à l'aide d'un service de communications électroniques dépose plainte auprès de la police, il s'attend à ce que cette dernière puisse localiser l'origine de cette fraude.

deze toegang krijgt tot het profiel van de klant. In dit geval kan de operator enkel een paswoord-reset uitvoeren om de fraudeur te blokkeren. Een operator kan maatregelen nemen indien een kwetsbaarheid in het netwerk gebruikt wordt door de fraudeur.

Toch is het van essentieel belang dat de operatoren de nodige tools en expertise inzake de opsporing van fraude ontwikkelen, dat ze de fraudegevallen analyseren en de herkomst ervan begrijpen en dat ze de passende acties ondernemen op basis van deze analyse, binnen de grenzen van de wet.

De verwerking en de bewaring van verkeersgegevens om de belangen van de operator en de eindgebruiker te vrijwaren van fraude en kwaadwillig gebruik van het netwerk vallen binnen de door de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) toegestane limieten.

De nodige gegevens

Er kunnen ook andere gegevens dan de factureringsgegevens nodig zijn om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, bijvoorbeeld de locatiegegevens van de beller en de gegevens in verband met de binnenkomende communicatie, zoals sms'en en inkomende oproepen.

De facturering maakt het bijvoorbeeld niet mogelijk om een binnenkomende sms die smishing vormt als dusdanig te identificeren en de winst die de fraudeur behaalt, zal niet noodzakelijk weerspiegeld worden in een uitgaande oproep.

Het is doorgaans niet mogelijk om aan de hand van de facturering bij te dragen tot de vaststelling van pesterijen via de telefoon (binnenkomende oproepen worden niet gefactureerd).

De facturering maakt het evenmin mogelijk om de locatie te achterhalen van de eindapparatuur gebruikt om de fraude te plegen, terwijl deze plaatsbepaling relevant kan zijn om de fraude op te sporen (verschillende locaties kunnen bijvoorbeeld incoherent of verdacht blijken) en te analyseren. Een operatorenvereniging heeft aangegeven dat de locatiegegevens niet door alle operatoren worden gebruikt om fraude te bestrijden. Het is de wens van de wetgever om het niveau van bescherming van de klanten van de operatoren op te trekken. Wanneer een abonnee die slachtoffer is van fraude gepleegd door middel van een elektronische-communicatiedienst overigens een klacht indient bij de politie, verwacht deze dat de politie de bron ervan kan bepalen.

Il est clair que les données nécessaires pour détecter et analyser la fraude et l'utilisation malveillante des réseaux et services peuvent varier en fonction des mesures prises par les opérateurs et des moyens mis en œuvre par ceux-ci pour atteindre cet objectif.

Cependant, dès lors que l'article 121/8 en projet prévoit désormais l'obligation pour tous les opérateurs de prendre les mesures appropriées de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés, la conservation de certaines données apparait comme manifestement nécessaire. Il s'agit, en particulier, des données reprises dans le "Call detail record" (en abrégé "CDR") ou dans un registre fonctionnellement équivalent.

Le *Call detail record* ("CDR") correspond au registre des détails d'appel, qui reprend les informations conservées par l'opérateur pour chaque appel téléphonique. Cette notion se réfère au standard international visé notamment au point 5 de la norme ETSI TS 122 115 V3.2.0 (2000-01). Figurent parmi ces informations, l'identification de l'appelant, l'identification de l'appelé, la date et l'heure de l'appel, la durée de l'appel, et certains autres paramètres liés à l'appel, tels que les fonctions utilisées et la raison de la fin de l'appel. Les CDR sont collectés régulièrement pour être transformés en rapports d'utilisation, de capacité, de performance et de diagnostic. Grâce à ces informations, il est plus facile de repérer les exceptions aux schémas d'appels réguliers, comme les appels en dehors des heures de travail, les appels internationaux, les écarts importants par rapport aux périodes de rapport précédentes et les destinations des appels qui ne reflètent pas les schémas d'appels normaux et permettent dès lors de détecter les anomalies et fraudes potentielles.

Le "*Call detail record*" ("CDR") étant utilisé pour les services de téléphonie, elle ne permet pas de couvrir l'ensemble des services de communications électroniques visés par les obligations prévues à l'article 122, § 4. Pour les services pour lesquels l'opérateur ne fait pas usage d'un "*Call detail record*", il convient alors de prendre en compte tout registre fonctionnellement équivalent, ou en d'autres termes, qui remplit les mêmes fonctions que le "CDR" (rappelées à l'alinéa précédent) pour ces autres services.

À la suite de l'avis de l'Autorité de protection des données, le paragraphe 4 de l'article 122 prévoit dorénavant une obligation de conservation des données de localisation de l'auteur de la communication (l'auteur

Natuurlijk kunnen de gegevens die nodig zijn om de fraude en het kwaadwillig gebruik van de netwerken en diensten op te sporen en te analyseren, verschillen naargelang van maatregelen getroffen door de operatoren en de middelen die zij inzetten om dat doel te verwezenlijken.

Daar ontwerpartikel 121/8 voortaan reeds voorziet in de verplichting voor alle operatoren om de gepaste maatregelen te nemen om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en te vermijden dat de eindgebruikers nadeel ondervinden of lastiggevallen worden, lijkt het overduidelijk dat bepaalde gegevens dienen te worden bewaard. Het gaat meer in het bijzonder over de gegevens opgenomen in de "Call detail record" (afgekort "CDR") of in een functioneel gelijkwaardig register.

De *Call detail record* ("CDR") stemt overeen met het register van de oproepdetails die de door de operator bewaarde informatie voor elke telefonische oproep vermeldt. Dat begrip verwijst naar de internationale standaard die met name in punt 5 van de ETSI-norm TS 122 115 V3.2.0 (2000-01) wordt beoogd. Tot die informatie behoren de identificatie van de oproeper, de identificatie van de opgeroepene, de datum en het tijdstip van de oproep, de duur van de oproep, en bepaalde andere parameters in verband met de oproep, zoals de gebruikte functies en de reden van de beëindiging van de oproep. De CDR worden geregeld opgevraagd om omgezet te worden in verslagen over gebruik, capaciteit, prestatie en diagnostiek. Dankzij deze informatie is het gemakkelijker om de uitzonderingen op de schema's van regelmatige oproepen te lokaliseren, zoals de oproepen buiten de werkuren, de internationale oproepen, de grote verschillen ten opzichte van de vorige verslagperiodes en de bestemmingen van de oproepen die geen normale oproepschema's voorstellen en het dan ook mogelijk maken om de anomalieën en mogelijke fraude op te sporen.

Aangezien de "*Call detail record*" ("CDR") gebruikt wordt voor de telefoniediensten, kunnen niet alle elektronische-communicatiediensten beoogd door de verplichtingen vastgelegd in artikel 122, § 4, gedekt worden. Voor de diensten waarvoor de operator geen gebruik maakt van een "Call detail record", dient elk functioneel gelijkwaardig register in aanmerking te worden genomen, of met andere woorden, elk register dat dezelfde functies vervult als de "CDR" (herhaald in het vorige lid) voor deze andere diensten.

Naar aanleiding van het advies van de Gegevensbeschermingsautoriteit, voorziet artikel 122, paragraaf 4, voortaan in een verplichting om de locatiegegevens van de persoon die de communicatie doet (de dader van de

de la fraude ou de l'utilisation malveillante du réseau) et pas du destinataire de la communication (la victime de cette fraude ou de cette utilisation malveillante). La localisation du destinataire de la communication sera cependant conservée si cela est utile pour détecter ou analyser la fraude ou l'utilisation malveillante du réseau.

Conformément à la demande de l'Autorité de protection des données, les données de trafic qui doivent être conservées par les opérateurs pour les finalités visées à l'article 122, § 4, sont ainsi précisées, de manière à ce que l'obligation légale soit suffisamment claire et précise.

Outre les données dont la conservation est rendue obligatoire en vertu de l'article 122, § 4, la possibilité est également laissée aux opérateurs de conserver d'autres données qui peuvent s'avérer nécessaires pour ce qui les concerne, au regard notamment des mesures appropriées qu'ils prennent sur le pied de l'article 121/8, ainsi que des moyens qu'ils y consacrent.

La durée de conservation

Il convient d'éviter que les opérateurs décident de conserver les données de trafic pendant un laps de temps trop court que pour pouvoir efficacement lutter contre les fraudes ou que les pratiques des différents opérateurs divergent fortement. Dès lors, l'article 122 prévoit dorénavant une durée de conservation de données. Dans bien des cas, l'opérateur ne pourra pas détecter la fraude ou l'utilisation malveillante du réseau lorsque la communication a eu lieu. Cependant, il est possible qu'il en soit informé ultérieurement (par exemple en cas de plainte de l'abonné auprès de l'opérateur). L'opérateur doit encore disposer de suffisamment de données de trafic (en ce compris des données de localisation) pour l'ensemble de ses abonnés pour pouvoir analyser la communication à l'origine de la fraude ou de l'utilisation malveillante du réseau.

Le délai de quatre mois à partir de la communication a été retenu pour l'application de l'alinéa 3, étant donné que la fraude peut avoir un impact sur la facturation de l'opérateur envers l'abonné (ou d'une entreprise envers l'abonné).

Le délai de quatre mois de conservation tient compte d'un cycle complet de facturation (premier mois suivant la consommation du service), d'une durée de contestation minimale (de 15 jours à 1 mois, le deuxième mois suivant la consommation du service), d'une période de traitement de la contestation permettant un échange entre l'abonné et l'opérateur (le troisième mois suivant la contestation du service) et d'une période de retard

fraude of van het kwaadwillig gebruik van het netwerk) te bewaren en niet van de geadresseerde van de communicatie (het slachtoffer van deze fraude of van dit kwaadwillig gebruik). De locatie van de geadresseerde van de communicatie zal evenwel bewaard worden indien dat nuttig blijkt om de fraude of het kwaadwillig gebruik van het netwerk op te sporen of te analyseren.

Conform het verzoek van de Gegevensbeschermingsautoriteit, worden de door de operatoren te bewaren verkeersgegevens voor de doeleinden beoogd in artikel 122, § 4, aldus gepreciseerd dat de wettelijke verplichting voldoende duidelijk en nauwkeurig is.

Buiten de gegevens die verplicht moeten bewaard worden krachtens artikel 122, § 4, wordt ook de mogelijkheid gelaten aan de operatoren om andere gegevens te bewaren die nodig kunnen blijken wat hen betreft, met name in het licht van de gepaste maatregelen die ze treffen in uitvoering van artikel 121/8, alsook van de middelen die ze daaraan wijden.

Bewaringstermijn

Er moet worden vermeden dat de operatoren beslissen om de verkeersgegevens te bewaren voor een periode die te kort is om fraude efficiënt te kunnen bestrijden of dat de praktijken van de verschillende operatoren sterk uiteenlopen. Vandaar dat artikel 122 voortaan in een duur voor gegevensbewaring voorziet. In heel wat gevallen zal de operator de fraude of het kwaadwillig gebruik van het netwerk niet kunnen opsporen wanneer de communicatie heeft plaatsgevonden. Het is evenwel mogelijk dat hij daar later van op de hoogte wordt gebracht (bijvoorbeeld in geval van een klacht van de abonnee bij de operator). De operator moet nog over voldoende verkeersgegevens beschikken (waaronder locatiegegevens) voor al zijn abonnees om de communicatie te kunnen analyseren die aan de oorsprong ligt van de fraude of het kwaadwillig gebruik van het netwerk.

De termijn van vier maanden vanaf de communicatie is in aanmerking genomen voor de toepassing van het derde lid, aangezien de fraude een impact kan hebben op de facturering van de operator tegenover de abonnee (of van een onderneming tegenover de abonnee).

De termijn van vier maanden bewaring houdt rekening met een volledige factureringscyclus (eerste maand volgend op het verbruik van de dienst), met een minimale duur voor betwisting (van 15 dagen tot 1 maand, de tweede maand volgend op het verbruik van de dienst), met een periode voor de behandeling van de betwisting die een uitwisseling tussen de abonnee en de operator mogelijk maakt (de derde maand volgend op de betwisting

possible dans ce traitement (le quatrième mois suivant la consommation).

Le délai de 4 mois permettra aussi de prendre en compte les évolutions en matière de fraude.

Pour détecter et analyser une fraude ou une utilisation malveillante du réseau, les opérateurs sont amenés à traiter les données de trafic en temps réel et les données de trafic conservées sur la base du paragraphe 2 (les données de trafic conservées dans le but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion) et du présent paragraphe.

Lorsque l'opérateur a détecté une fraude potentielle ou avérée envers son abonné, il lui revient de prendre les mesures les plus appropriées pour protéger son abonné. Une de ces mesures peut être l'information de ce dernier, par exemple l'information que l'appel pourrait être frauduleux.

Par ailleurs, les opérateurs doivent pouvoir contribuer à établir une utilisation malveillante du réseau (par exemple en confirmant qu'une certaine communication entrante a bien eu lieu dans le cadre d'une plainte pour harcèlement par téléphone).

En pratique, en cas de harcèlement par téléphone, la victime doit s'adresser au service de médiation pour les télécommunications.

Ce dernier, qui a pour mission l'aide aux victimes et n'est pas rattaché à un service de police, pourra alors obtenir via les opérateurs concernés les nom, prénom et adresse de l'auteur du harcèlement par téléphone et pourra fournir ces données à la victime de ce harcèlement (voir article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques). En pratique, un délai de conservation des données inférieur à 12 mois serait problématique, au vu des différentes étapes susmentionnés à suivre. Il convient également de souligner que le harcèlement par téléphone n'aura pas d'impact sur la facturation de l'opérateur à l'abonné, étant donné qu'il s'agit de communications entrantes.

En réponse à une préoccupation exprimée par le Conseil d'État dans son avis n° 69.381/4 du 28 juin 2021 relatif au présent avant-projet de loi, il est précisé qu'il n'appartient pas à l'opérateur mais aux autorités compétentes en la matière, comme le service de médiation, d'établir la réalité d'une utilisation malveillante du réseau. Dans

van de dienst) en met een periode van mogelijke vertraging in die behandeling (de vierde maand volgend op het verbruik).

De termijn van 4 maanden zal het ook mogelijk maken om rekening te houden met de ontwikkelingen op het stuk van fraude.

Om fraude of kwaadwillig gebruik van het netwerk op te sporen en te analyseren, dienen de operatoren de verkeersgegevens in real time te verwerken alsook de gegevens bewaard krachtens paragraaf 2 (de verkeersgegevens bewaard voor doeleinden van facturering van de abonnees of om de interconnectiebetalingen uit te voeren) en krachtens deze paragraaf.

Wanneer de operator een mogelijk of bewezen geval van fraude heeft opgespoord jegens zijn abonnee, dient hij de meest gepaste maatregelen te nemen om zijn abonnee te beschermen. Een van die maatregelen kan bestaan in het informeren van deze laatste, bijvoorbeeld hem melden dat de oproep frauduleus kan zijn.

Verder moeten de operatoren kunnen bijdragen tot het vaststellen van kwaadwillig gebruik van het netwerk (bijvoorbeeld door te bevestigen dat er wel degelijk een zekere communicatie is binnengekomen in het kader van een klacht in verband met telefonische pesterijen).

In geval van telefonische pesterijen moet het slachtoffer zich in de praktijk richten tot de Ombudsdienst voor telecommunicatie.

Deze laatste, die als opdracht heeft hulp te verlenen aan de slachtoffers en die niet onder een politiedienst valt, zal dan via de betrokken operatoren de naam, voornaam en het adres van de dader van de telefonische pesterijen kunnen krijgen en zal deze gegevens kunnen verstrekken aan het slachtoffer van die pesterijen (zie artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven). In de praktijk zou een termijn van gegevensbewaring van minder dan 12 maanden problematisch zijn gezien de verschillende voormelde stappen die moeten worden gevolgd. Er dient ook te worden benadrukt dat de telefonische pesterijen geen impact zullen hebben op de facturering van de operator aan de abonnee, aangezien het om binnenkomende communicatie gaat.

In antwoord op een bekommernis die de Raad van State heeft geuit in zijn advies nr. 69.381/4 van 28 juni 2021 met betrekking tot dit voorontwerp van wet, wordt gepreciseerd dat het niet aan de operator is maar aan de ter zake bevoegde autoriteiten, zoals de ombudsdienst, om het bestaan van kwaadwillig gebruik van het netwerk

cette perspective, l'alinéa 4 de l'article 122, § 4 en projet précise désormais qu'en cas de fraude présumée ou d'utilisation malveillante présumée, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec la fraude présumée ou l'utilisation malveillante présumée.

L'arrêté royal

La délégation au Roi introduite dans le paragraphe 4 permet de préciser et d'étendre, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de l'Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire en matière de lutte contre la fraude ou l'utilisation malveillante du réseau.

L'adoption de cet arrêté royal n'est pas obligatoire, au vu des défis suivants. D'abord, les fraudes évoluent significativement avec le temps. Certains types de fraude peuvent disparaître ou diminuer en importance alors que de nouveaux types de fraude peuvent voir le jour. Ensuite, les données que les opérateurs conservent pour lutter contre les fraudes peuvent être différentes selon le type de service de communications électroniques fourni, la taille de l'opérateur et les outils "anti-fraude" dont il dispose ou le type d'utilisateurs du service.

De plus, les actions que l'opérateur prend lorsqu'il détecte une fraude potentielle ou avérée peuvent être diverses en fonction du type de fraude et du degré de certitude que l'opérateur a par rapport au fait qu'il s'agit bien d'une fraude (seulement des indices ou une certitude à cet égard).

La pratique devra donc être évaluée pour déterminer si un tel arrêté royal est nécessaire.

La communication des données aux autorités

Pour que les autorités compétentes (les autorités judiciaires, les services de police, les officiers de police judiciaire de l'IBPT, etc.) puissent investiguer sur une fraude ou une utilisation malveillante d'un réseau et retrouver l'auteur de cette fraude ou de cette utilisation malveillante, il est nécessaire qu'elles reçoivent de l'opérateur toutes les données légalement conservées y afférentes.

Le mot "présumé" est ajouté puisque les autorités doivent d'abord avoir connaissance de l'infraction

aan te tonen. In dat licht preciseert het vierde lid van ontwerpartikel 122, § 4, voortaan dat in geval van vermoede fraude of van vermoed kwaadwillig gebruik, de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermoede fraude of het vermoede kwaadwillig gebruik kunnen doorsturen.

Het koninklijk besluit

Aan de hand van de delegatie aan de Koning ingevoerd in paragraaf 4, kunnen, bij besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor de bestrijding van fraude of kwaadwillig gebruik van het netwerk, worden gepreciseerd en uitgebreid.

De aanneming van dit koninklijk besluit is niet verplicht in het licht van de volgende uitdagingen. Ten eerste evolueert fraude aanzienlijk mettertijd. Bepaalde vormen van fraude kunnen verdwijnen of minder belangrijk worden terwijl nieuwe soorten van fraude kunnen opduiken. Vervolgens kunnen de gegevens die de operatoren bewaren om fraude tegen te gaan, verschillen afhankelijk van het type van de verstrekte elektronischecommunicatiedienst, de omvang van de operator en de "antifraudetools" waarover hij beschikt of het soort van gebruikers van de dienst.

Bovendien kunnen de acties die de operator onderneemt wanneer hij een mogelijk of bewezen geval van fraude heeft opgespoord, variëren naargelang van het type van fraude en van de graad van zekerheid die de operator heeft ten opzichte van het feit dat het wel degelijk om fraude gaat (enkel aanwijzingen of een zekerheid wat dat betreft).

De praktijk zal dus moeten worden geëvalueerd om vast te stellen of een dergelijk koninklijk besluit noodzakelijk is.

Het bezorgen van de gegevens aan de autoriteiten

Opdat de bevoegde autoriteiten (de gerechtelijke autoriteiten, de politiediensten, de officiers van gerechtelijke politie van het BIPT, enz. een geval van fraude of een kwaadwillig gebruik van een netwerk kunnen onderzoeken, en de pleger van deze fraude of dit kwaadwillig gebruik kunnen terugvinden, moeten zij vanwege de operator alle wettelijk bewaarde gegevens ontvangen.

Het woord "vermoed" wordt toegevoegd aangezien de autoriteiten eerst kennis moeten hebben van de potentiële

potentielle avant de pouvoir mener leur enquête visant à établir l'existence d'un délit.

Le paragraphe 4/1 de l'article 122

Introduction

Le paragraphe 4/1 est introduit vu que les données de trafic peuvent contribuer à la sécurité des réseaux, qu'il est essentiel d'assurer. La sécurité des réseaux, qui se rattache à la sécurité publique, est essentielle pour la société dans son ensemble. Un incident au niveau du réseau d'un opérateur peut avoir des conséquences très dommageables sur de nombreux plans (vol ou perte de données, impact sur tous les services qui sont offerts à l'aide du réseau). L'importance de la sécurité des réseaux va croître dans le futur avec le développement de la 5G, dont seront dépendants de nombreux services et applications.

À l'occasion de la consultation publique, certains opérateurs se sont interrogés quant à la nécessité d'une telle disposition, alors que l'article 114, § 1er, de la même loi prévoit déjà l'obligation de prendre les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée. Bien que l'article 114 vise en effet le même objectif de protection de sécurité des réseaux et services, l'article 122, § 4/1, proposé précise l'un des moyens pour atteindre cet objectif, que constitue la conservation et le traitement de certaines données de trafic.

L'article 2, 21), de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen définit la sécurité des réseaux et des services comme suit: "la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services".

Cadre de l'Union européenne

À nouveau, cette finalité figure parmi les motifs de traitement admissibles au regard de la directive "vie privée et communications électroniques" (directive 2002/58/CE). En effet, le considérant 29 de la directive "vie privée et communications électroniques" (directive 2002/58/CE) prévoit que: "Au besoin, et au cas par cas, le fournisseur d'un service peut traiter des données relatives au trafic

inbreuk, voordat ze hun onderzoek kunnen voeren om het bestaan van een wanbedrijf vast te stellen.

Paragraaf 4/1 van artikel 122

Inleiding

Paragraaf 4/1 wordt ingevoerd, aangezien de verkeersgegevens kunnen bijdragen tot de veiligheid van de netwerken, waarvan het van fundamenteel belang is dat die gewaarborgd is. Netwerkveiligheidi, wat onder staatsveiligheid valt, is essentieel voor de maatschappij in haar geheel. Een incident op het netwerk van een operator kan erg schadelijke gevolgen hebben op tal van niveaus (diefstal of verlies van gegevens, impact op de diensten die worden aangeboden via het netwerk). Het belang van netwerkveiligheid zal toenemen in de toekomst met de ontwikkeling van 5G, waarvan tal van diensten en applicaties zullen afhangen.

Ter gelegenheid van de openbare raadpleging hebben bepaalde operatoren zich vragen gesteld bij de noodzaak van een dergelijke bepaling, aangezien artikel 114, § 1, van dezelfde wet reeds voorziet in de verplichting om maatregelen van technische en organisatorische aard te treffen om het risico inzake veiligheid van de netwerken en diensten op gepaste wijze te beheersen. Hoewel artikel 114 inderdaad hetzelfde doel van vrijwaring van de veiligheid van de netwerken en diensten beoogt, preciseert het voorgestelde artikel 122, § 4/1, een van de middelen om dat doel van bewaring en verwerking van bepaalde verkeersgegevens te verwezenlijken.

Artikel 2, 21), van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie definieert de beveiliging van netwerken en diensten als volgt: "het vermogen van elektronische-communicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van die netwerken en diensten, van de opgeslagen, verzonden of verwerkte gegevens of van de daaraan gerelateerde diensten die via die elektronische-communicatienetwerken en -diensten worden aangeboden, in gevaar brengen".

Het kader van de Europese Unie

Ook dit doeleinde is opgenomen in de toegestane redenen voor verwerking in het licht van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG). Considerans 29 van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG) bepaalt het volgende: "De dienstenaanbieder mag zo nodig in individuele gevallen verkeersgegevens met

qui concernent des abonnés ou des utilisateurs s'il s'agit de déceler une défaillance technique ou une erreur dans la transmission des communications.".

En outre, la sécurité des réseaux figure également parmi les dérogations nationales permises en vertu de l'article 15, § 1, de la même directive (cf. arrêt de la CJUE du 29 janvier 2008, Promusicae, C-275/06, pt. 52).

Pour le surplus, cette finalité est également reprise expressément parmi les motifs permettant le traitement de données de trafic par les opérateurs à l'article 6, § 1 du projet de règlement ePrivacy (voué à remplacer la directive précitée).

De même qu'indiqué précédemment pour ce qui concerne la lutte contre la fraude et l'utilisation malveillante du réseau, de manière à moderniser la présente loi et à tenir compte de l'importance croissante de l'objectif de protection de la sécurité et du bon fonctionnement des réseaux et services de communications électroniques des opérateurs, il est souhaitable d'inclure expressément cet objectif comme finalité justifiant la conservation et le traitement de données de trafic.

L'obligation de conserver et traiter des données de trafic en vue de la sécurité du réseau

L'analyse d'une attaque (potentielle) envers le réseau n'est pas possible sans données de trafic.

Il n'est pas toujours possible pour l'opérateur de retrouver l'attaquant, de pouvoir l'identifier et de localiser l'origine de l'attaque sur la base des données de trafic, étant donné que certaines attaques peuvent être très sophistiquées.

Le projet de paragraphe 4/1 soumis à l'avis de l'Autorité de protection des données obligeait les opérateurs à conserver et exploiter les données de trafic lorsque nécessaire pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques.

Au point 79 de son avis, l'Autorité de protection des données a cependant indiqué que "la raison pour laquelle il est nécessaire de passer d'une possibilité à une obligation n'apparait pas suffisamment développée et étayée dans l'Exposé des motifs.". Suite à cet avis, la possibilité de conserver les données nécessaires a été restaurée à l'article 122, § 4/1, à la place de l'obligation initialement proposée pour les motifs suivants.

betrekking tot abonnees en gebruikers verwerken om technische defecten of fouten in de transmissie van communicatie op te sporen.".

Bovendien behoort ook de beveiliging van de netwerken tot de toegestane nationale afwijkingen krachtens artikel 15, § 1, van dezelfde richtlijn (cf. arrest van het HvJ-EU van 29 januari 2008, Promusicae, C-275/06, pt. 52).

Wat het overige betreft, is dit doeleinde eveneens uitdrukkelijk opgenomen in de redenen die de operatoren toestaan om verkeersgegevens te verwerken in artikel 6, § 1, van het ontwerp van ePrivacy-verordening (die de voormelde richtlijn zal vervangen).

Zoals eerder aangegeven op het stuk van bestrijding van fraude en kwaadwillig gebruik van het netwerk, is het wenselijk, teneinde deze wet te updaten en rekening te houden met het toenemende belang van het doel bestaande in de vrijwaring van de veiligheid en de goede werking van de elektronische-communicatienetwerken en -diensten van de operatoren, om dit doel uitdrukkelijk op te nemen als reden voor de bewaring en verwerking van verkeersgegevens.

De verplichting om verkeersgegevens te bewaren en om te verwerken met het oog op netwerkveiligheid

Een (potentiële) aanslag op het netwerk analyseren, is niet mogelijk zonder verkeersgegevens.

Het is voor een operator niet altijd mogelijk om de aanvaller te vinden, om deze te identificeren en de herkomst van de aanval te lokaliseren aan de hand van verkeersgegevens aangezien bepaalde aanvallen erg gesofisticeerd kunnen zijn.

Ontwerpparagraaf 4/1, die ter advies is voorgelegd aan de Gegevensbeschermingsautoriteit, verplichtte de operatoren om verkeersgegevens te bewaren en te benutten wanneer dat nodig is om de veiligheid en correcte werking van hun netwerken en diensten voor elektronische communicatie te garanderen.

In punt 79 van haar advies heeft de Gegevensbeschermingsautoriteit echter aangegeven: "De reden waarom een mogelijkheid werd omgezet in een verplichting is echter niet voldoende toegelicht en gestaafd in de memorie van toelichting". Naar aanleiding van dat advies werd de mogelijkheid om de noodzakelijke gegevens te bewaren, hersteld in artikel 122, § 4/1, in de plaats van de initieel voorgestelde verplichting om de volgende redenen.

D'abord, comme indiqué précédemment concernant le nouvel article 121/8 en projet, les opérateurs sont d'ores et déjà soumis à des obligations de prendre les mesures en vertu des articles 114 et 114/1 de la loi télécom.

En outre, les atteintes à la sécurité des réseaux portent directement préjudice à l'opérateur, de sorte que celui-ci est davantage incité à prendre les mesures nécessaires pour s'en prémunir. La nécessité de mettre à leur charge une obligation complémentaire de conservation des données nécessaires apparait donc, en l'état actuel, moins cruciale.

Par ailleurs, il s'avère particulièrement difficile d'établir une liste fixe et précise de données nécessaires aux fins de veiller à la sécurité des réseaux. Un grand nombre de données de trafic peuvent s'avérer nécessaires pour ce faire et celles-ci varient en fonction des spécificités de chaque type d'opérateur (OTT, opérateur télécom classique), du service concerné, mais aussi du type d'atteinte à la sécurité du réseau. Or, les atteintes à la sécurité des réseaux sont particulièrement et de plus en plus diversifiées.

Les opérateurs peuvent par exemple exploiter des données de trafic en temps réel ou des données de trafic conservées pour rechercher les attaques sur le réseau ou pour investiguer sur une attaque (potentielle) sur le réseau.

Cette disposition n'oblige pas les opérateurs à exploiter l'ensemble des données de trafic par défaut, mais leur réserve la possibilité de déterminer par eux-mêmes les données nécessaires pour ce faire.

Enfin, la pratique montre qu'une attaque envers le réseau d'un opérateur peut être hautement sophistiquée et qu'il est possible que l'opérateur ne détecte une intrusion dans son réseau qu'après un certain laps de temps. Dès lors, il est nécessaire que l'opérateur puisse remonter suffisamment loin dans le passé, une intrusion dans le réseau pouvant mener à une perte ou à un vol de données. Pour pouvoir remonter dans le passé, il est nécessaire que des données de trafic aient été conservées. La durée de 12 mois a donc été retenue comme durée de conservation maximale, sauf cas spécifique à investiguer.

Le paragraphe 4/2 de l'article 122

Un opérateur doit pouvoir conserver des données de trafic pour répondre à ses obligations légales, comme par exemple la législation comptable ou fiscale ou pour répondre à une injonction d'une autorité de geler les données (également connu comme le "*quick freeze*"), qui se

Zoals eerder aangegeven inzake het nieuwe ontwerpartikel 121/8, zijn de operatoren in de eerste plaats onderworpen aan verplichtingen om maatregelen te treffen krachtens de artikelen 114 en 114/1 van de telecomwet.

Bovendien berokken de inbreuken op de netwerkveiligheid rechtstreeks schade aan de operator waardoor deze meer wordt aangespoord om de nodige maatregelen te treffen om zich er tegen te beveiligen. De noodzaak om hen een bijkomende verplichting van bewaring van de noodzakelijke gegevens op te leggen, lijkt in de huidige omstandigheden dus minder cruciaal.

Het lijkt overigens bijzonder moeilijk om een vaste en precieze lijst op te stellen van de gegevens die noodzakelijk zijn voor de doeleinden van vrijwaring van de netwerkveiligheid. Om dat te bewerkstelligen kan een groot volume verkeersgegevens noodzakelijk blijken, die variëren naargelang van de specificiteiten van elk type van operator (OTT, klassieke telecomoperator), van de betreffende dienst, maar ook van het soort van inbreuk op de netwerkveiligheid. Bovendien zijn de inbreuken op de netwerkveiligheid bijzonder en steeds meer gediversifieerd.

De operatoren mogen bijvoorbeeld verkeersgegevens in real time of bewaarde verkeersgegevens benutten om de aanvallen op het netwerk te zoeken of om een (mogelijke) aanval op het netwerk te onderzoeken.

Deze bepaling verplicht de operatoren niet om automatisch alle verkeersgegevens te benutten, maar laat hen de mogelijkheid om zelf de daartoe noodzakelijke gegevens te bepalen.

Ten slotte leert de praktijk ons dat een aanval op het netwerk van een operator heel ingewikkeld kan zijn en dat het mogelijk is dat de operator een indringing in zijn netwerk pas na verloop van enige tijd ontdekt. Vandaar dat het nodig is dat de operator voldoende kan terugkeren in de tijd, omdat een indringing in het netwerk kan leiden tot een verlies of een diefstal van gegevens. Om te kunnen terugkeren in het verleden, is het nodig dat de verkeersgegevens werden bewaard. Als maximale bewaringstermijn werd dus gekozen voor 12 maanden, behalve in specifiek te onderzoeken gevallen.

Paragraaf 4/2 van artikel 122

Een operator moet verkeersgegevens kunnen bewaren om te voldoen aan zijn wettelijke verplichtingen, bijvoorbeeld de boekhoudkundige of fiscale wetgeving of om te voldoen aan een bevel vanwege een autoriteit om de gegevens te bevriezen (ook bekend onder de

trouve par exemple dans le Code d'instruction criminelle. Ces obligations légales ne ressortent pas du présent paragraphe mais bien des législations spécifiques qui les prévoient. Cette disposition permet également de tenir compte des évolutions futures (nouvelles obligations).

Conformément à l'article 15, § 1 de la directive "vie privée et communications électroniques" (directive 2002/58/CE), toute obligation légale de conservation de données de trafic doit être nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour atteindre la finalité poursuivie, et adoptée dans le respect des principes généraux du droit européen, en ce compris ceux visés par la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'homme.

Comme l'Autorité de protection des données l'indique dans son avis, les obligations dont il est question au paragraphe 4/2 doivent être imposées par une loi au sens formel du terme. La disposition a donc été adaptée de la manière demandée.

Le paragraphe 5 de l'article 122

Les modifications au paragraphe 5 sont nécessaires pour tenir compte des nouveaux paragraphes 4/1 et 4/2 de l'article 122. Par ailleurs, la Cellule de coordination de l'opérateur est chargée de fournir à une autorité les données de trafic qu'elle demande.

Le paragraphe 6 de l'article 122

Le service de médiation pour les télécommunications a été ajouté aux autorités qui peuvent être informées des données de trafic et de facture pertinentes en vue du règlement de litiges.

Cet ajout clarifie la possibilité pour l'opérateur de transmettre des données de trafic au service de médiation pour les télécommunications lorsqu'une plainte à son encontre est introduite auprès de ce service.

La présente disposition ne confère cependant pas de compétences nouvelles au service de médiation pour les télécommunications.

Art. 6 (modifications à l'article 123)

L'article 123 renvoie dorénavant aux "données de localisation autres que les données relatives au trafic" pour mieux refléter l'intitulé de l'article 9 de la

naam "*quick freeze*"), wat bijvoorbeeld vervat is in het Wetboek van Strafvordering. Deze wettelijke verplichtingen vloeien niet voort uit deze paragraaf maar wel degelijk uit specifieke wetgevingen die daarin voorzien. Deze bepaling maakt het ook mogelijk om rekening te houden met de toekomstige ontwikkelingen (nieuwe verplichtingen).

Conform artikel 15, § 1, van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG), moet elke wettelijke verplichting tot bewaring van verkeersgegevens in een democratische samenleving noodzakelijk, redelijk en proportioneel zijn om het streefdoel te bereiken, en aangenomen worden met naleving van de algemene beginselen van het Europees recht, waaronder diegene die beoogd worden in het Handvest van de grondrechten van de Europese Unie en in het Europese Verdrag tot bescherming van de rechten van de mens.

Zoals de Gegevensbeschermingsautoriteit aangeeft in haar advies, moeten de verplichtingen waarvan sprake in paragraaf 4/2 worden opgelegd door een wet in de formele betekenis van de term. De bepaling werd dus aangepast op de gevraagde manier.

Paragraaf 5 van artikel 122

De wijzigingen in paragraaf 5 zijn noodzakelijk om rekening te houden met de nieuwe paragrafen 4/1 en 4/2 van artikel 122. Bovendien is de Coördinatiecel van de operator ermee belast aan een autoriteit de verkeersgegevens te verstrekken die zij vraagt.

Paragraaf 6 van artikel 122

De Ombudsdienst voor telecom is toegevoegd aan de autoriteiten die ingelicht kunnen worden over de relevante verkeers- en factuurgegevens met het oog op geschillenbeslechting.

Deze toevoeging verduidelijkt de mogelijkheid voor de operator om verkeersgegevens door te sturen naar de Ombudsdienst voor telecom wanneer bij die dienst tegen deze operator een klacht is ingediend.

Deze bepaling kent echter geen nieuwe bevoegdheden toe aan de Ombudsdienst voor telecom.

Art. 6 (aanpassingen aan artikel 123)

Artikel 123 verwijst voortaan naar "andere locatiegegevens dan verkeersgegevens" om het opschrift van artikel 9 van de richtlijn betreffende privacy en

directive"vie privée et communications électroniques" (directive 2002/58/CE) qu'il transpose. La signalisation mobile contient certaines données de localisation sous la forme de "mises à jour de localisation".

Les données de localisation qui constituent des données de trafic sont traitées par l'article 122 de la loi télécom.

En outre, l'article 123 est complété pour tenir compte des évolutions techniques et légales.

Il convient bien entendu de rappeler qu'un opérateur ne doit conserver que les données qu'il traite ou qu'il génère.

Conformément à la demande de l'Autorité de protection des données, des durées maximales de conservation des données ont été ajoutées. Il s'agit des mêmes durées que celles retenues pour l'article 122, § 4.

L'alinéa 1er, 5° du paragraphe 1er confirme qu'un opérateur est autorisé à traiter des données de localisation pour répondre à une obligation légale.

Ainsi, par exemple, un opérateur pourrait recevoir une injonction d'une autorité de geler certaines données de localisation (conservation rapide), comme prévu dans l'arrêt Quadrature du Net du 6/10/2020 de la CJUE (affaires C-511/18, C-512/18 et C- 520/18: *La Quadrature du Net*, *French Data Network* et Ordre des barreaux francophones et germanophone).

Comme l'Autorité de protection des données l'indique dans son avis, les obligations dont il est question au paragraphe 1er, 5°, doivent être imposées par une loi au sens formel du terme. La disposition a donc été adaptée en ce sens.

Un autre exemple est la fourniture par un opérateur de données de localisation à une autorité (par exemple les autorités judiciaires, les services de renseignement et de sécurité ou la Cellule des personnes disparues de la Police Fédérale) pour répondre à sa demande. Cette autorité ne pourra bien entendu exiger de telles données que si cela est prévu dans sa législation organique.

Lorsque l'opérateur doit traiter des données pour les fournir à une autorité, c'est sa Cellule de coordination qui devra intervenir pour ce traitement.

Art. 7 (modification à l'article 125)

Dans son arrêt du 22 avril 2021 (n° 57/2021), la Cour constitutionnelle a annulé l'abrogation de l'article 125,

elektronische communicatie (Richtlijn 2002/58/EG) die het omzet, beter te weerspiegelen. In de mobiele signalisatie zitten bepaalde locatiegegevens in de vorm van "locatie-updates".

Locatiegegevens die verkeersgegevens vormen, worden behandeld in artikel 122 van de telecomwet.

Bovendien wordt artikel 123 aangevuld om rekening te houden met de technische en wettelijke ontwikkelingen.

Er dient evenwel aan te worden herinnerd dat een operator enkel de gegevens moet bewaren die hij behandelt of genereert.

Conform het verzoek van de Gegevensbeschermingsautoriteit werden maximale termijnen voor gegevensbewaring toegevoegd. Het betreft dezelfde termijnen als deze gekozen voor artikel 122, § 4.

Het eerste lid, 5°, van paragraaf 1 bevestigt dat een operator locatiegegevens mag verwerken om aan een wettelijke verplichting te voldoen.

Zo zou een operator van een autoriteit een bevel kunnen krijgen om bepaalde locatiegegevens te bevriezen (snelle bewaring), zoals bepaald in het arrest Quadrature du Net van 6/10/2020 van het HvJ-EU (de zaken C-511/18, C-512/18 en C-520/18: *La Quadrature du Net*, *French Data Network* et *Ordre des barreaux francophones et germanophone*).

Zoals de Gegevensbeschermingsautoriteit aangeeft in haar advies, moeten de verplichtingen waarvan sprake in paragraaf 1, 5°, worden opgelegd door een wet in de formele betekenis van de term. De bepaling werd bijgevolg in die zin aangepast.

Een ander voorbeeld is de verstrekking door een operator van locatiegegevens aan een autoriteit (bijv. de gerechtelijke autoriteiten, de inlichtingen- en veiligheidsdiensten of de cel Vermiste Personen van de federale politie) om aan haar verzoek te voldoen. Deze autoriteit zal zulke gegevens uiteraard maar mogen eisen als die is vastgelegd in haar organieke wet.

Wanneer de operator gegevens moet verwerken om ze aan een autoriteit te verstrekken, zal zijn Coördinatiecel voor die verwerking moeten zorgen.

Art. 7 (wijziging aan artikel 125)

In zijn arrest van 22 april 2021 (nr. 57/2021) heeft het Grondwettelijk Hof de opheffing van artikel 125, § 2, van

§ 2, de la loi du 13 juin 2005. Il convient de réintroduire cette abrogation, qui permet de simplifier cette loi.

Art. 8 (remplacement de l'article 126)

Certaines modifications ont été apportées à l'article 126 de manière à s'aligner sur la terminologie et les définitions qui sont employées dans la loi télécom depuis la transposition dans cette loi du Code des communications électroniques européen (directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen).

Concernant le paragraphe 1er et vu que la notion de service de communications électroniques est définie dans le Code de manière plus large qu'actuellement, il n'est plus nécessaire de viser les opérateurs et les fournisseurs de services mais il suffit de viser les opérateurs.

Le présent article est applicable lorsqu'un service de communications électroniques est fourni en Belgique.

Pour mettre en œuvre l'arrêt de la Cour constitutionnelle du 22 avril 2021 et l'arrêt Quadrature du Net de la Cour de Justice de l'Union européenne, ne sont plus visées par l'obligation de conservation que les données de souscription et les données qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé.

Les données de souscription comprennent entre autres le numéro de téléphone, l'adresse e-mail, la date de début et de fin de la souscription. Le Conseil d'État français, qui a été amené à examiner la législation française en matière de conservation de données de trafic par les opérateurs pour les autorités (arrêt du 21/04/2021 nos 393099, 394922, 397844, 397851, 424717, 424718, *FRENCH DATA NETWORK* et autres), a considéré à cet égard ce qui suit: "il résulte clairement de la directive du 12 juillet 2002 et du RGPD qu'ils ne s'opposent pas à une obligation de conservation généralisée et indifférenciée, pour une durée d'un an, des informations autres que celles relatives à l'identité civile fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, d'une part, et des données relatives aux paiements, d'autre part, mentionnées respectivement aux 3° et 4° de l'article 1er du décret du 25 février 2011" (point 36).

Dans son arrêt La Quadrature du Net du 6/10/2020, la CJUE autorise la conservation généralisée et

de wet van 13 juni 2005 vernietigd. Deze opheffing, die deze wet kan vereenvoudigen, dient opnieuw te worden ingevoerd.

Art. 8 (vervanging van artikel 126)

Bepaalde wijzigingen werden in artikel 126 aangebracht om zich te conformeren aan de terminologie en definities die in de telecomwet gebruikt worden sinds de omzetting in deze wet van het Europees wetboek voor elektronische communicatie (Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie).

Wat betreft paragraaf 1 en aangezien het begrip van elektronische-communicatiedienst in het Wetboek ruimer gedefinieerd is dan nu het geval is, is het niet meer noodzakelijk om de operatoren en de aanbieders van diensten te beogen, maar volstaat het om de operatoren te beogen.

Dit artikel is van toepassing wanneer een elektronische-communicatiedienst in België wordt verstrekt.

Voor de tenuitvoerlegging van het arrest van het Grondwettelijk Hof van 22 april 2021en het arrest-*Quadrature du Net* van het Europees Hof van Justitie worden voor de bewaringsplicht enkel nog de abonnementsgegevens en gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst beoogd.

De abonnementsgegevens omvatten onder andere het telefoonnummer, het e-mailadres, de start- en einddatum van het abonnement. De Franse Conseil d'État, die de Franse wetgeving betreffende bewaring van verkeersgegevens door de operatoren voor de autoriteiten moest onderzoeken (arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, *FRENCH DATA NETWORK* et autres), heeft daarover het volgende gesteld: "uit de richtlijn van 12 juli 2002 en van de AVG blijkt duidelijk dat zij niet gekant zijn tegen een verplichting tot algemene en ongedifferentieerde bewaring, voor de duur van een jaar, van andere inlichtingen dan die in verband met de burgerlijke identiteit die verstrekt zijn bij het sluiten van een contract door een gebruiker of bij het aanmaken van een account enerzijds, en van de gegevens met betrekking tot de betalingen anderzijds, respectievelijk vermeld in de bepalingen onder 3° en 4° van artikel 1 van het decreet van 25 februari 2011" (punt 36) (vrij vertaald).

In zijn arrest-*La Quadrature du Net* van 6/10/2020 staat het HvJ-EU de algemene en ongedifferentieerde bewaring

indifférenciée de l'adresse IP à la source de la communication (ci-après l'adresse IP source). Dans le même arrêt, la CJUE rappelle que l'adresse IP source est le seul moyen susceptible de permettre l'identification de l'auteur d'une infraction en ligne (point 154 de l'arrêt).

Cependant, la conservation de cette seule donnée n'est pas suffisante pour atteindre l'objectif poursuivi (identification *in fine* de l'utilisateur final). En pratique, ainsi que les opérateurs l'ont indiqué lors de la consultation publique sur l'avant-projet de loi, des données de trafic liées à l'adresse IP source doivent être conservées avec cette adresse pour relier l'adresse IP à une personne spécifique. Il en va de même pour retrouver le numéro de téléphone utilisé ou le numéro MSISDN ("*Mobile Subscriber Integrated Services Digital Network*", à savoir le numéro de téléphone avec le préfixe international) servi.

Les identifiants techniques qui servent principalement à identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé comprennent entre autres l'adresse IP source, l'IMEI (*International Mobile Equipment Identity*), l'IMSI (*International Mobile Subscriber Identity*), l'ICCID (*Integrated Circuit Card Identifier*), l'adresse MAC, le MSISDN (*Mobile Station Integrated Services Digital Network*), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées. À ce jour, la Cour de justice de l'Union européenne ne s'est expressément prononcée que sur l'adresse IP source mais pas sur les autres données techniques précitées, dont la conservation est également nécessaire à des fins d'identification.

Au vu de l'utilité que représentent ces données techniques afin de permettre l'identification d'auteurs d'infractions en ligne ou hors ligne, la mesure de conservation prévue est proportionnée.

La CJUE n'a pas indiqué dans l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, point 20) que la conservation de l'IMEI était interdite. Dans cet arrêt, a été considérée comme ne constituant pas une ingérence grave aux droits fondamentaux (vie privée et protection des données à caractère personnel), la demande de la police judiciaire, pour les besoins d'une enquête pénale, de se voir transmettre les numéros de téléphone activés, pendant une période de douze jours, avec le code relatif à l'identité internationale d'équipement mobile (ci-après le "code IMEI") du téléphone mobile volé ainsi que les données à caractère personnel relatives à l'identité civile des

toe van het IP-adres van de bron van de communicatie (hierna IP-bronadres). In hetzelfde arrest herinnert het HvJ-EU eraan dat het IP-bronadres het enige middel is aan de hand waarvan de dader van een online-inbreuk kan worden geïdentificeerd (punt 154 van het arrest).

Het bewaren van enkel dit gegeven is evenwel niet voldoende om het streefdoel te bereiken (uiteindelijke identificatie van de eindgebruiker). In de praktijk, zoals de operatoren het hebben aangegeven tijdens de openbare raadpleging over het voorontwerp van wet, moeten verkeersgegevens gelieerd aan het IP-bronadres samen met dit adres bewaard worden om het IP-adres aan een specifieke persoon te linken. Hetzelfde geldt om het gebruikte telefoonnummer of MSISDN-nummer ("*Mobile Subscriber Integrated Services Digital Network*", met name het telefoonnummer met het internationale prefix) terug te vinden.

De technische identificatiecodes die hoofdzakelijk dienen om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, omvatten onder andere het IP-bronadres, de IMEI (*International Mobile Equipment Identity*), IMSI (*International Mobile Subscriber Identity*), ICCID (*Integrated Circuit Card Identifier*), het MAC-adres, het MSISDN (*Mobile Station Integrated Services Digital Network*), of andere identificatiecodes die zullen worden ontwikkeld in het kader van 5G of afhankelijk van de evolutie van de gebruikte technologieën. Tot op heden heeft het Hof van Justitie van de Europese Unie zich enkel uitdrukkelijk uitgesproken over het IP-adres aan de bron, maar niet over de voormelde andere technische gegevens, waarvan de bewaring eveneens noodzakelijk is voor identificatiedoeleinden.

In het licht van het nut dat deze technische gegevens vertegenwoordigen voor de identificatie van daders van overtredingen online en offline, is de geplande bewaringsmaatregel evenredig.

Het HvJ-EU heeft in het arrest van 2 oktober 2018, Ministerio Fiscal (C207/16, punt 20) niet vermeld dat de bewaring van de IMEI verboden was. In dat arrest werd beschouwd dat het volgende geen ernstige inmenging vormt in de grondrechten (persoonlijke levenssfeer en bescherming van de persoonsgebonden gegevens): het verzoek van de gerechtelijke politie, ten behoeve van een strafrechtelijk onderzoek, om de telefoonnummers te krijgen die gedurende een periode van twaalf dagen werden geactiveerd aan de hand van de code voor de internationale identiteit van het mobiele toestel (hierna de "IMEI-code") van de gestolen mobiele telefoon alsook

titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code.

Dans son avis, l'Autorité de protection des données indique ce qui suit:

"102. L'avant-projet de loi – et le projet d'arrêté qui l'exécute – prévoient également la conservation des numéros d'identification des terminaux des utilisateurs finaux. Sauf erreur, l'exigence de conservation de cette donnée est nouvelle. Les numéros d'identification des terminaux des utilisateurs finaux constituent un identifiant unique des équipements terminaux qui permettent de "tracer" un terminal à travers l'ensemble des services de communications électroniques qu'il utilise. La conservation préventive et systématique de ces numéros constitue dès lors une ingérence importante dans les droits au respect de la vie privée et à la protection des données à caractère personnel. Leur conservation doit dès lors être soumise au strict respect des conditions de nécessité et de proportionnalité au regard des objectifs poursuivis. À cet égard, la jurisprudence de la Cour de Luxembourg concernant la conservation généralisée des adresses IP peut être utilement mobilisée pour déterminer les conditions que doit rencontrer une mesure législative qui impose la conservation de telles données d'identification unique des équipements terminaux des abonnés. Le délégué du ministre, dans une réponse à une demande d'informations complémentaires, souligne d'ailleurs, lui aussi, que le raisonnement suivi par la CJUE à propos des adresses IP "peut être suivi quant aux autres données techniques nécessaires pour identifier l'utilisateur final, l'équipement terminal, le service de communications électroniques employé". Ainsi, la conservation de ces données ne devrait être imposée qu'afin de poursuivre un objectif présentant une importance particulière (comme la lutte contre la criminalité grave), la durée de leur conservation devrait être strictement limitée au regard de cet objectif et il faudrait prévoir des conditions et des garanties strictes quant à l'exploitation de ces données. L'avant-projet de loi et le projet d'arrêté, qui ne rencontrent pas ces exigences, devront donc être adaptés afin d'y répondre."

Tout d'abord, contrairement à ce que l'Autorité de protection des données indique, l'exigence de conservation des numéros d'identification des terminaux des utilisateurs finaux n'est pas nouvelle mais résulte déjà de l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.

Ensuite, contrairement à ce que cette Autorité indique dans son avis, une telle donnée à elle seule ne permet

de persoonsgebonden gegevens met betrekking tot de burgerlijke identiteit van de houders of van de gebruikers van de telefoonnummers die overeenstemmen met de via deze code geactiveerde simkaarten.

In haar advies geeft de Gegevensbeschermingsautoriteit het volgende aan:

"102. Het voorontwerp van wet – en het ontwerpbesluit tot uitvoering ervan – voorziet ook in de bewaring van de identificatienummers van de eindapparaten van de eindgebruikers. Behoudens vergissing werd de bewaring van dit gegeven nog niet eerder geëist. De identificatienummers van de eindapparaten van de eindgebruikers zijn een unieke identificatie van de eindapparaten waarmee een apparaat kan worden "getraceerd" via alle elektronische communicatiediensten die het gebruikt. De preventieve en systematische bewaring van deze nummers vormt dus een ernstige inmenging in de privacyrechten en in het recht op bescherming van de persoonsgegevens. Daarom moet de bewaring ervan strikt noodzakelijk en strikt evenredig zijn met de beoogde doelen. In dit opzicht kan de rechtspraak van het Hof van Luxemburg aangaande de algemene bewaring van de IP-adressen worden aangewend om te bepalen aan welke voorwaarden een wetgevende maatregel die verplicht tot de bewaring van die unieke identificatiegegevens van de eindapparaten van de abonnees moet voldoen. In een antwoord op een verzoek om verdere inlichtingen, benadrukt ook de afgevaardigde van de minister dat de redenering van het HvJ-EU aangaande de IP-adressen "ook kan worden gevolgd voor andere technische gegevens die nodig zijn om de eindgebruiker, het eindapparaat en de gebruikte elektronische communicatiedienst te identificeren". De bewaring van die gegevens zou dus enkel mogen worden opgelegd om een doel na te streven van bijzonder belang (zoals de bestrijding van zware criminaliteit), de bewaartermijn zou niet langer mogen zijn dan strikt noodzakelijk is gelet op dat doel en er zou moeten worden voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens. Aangezien het voorontwerp van wet en het ontwerpbesluit niet aan die eisen voldoen, moeten ze worden aangepast."

Allereerst is, in tegenstelling tot wat de Gegevensbeschermingsautoriteit aangeeft, de eis tot bewaring van de identificatienummers van de eindapparaten van de eindgebruikers niet nieuw, maar vloeit die reeds voort uit het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Vervolgens, in tegenstelling tot wat de Gegevensbeschermingsautoriteit in haar advies aangeeft, maakt

pas de “tracer” un terminal à travers l’ensemble des services de communications électroniques qu’il utilise. Cependant, pour protéger la vie privée des individus, il convient de déterminer si une demande d’une autorité envers un opérateur basée sur ce type de données permet d’obtenir des données sensibles ou pas sur un utilisateur. Si c’est le cas, alors des conditions strictes doivent être applicables à la demande de l’autorité.

L’Autorité de protection des données fait la comparaison avec l’adresse IP à la source de la communication. À cet égard, au point 153 de son arrêt La Quadrature du Net, la CJUE considère que “les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d’un internaute et, par suite, de son activité en ligne, ces données permettent d’établir le profil détaillé de ce dernier”. Cependant, il faut rappeler que les opérateurs ne sont pas autorisés à conserver les adresses IP de destination dans le cadre du service d’accès à internet mais doivent uniquement conserver les adresses IP à la source de la communication. Dans le cadre de l’article 126/1, les opérateurs doivent conserver l’adresse IP de destination d’une communication téléphonique par internet (il s’agit dans ce cas de l’équivalent du numéro de téléphone appelé).

Les adresses IP à la source de la connexion ne permettent pas à elles seules d’effectuer le traçage exhaustif du parcours de navigation d’un internaute.

Il convient de rappeler que si un opérateur ne traite pas de données à conserver ni ne les génère, l’obligation de conserver des données est en pratique sans objet pour lui.

La durée de conservation de 12 mois a été maintenue, dès lors que cette durée correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave.

Cependant, une distinction est effectuée entre l’adresse IP utilisée pour souscrire au service et les autres adresses IP. En effet, l’adresse IP utilisée pour souscrire au service est une donnée qui doit être conservée par l’opérateur dans le cadre de l’arrêté royal du 19 septembre 2013 portant exécution de l’article 126 de la loi du 13 juin 2005 relative aux communications électroniques (pour autant que l’opérateur traite ou génère cette donnée), afin de pouvoir établir ou vérifier l’identité de l’abonné (conservation jusqu’à 12 mois après la fin du contrat). Les

een dergelijk gegeven op zich het niet mogelijk om een eindtoestel te “traceren” door alle elektronischecommunicatiediensten die het gebruikt heen. Om de privacy van de individuen te beschermen, moet evenwel worden bepaald of een verzoek van een autoriteit aan een operator dat gebaseerd is op dergelijke gegevens het mogelijk maakt om over een gebruiker al dan niet gevoelige gegevens te verkrijgen. Als dat zo is dan moeten strikte voorwaarden toegepast kunnen worden op verzoek van de autoriteit.

De Gegevensbeschermingsautoriteit maakt de vergelijking met het IP-adres dat aan de bron ligt van de communicatie. In dat opzicht beschouwt het HvJ-EU in zijn arrest *La Quadrature du Net* in punt 153 het volgende: “Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld.” Evenwel moet eraan worden herinnerd dat de operatoren geen IP-adressen van de bestemming mogen bewaren in het kader van de internettoegangsdienst maar enkel de IP-adressen aan de bron van de communicatie moeten bewaren. In het kader van artikel 126/1 moeten de operatoren het IP-adres van bestemming van een telefonische communicatie via het internet bewaren (in dat geval gaat het om het equivalent van het gebelde telefoonnummer).

De IP-adressen aan de bron van de verbinding alleen maken het niet mogelijk om de volledige zoekgeschiedenis van een internetgebruiker te traceren.

Er dient te worden aan herinnerd dat indien een operator de te bewaren gegevens niet verwerkt en niet genereert, de verplichting tot gegevensbewaring in de praktijk zonder voorwerp is voor hem.

De bewaringstermijn van 12 maanden werd behouden, aangezien deze termijn overeenstemt met de strikt noodzakelijke bewaringstermijn om de autoriteiten in staat te stellen om hun onderzoeken tot een goed einde te brengen, in het bijzonder op het stuk van de strijd tegen de zware criminaliteit.

Er wordt evenwel een onderscheid gemaakt tussen het IP-adres dat gebruikt is om op de dienst in te tekenen en de overige IP-adressen. Het IP-adres dat gebruikt is om in te tekenen op de dienst is immers een gegeven dat door de operatoren moet worden bewaard in het kader van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, om de identiteit van de abonnee te kunnen vaststellen of nagaan (bewaring tot 12 maanden na het einde van het contract). De

autres adresses IP, soit les adresses IP à la source de la communication, sont conservées dans le cadre de l'article 126 jusqu'à 12 mois après la fin de la session.

Lors de la consultation publique sur l'avant-projet de loi, certains opérateurs ont indiqué que la durée de conservation des adresses MAC, du numéro IMEI et d'autres numéros qui permettent d'identifier l'équipement terminal devait être identique à la durée de conservation des adresses IP (autres que l'adresse IP ayant servi à la souscription du service) et donc être plus courte que douze mois après la fin du contrat. Ces opérateurs indiquent que leurs clients peuvent utiliser de multiples adresses MAC sur une courte période de temps et que la conservation de ces données risque de générer un volume de données significatif. Cette remarque a été prise en compte. Par conséquent, le Roi fixera une liste de données d'identification technique dont la durée de conservation est limitée à un an après la fin de session.

Art. 9 (insertion de l'article 126/1)

Introduction

L'ancien article 126/1 de la LCE a été déplacé vers l'article 127/3 de la même loi. L'article 8 donne donc un contenu tout à fait nouveau à l'article 126/1.

La Cour de justice européenne a statué dans l'arrêt "Quadrature du Net" du 6 octobre 2020 que le droit de l'Union européenne, en particulier l'article 15, paragraphe 1 de la directive 2002/58, doit être interprété comme s'opposant à des mesures législatives prévoyant la conservation préventive, générale et sans discrimination, de données relatives au trafic et de données de localisation. La Cour constitutionnelle a suivi ce raisonnement dans son arrêt du 22 avril 2021, et a annulé (partiellement) la loi du 29 mai 2016 sur la collecte et la conservation des données dans le secteur des communications électroniques.

Conformément à cette jurisprudence, le présent article prévoit une conservation ciblée sur base géographique afin de permettre aux autorités judiciaires et aux services de renseignement de remplir leurs missions. L'accès aux données de communication est indispensable pour les enquêtes criminelles et les enquêtes à des fins de renseignement, tout comme la possibilité de disposer de données dites "historiques", c'est-à-dire de pouvoir remonter un certain laps de temps dans le passé, en examinant des données conservées antérieurement à la demande des autorités.

overige IP-adressen, namelijk de IP-adressen aan de bron van de communicatie, worden in het kader van artikel 126 bewaard tot 12 maanden na het einde van de sessie.

Tijdens de openbare raadpleging over het voorontwerp van wet, hebben sommige operatoren laten weten dat de bewaartermijn van de MAC-adressen, van het IMEI-nummer en van andere nummers aan de hand waarvan het eindtoestel geïdentificeerd kan worden, identiek moest zijn aan de bewaartermijn van de IP-adressen (andere dan het IP-adres dat gediend heeft voor de intekening op de dienst) en dus korter moet zijn dan twaalf maanden na het einde van het contract. Deze operatoren geven aan dat hun klanten op korte tijd talrijke MAC-adressen kunnen gebruiken en dat de bewaring van deze gegevens riskeert een aanzienlijk datavolume te doen ontstaan. Met die opmerking is rekening gehouden. Bijgevolg zal de Koning een technische lijst van identificatiegegevens vaststellen waarvan de bewaartijd beperkt is tot een jaar na het einde van de sessie.

Art. 9 (invoeging van artikel 126/1)

Inleiding

Het oude artikel 126/1 van de WEC wordt door huidig wetsontwerp verplaatst naar artikel 127/3 van dezelfde wet. Artikel 8 geeft aan artikel 126/1 dus een volledig nieuwe inhoud.

Het Europese Hof van Justitie heeft in het arrest "*Quadrature du Net*" van 6 oktober 2020 bepaald dat het Unierecht, meer bepaald artikel 15, paragraaf 1 van de Richtlijn 2002/58 in die zin geïnterpreteerd moet worden dat het zich verzet tegen de wetgevende maatregelen die voorzien in een preventieve algemene en ongedifferentieerde bewaring van verkeersgegevens en locatiegegevens. Het Grondwettelijk Hof heeft deze redenering gevolgd in het arrest van 22 april 2021, en heeft de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (gedeeltelijk) vernietigd.

Conform deze rechtspraak voorziet huidig artikel in een gerichte bewaring op basis van een geografisch criterium, die zowel de gerechtelijke autoriteiten als de inlichtingendiensten in staat moet stellen om hun opdrachten te vervullen. De toegang tot de communicatiegegevens is onontbeerlijk, voor strafonderzoeken en onderzoeken met het oog op inlichtingen, net als de mogelijkheid om te beschikken over de zogenaamde "historische" data, d.w.z. de mogelijkheid om een bepaalde periode in het verleden terug te gaan, door gegevens te bestuderen die eerder op verzoek van de autoriteiten zijn bewaard.

Il convient également de noter que la conservation peut être bénéfique à la fois pour la victime, pour ses propres données (par exemple, dans les cas de harcèlement, il est important de pouvoir remonter dans le passé des données de la victime afin d'identifier l'origine d'un appel, d'un courriel ou d'un SMS), et pour l'accusé (les données de localisation peuvent prouver que l'accusé ne se trouvait pas sur la scène du crime au moment où celui-ci a été commis). Il peut aussi s'agir d'identifier des témoins ce qui peut jouer à charge comme à décharge. (Parl. Chambre, DOC 54 1567/001, p. 10-11).

Dans son arrêt du 6 octobre 2020, la Cour de justice a elle-même suggéré un certain nombre de pistes qui pourraient pallier l'absence d'une conservation généralisée et indifférenciée. L'une d'entre elles est ce qu'on appelle la "conservation ciblée", qui fait l'objet du présent article.

En effet, la Cour a déclaré, en résumé, au paragraphe 168:

"En revanche, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable.".

La Cour s'est penchée sur cette problématique dans les paragraphes 146 et suivants, que nous reproduisons ici afin de mieux comprendre le présent article (arrêt "Quadrature du Net", §§ 146 à 151).

"146. En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que

Er moet trouwens ook gewezen worden op het feit dat de bewaring zowel in het voordeel kan zijn van het slachtoffer, voor zijn eigen gegevens (bijvoorbeeld, in zaken met betrekking tot belaging is het van belang om in het verleden van de gegevens van het slachtoffer te kunnen teruggaan met het oog op het identificeren van de oorsprong van een oproep, een e-mail of een sms), als van de beschuldigde (de lokalisatiegegevens kunnen aantonen dat de beschuldigde niet op de plaats van het misdrijf was op het tijdstip waarop het werd gepleegd). Het kan ook van belang zijn om getuigen te identificeren, wat zowel à charge als à décharge kan meespelen (Parl. St., Kamer, DOC 54 1567/001, blz. 10-11).

Het Hof van Justitie reikte in het arrest van 6 oktober 2020 zelf een aantal pistes aan die het gebrek aan een algemene en ongedifferentieerde bewaring kunnen opvangen. Eén van die pistes betreft de zogenaamde "gerichte bewaring", en is het voorwerp van huidig artikel.

Het Hof stelde immers, in de samenvattende paragraaf 168, het volgende:

"Artikel 15, lid 1, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, verzet zich daarentegen niet tegen wettelijke maatregelen die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd.".

Het Hof ging in de paragrafen 146 en volgende dieper in op deze problematiek. We nemen deze paragrafen hier over om huidig artikel beter te begrijpen (arrest "*Quadrature du Net*, §§ 146 tot 151).

"146. Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onderhavige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, a fortiori, bescherming van de nationale veiligheid – gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name

comporte une conservation ciblée des données relatives au trafic et des données de localisation."

147. Ainsi, comme l'a déjà jugé la Cour, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 108).

148. S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111).

149. À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.

150. La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15,

het Grondwettelijk Hof heeft gerefereerd – de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt."

147. Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 108).

148. De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand van de categorieën betrokken personen, aangezien artikel 15, lid 1, van Richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 111).

149. In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zijn die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.

150. Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 111). Het kan daarbij met

EU:C:2016:970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.

151. Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.".

Le Conseil d'État s'est interrogé, de manière légitime, sur la limitation temporelle de la présente mesure de conservation ciblée sur base géographique et son renouvellement périodique. À cet égard, selon le législateur, l'objectif de ce principe de limitation temporelle exigé par la Cour de Justice de l'Union européenne vise précisément à renforcer le caractère strictement nécessaire de la mesure de conservation et dès lors à s'assurer qu'un examen de la persistance de la nécessité de procéder à la conservation est effectué.

Néanmoins, l'introduction d'une nouvelle législation en la matière, qui est la manière la plus adéquate de mettre en œuvre en Belgique la conservation de données sur base géographique, se concilierait difficilement avec un renouvellement périodique de la mesure car cela impliquerait de mener à intervalles réguliers un nouveau processus législatif. Ces modifications législatives récurrentes créeraient une insécurité juridique tant pour les opérateurs que pour le citoyen. Pour cette raison, et afin de respecter l'exigence de limitation de la mesure et de son renouvellement, le législateur a opté pour une évaluation annuelle de la législation, au terme de laquelle, sur la base d'un rapport d'évaluation annuelle, le Parlement peut décider d'adapter la législation en modifiant notamment les zones géographiques concernées.

En outre, pour ce qui concerne la conservation de données au niveau des arrondissements judiciaires et des zones de police, celle-ci est enclenchée uniquement sur la base de statistiques annuelles faisant à chaque fois l'objet d'une validation par une autorité de contrôle.

Enfin, le changement d'affectation d'une zone, tel qu'un bâtiment qui ne serait plus utilisé comme gare,

name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.

151. Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.".

De Raad van State heeft terecht vraagtekens geplaatst bij de beperking in de tijd van de huidige geografisch gerichte bewaringsmaatregel en de periodieke hernieuwing ervan. In dit verband heeft dit door het Europese Hof van Justitie voorgeschreven beginsel van beperking in de tijd volgens de wetgever juist tot doel het strikt noodzakelijke karakter van de bewaringsmaatregel te versterken en dus te waarborgen dat wordt onderzocht of de noodzaak tot bewaring blijft bestaan.

De invoering van nieuwe wetgeving op dit gebied, wat de meest geschikte manier is om de bewaring van geografische gegevens in België ten uitvoer te leggen, is echter moeilijk te verenigen met een periodieke hernieuwing van de maatregel, aangezien dit zou betekenen dat op gezette tijden een nieuw wetgevingsproces moet worden gevoerd. Dergelijke terugkerende wetswijzigingen zouden zowel voor de operatoren als voor de burgers rechtsonzekerheid creëren. Daarom, en om te voldoen aan de eis van beperking van de maatregel en de hernieuwing ervan, heeft de wetgever gekozen voor een jaarlijkse evaluatie van de wetgeving, na afloop waarvan het Parlement, op basis van een jaarlijks evaluatieverslag, kan besluiten de wetgeving aan te passen door de betrokken geografische gebieden te wijzigen.

Bovendien, wat de gegevensbewaring op het niveau van de gerechtelijke arrondissementen en de politiezones betreft, deze wordt enkel geactiveerd op basis van jaarlijkse statistieken, die telkens door een toezichthoudende autoriteit worden gevalideerd.

Tenslotte zal rekening worden gehouden met de verandering van gebruik van een zone, zoals een gebouw

sera pris en compte dès ce changement d'affectation. Dans cette optique, le législateur estime que le caractère strictement nécessaire de la mesure de conservation est respecté.

La piste d'une conservation ciblée, dans laquelle une distinction est faite sur la base de personnes ou de zones géographiques, a déjà été analysée précédemment dans le cadre de la rédaction de la loi du 29 mai 2016. L'exposé des motifs de la loi dit à cet égard ce qui suit (Parl, Chambre, DOC 54 1567/001, p. 12):

"Quant à la référence à une "zone géographique" ou un "cercle de personnes", une activation de l'article 126 LCE sur base de ce type de critère s'apparenterait à du profilage avec les risques de discrimination qui en découlent."

Un examen plus approfondi de l'arrêt de la Cour de justice du 6 octobre 2020, et plus précisément des paragraphes cités ci-dessus, a conduit le législateur à conclure que la conservation ciblée avec une distinction basée sur les zones géographiques est effectivement une option, pour autant que cette distinction soit fondée sur des éléments objectifs et non discriminatoires. Au paragraphe 150, la Cour indique: "Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages".

Le nouvel article 126/1 remplace l'ancien article 126 de la loi sur les communications électroniques en se basant sur cette option. Il est structuré comme suit:

— le paragraphe 1er contient le principe de l'obligation de conservation et la durée de conservation par défaut (12 mois), ainsi que les finalités de la conservation;

— le paragraphe 2 définit les données à conserver;

— le paragraphe 3 indique d'une part les zones géographiques, qui, sur la base de données de statistiques de criminalité ou du niveau général de la menace, doivent faire l'objet d'une conservation temporaire des données, et, d'autre part, les zones géographiques, qui vu leur nature spécifique doivent faire l'objet d'une conservation de données pendant 12 mois;

dat niet langer als station wordt gebruikt, en dit van zodra het gebruik is gewijzigd. In dit verband is de wetgever van mening dat het strikt noodzakelijke karakter van de bewaringsmaatregel wordt gerespecteerd.

De piste van een gerichte bewaring, waarin een onderscheid gemaakt wordt op grond van personen of geografische zones werd al eerder geanalyseerd naar aanleiding van de redactie van de wet van 29 mei 2016. De memorie van toelichting bij de wet zegt daarover het volgende (Parl St., Kamer, DOC 54 1567/001, blz. 12):

"Met betrekking tot de verwijzing naar een "geografische zone" of een "kring van personen" zou een activering van artikel 126 WEC op grond van dit type criterium op profilering lijken, met de risico's van discriminatie die eruit voortvloeien."

Nader onderzoek van de uitspraak van het Hof van Justitie van 6 oktober 2020, en meer bepaald van de hierboven geciteerde paragrafen, bracht de wetgever tot de conclusie dat een gerichte bewaring met een onderscheid op basis van geografische zones wel degelijk een optie is, zolang dat onderscheid gebaseerd is op objectieve en niet-discriminerende elementen. In paragraaf 150 zegt het Hof daarover het volgende: "Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones."

Het nieuwe artikel 126/1 vervangt het oude artikel 126 van de wet betreffende de elektronische communicatie, en is op deze optie gebaseerd. Het is opgebouwd als volgt:

— paragraaf 1 bevat het principe en de standaardduur van de bewaarplicht (12 maanden), alsook de doeleinden van de bewaring;

— paragraaf 2 bepaalt de gegevens die bewaard worden;

— paragraaf 3 geeft aan dat er aan de ene kant geografische zones zijn die, op basis van criminaliteitsstatistieken of op basis van het algemene dreigingsniveau, het onderwerp uitmaken van een tijdelijke bewaarplicht. Aan de andere kant zijn er ook geografische zones die, door hun specifieke aard het onderwerp uitmaken van een bewaarplicht gedurende 12 maanden;

— le paragraphe 4 précise certains aspects du concept de zones géographiques auxquelles la conservation se rapporte;

— le paragraphe 5 donne quelques délégations au Roi, dont la possibilité de déterminer des zones supplémentaires sur la base des critères énumérés dans la loi;

— enfin, le paragraphe 6 prévoit que les ministres compétents soumettent un rapport d'évaluation annuel à la Chambre des représentants.

Paragraphe 1er

Lien avec la législation générale en matière de protection de la vie privée

Le premier alinéa du paragraphe 1er de l'article commence par prévoir qu'il s'applique sans préjudice des dispositions de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et du RGPD. La loi du 30 juillet 2018 est la loi générale qui s'applique en tout état de cause en matière de protection des données à caractère personnel. Outre la loi du 30 juillet 2018, l'article fait également référence au Règlement général sur la protection des données, le règlement européen ayant un effet direct qui uniformise les règles relatives au traitement des données à caractère personnel par les entreprises privées et les autorités publiques dans toute l'Union européenne.

La présente loi particularise et complète les règles générales en matière de protection des données prévues par la loi du 30 juillet 2018 et le RGPD au regard des communications électroniques. Dans le même sens, ce nouvel article 126/1 s'applique dans les limites légalement prévues et conformément aux règles générales de protection des données.

Dès lors, les fournisseurs et opérateurs sont explicitement tenus de respecter l'ensemble des dispositions de la loi du 30 juillet 2018, en ce qui concerne notamment la qualité des données (exactitude, mise à jour, conservation sous une forme permettant l'identification des personnes concernées, etc.), les obligations du responsable de traitement (confidentialité, mesures techniques et organisationnelles, sous-traitance, etc.), et les droits de la personne concernée. Cette dernière conserve bien entendu ses droits: elle devra être informée par les fournisseurs et les opérateurs de la conservation de ses données pendant la période fixée par la loi, elle pourra accéder à ses données et pourra, le cas échéant, les faire rectifier. Il va de soi que la personne concernée

— paragraaf 4 definieert het concept van geografische zones waarop de bewaring betrekking heeft;

— paragraaf 5 geeft een aantal delegaties aan de Koning, o.a. de mogelijkheid om op basis van de in de wet opgesomde criteria, aanvullende zones te bepalen op basis van hun specifieke aard;

— paragraaf 6, tenslotte, bepaalt dat de bevoegde ministers een jaarlijks evaluatieverslag uitbrengen aan de Kamer van volksvertegenwoordigers.

Paragraaf 1

Verband met de algemene wetgeving inzake de bescherming van de persoonlijke levenssfeer

Het eerste lid van paragraaf 1 van het artikel start met te bepalen dat het van toepassing is onverminderd de bepalingen van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de AVG. De wet van 30 juli 2018 is de algemene wet die in elk geval van toepassing is inzake de bescherming van persoonsgegevens. Naast de wet van 30 juli 2018, verwijst het artikel ook naar de Algemene Verordening Gegevensbescherming, de Europese verordening met rechtstreekse werking die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

Deze wet preciseert en vervolledigt de algemene regels inzake gegevensbescherming waarin de wet van 30 juli 2018 en de AVG voorzien met betrekking tot elektronische communicatie. In dezelfde zin is dit nieuwe artikel 126/1 van toepassing binnen de grenzen waarin de wet voorziet en overeenkomstig de algemene regels inzake gegevensbescherming.

Daarom zijn de operatoren uitdrukkelijk verplicht alle bepalingen van de wet van 30 juli 2018 na te leven, wat betreft meer bepaald de kwaliteit van de gegevens (nauwkeurigheid, bijwerking, bewaring op een manier die het mogelijk maakt de betrokken personen te identificeren, enz.), de verplichtingen van de persoon die verantwoordelijk is voor de verwerking (vertrouwelijkheid, technische en organisatorische maatregelen, uitbesteding, enz.), en de rechten van de betrokken persoon. Deze laatste behoudt uiteraard zijn rechten: de aanbieders en operatoren dienen de persoon op de hoogte te brengen van de bewaring van zijn gegevens gedurende de wettelijk vastgestelde periode; de persoon dient zijn gegevens te kunnen inzien en, indien nodig,

ne peut accéder qu'à ses données personnelles et pas aux données d'autres personnes.

Il est par ailleurs important de rappeler que dès lors que les données doivent être conservées à titre préventif par les opérateurs sur la base de cet article, seuls les services qui disposent d'une base légale et du besoin d'en connaître pour les seules finalités visées par le présent article peuvent selon leur procédure ad hoc demander ces données.

Les entreprises tenues de conserver des données

L'alinéa 1er du paragraphe 1er traite également du champ d'application de l'article, qui s'applique tant aux opérateurs fournissant des services de communication, y compris de téléphonie, ou des services d'accès à Internet aux utilisateurs finals, qu'aux opérateurs fournissant des réseaux de communications électroniques sous-jacents.

Le paragraphe 1er précise en outre que les données ne sont conservées par les opérateurs concernés que dans la mesure où ces données ont été générées ou traitées par eux dans le cadre de la fourniture des services de communication concernés, et uniquement dans les zones géographiques prédéfinies. En d'autres termes, il n'y a aucune obligation de conserver les données lorsque celles-ci:

1° ne sont pas générées ou traitées par les opérateurs concernés;

2° ne sont pas générées ou traitées dans les zones géographiques déterminées au paragraphe 3.

Finalités de la conservation

Le paragraphe 1er prévoit également que les données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique et et de la sauvegarde des intérêts vitaux d'une personne physique.

À cet égard, nous pouvons noter que la finalité de la lutte contre les infractions graves, pour laquelle ces données sont conservées et peuvent être demandées, comprend également une enquête portant sur un éventuel abus de marché menée par l'auditeur de la FSMA. Les infractions à l'interdiction des abus de marché (articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché)) deze te laten rechtzetten. Het spreekt vanzelf dat de betrokken persoon slechts zijn persoonlijke gegevens kan inkijken en niet de gegevens van andere personen.

Het is overigens ook nuttig erop te wijzen dat, aangezien de gegevens op basis van dit artikel door de operatoren voor preventieve doeleinden moeten worden bewaard, enkel de diensten die een wettelijke basis hebben en een need-to-know hebben voor de finaliteiten bedoeld in huidig artikel, deze gegevens kunnen opvragen overeenkomstig hun ad hoc procedure.

De ondernemingen die verplicht zijn tot de bewaring van gegevens

Het eerste lid van paragraaf 1 behandelt ook het toepassingsgebied van het artikel, dat van toepassing is op zowel operatoren die aan de eindgebruikers communicatiediensten, met inbegrip van telefonie, of internettoegangsdiensten aanbieden, als de operatoren die onderliggende elektronische communicatienetwerken aanbieden.

Paragraaf 1 preciseert verder dat de gegevens enkel bewaard worden door de betrokken operatoren voor zover deze gegevens werden gegenereerd of behandeld door hen in het kader van de verstrekking van de betrokken communicatiediensten, en enkel binnen de vooraf bepaalde geografische zones. Er is m.a.w. geen verplichting gegevens te bewaren wanneer deze:

1° niet gegenereerd of verwerkt worden door de betrokken operatoren;

2° niet gegenereerd of verwerkt worden binnen de geografische zones bepaald in paragraaf 3.

Doeleinden van de bewaring

Paragraaf 1 bepaalt ook dat de gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

In dit verband kan worden opgemerkt dat onder het doel van de strijd tegen zware criminaliteit waarvoor deze gegevens worden bewaard en kunnen worden opgevraagd, ook een onderzoek naar marktmisbruik door de auditeur van de FSMA valt. Inbreuken op het verbod op marktmisbruik (artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik)), maken immers een ernstig misdrijf uit

constituent en effet un délit grave (voir également le commentaire des articles 11 et 33 du présent projet de loi). Leur impact sur l'intégrité des marchés financiers et sur la confiance des investisseurs est en effet considérable. Il s'agit au sein du secteur financier, de l'une des infractions les plus graves, comme en témoignent également le fait que le règlement relatif aux abus de marché exige pour ces infractions des amendes maximales d'un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement et à la plupart des autres législations financières européennes, et le fait que la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché exige que les États membres prévoient également des sanctions pénales pour les abus de marché (élaborées dans les articles 39 et 40 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, qui prévoient des peines d'emprisonnement maximales de quatre ans, et de quatre et deux ans respectivement).

Concernant la finalité relative à la sauvegarde des intérêts vitaux de la personne concernée, le Conseil d'État dans son avis 69.381/4 du 28 juin 2021 fait remarquerqu' "il y a lieu de constater qu'elle relève d'un autre contexte que celui des questions préjudicielles auxquelles la Cour de Justice a répondu dans son arrêt La Quadrature du Net" et qu' "en tout état de cause, une telle finalité peut, à priori, être considérée comme relevant de la sauvegarde de la sécurité publique et des obligations positives incombant à ce titre aux États membres, en vue de garantir la vie et la sécurité des personnes" (p. 52).

Paragraphe 2: Les données à conserver

Le paragraphe 2 de l'article 126/1 énumère les catégories de données qui doivent être conservées par les opérateurs. Ce paragraphe reprend essentiellement les mêmes catégories de données que celles prévues à l'ancien article 126, annulé par la Cour constitutionnelle, à l'exception des données de connexion en dehors de toute communication. L'on peut se référer, à cet égard, à l'exposé des motifs de la loi du 29 mai 2016 (Doc. Parl., Chambre, 54-1567/001, p. 27). Les données ressortant de ces catégories sont déterminées par le Roi. Cet arrêté royal existe déjà: il s'agit de l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques. Cet arrêté royal sera modifié pour couvrir aussi les données de la 5G. Des adaptations seront également effectuées en conséquence de la portée plus réduite de l'article 126 (données d'identification) et du nouvel article 126/1 (autres données de trafic et de localisation).

(zie ook de toelichting bij artikelen 11 en 33 van onderhavig wetsontwerp). De impact daarvan op de integriteit van de financiële markten en het vertrouwen van de beleggers is immers groot. Binnen de financiële sector gaat het om één van de meest ernstige inbreuken, wat o.m. blijkt uit het feit dat de Verordening marktmisbruik voor deze inbreuken aanzienlijk hogere minimale maximumboetes vereist dan voor de inbreuken op andere bepalingen van de verordening en op de meeste andere Europese financiële wetgeving, alsook uit het feit dat Richtlijn 2014/57/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende strafrechtelijke sancties voor marktmisbruik de lidstaten oplegt om voor marktmisbruik ook strafrechtelijke sancties te voorzien (uitgewerkt in de artikelen 39 en 40 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, die voorzien in maximale gevangenisstraffen van vier jaar, respectievelijk vier en twee jaar).

Voor wat betreft het doeleinde m.b.t. de bescherming van de vitale belangen van de betrokken persoon, merkt de Raad van State op in zijn advies 69.381/4 van 28 juni 2021 dat het "valt evenwel op te merken dat het deel uitmaakt van een andere context dan die van de prejudiciële vragen waarop het Hof van Justitie geantwoord heeft in zijn arrest La Quadrature du Net", en dat "een dergelijk doeleinde kan hoe dan ook a priori geacht worden te vallen onder de bescherming van de openbare veiligheid en onder de positieve verplichtingen die in dat verband op de lidstaten rusten ter bescherming van het leven en de veiligheid van personen".

Paragraaf 2: De te bewaren gegevens

In paragraaf 2 van het artikel 126/1 worden de categorieën van gegevens opgesomd die door de operatoren bewaard zullen worden. Deze paragraaf omvat in wezen dezelfde categorieën van gegevens als in het vroegere artikel 126, dat door het Grondwettelijk Hof nietig is verklaard, met uitzondering van de verbindingsgegevens buiten elke communicatie. Er kan verwezen worden naar de memorie van toelichting bij de wet van 29 mei 2016 (Parl. St., Kamer, 54-1567/001, p. 27)). De gegevens die tot deze categorieën behoren, worden bepaald door de Koning. Dit koninklijk besluit bestaat al: het gaat om het Koninklijk Besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Dit koninklijk besluit zal aangepast worden om de 5G-gegevens te omvatten. Er zullen ook aanpassingen worden aangebracht als gevolg van het beperktere toepassingsgebied van artikel 126 (identificatiegegevens) en het nieuwe artikel 126/1 (andere verkeers- en locatiegegevens).

Pour ce qui concerne les métadonnées de communications électroniques, il est rappelé explicitement que l'article ne couvre pas le contenu des communications. Le terme "métadonnées" exclut d'office le contenu des communications. Par conséquent, la conservation du contenu de la communication n'est pas possible.

L'alinéa 2 du deuxième paragraphe fait référence à un arrêté royal dans lequel peuvent être déterminées les exigences auxquelles ces données doivent correspondre.

Paragraphe 3

Les catégories de lieux où il peut y avoir une conservation de données: introduction

Il est premièrement important de rappeler que l'identification dans la loi des catégories de lieux et des lieux où il peut y avoir une conservation des données implique, ipso facto, qu'il n'y a plus de conservation générale et indifférenciée de données de localisation ou de trafic puisque la détermination de ces lieux et de la durée de conservation des données y relative amènent en droit et en fait à cibler la conservation des données réalisée à titre préventif.

Deuxièmement, le critère géographique suggéré par la Cour de Justice de l'Union européenne est utilisé dans le présent article de deux façons complémentaires.

Il permet d'une part, de circonscrire les lieux caractérisés, comme le précise le point 150 de l'arrêt, par "un nombre élevé d'actes de criminalité grave" et d'autre part d'énumérer les lieux stratégiques, qui nécessitent de par leur nature (leur affectation, leur caractéristique, leur symbolique) une protection, notamment via l'instauration d'une conservation de données sur ces lieux car ils pourraient être la cible d'actes de criminalité grave ou être exposés à des menaces pour la sécurité nationale.

La détermination des zones géographiques

En fonction des hypothèses visées dans le paragraphe 3, la zone géographique sera définie par:

— un ou plusieurs arrondissements (§ 3, alinéa 1er, 1°, 1er tiret);

— une ou plusieurs zones de police (§ 3, alinéa 1er, 1°, second tiret);

— une ou plusieurs communes (par exemple dans le cadre des infrastructures critiques);

Voor wat betreft de elektronische communicatiemetagegevens wordt overigens uitdrukkelijk herhaald dat het artikel geen betrekking heeft op de inhoud van communicaties. Het woord "metagegevens" sluit sowieso de inhoud van de communcatie uit. De bewaring van de inhoud van de communicatie is dus niet mogelijk.

Het tweede lid van paragraaf 2 verwijst naar een koninklijk besluit waarin de vereisten waaraan deze gegevens moeten beantwoorden bepaald kunnen worden.

Paragraaf 3

Categorieën van plaatsen waar gegevens kunnen worden opgeslagen: inleiding

In de eerste plaats is het belangrijk eraan te herinneren dat de identificatie in de wet van de categorieën van plaatsen en van de plaatsen waar gegevens mogen worden bewaard, ipso facto impliceert dat er geen sprake meer is van een algemene en ongedifferentieerde bewaring van locatie- of verkeersgegevens, aangezien de vaststelling van deze plaatsen en van de duur van de bewaring van de daarop betrekking hebbende gegevens in rechte en in de feiten leidt tot een gerichte gegevensbewaring op preventieve basis.

Ten tweede wordt het door het Europese Hof van Justitie voorgestelde geografische criterium in dit artikel op twee complementaire manieren gebruikt.

Enerzijds kunnen zo, zoals in punt 150 van het arrest wordt gesteld, plaatsen worden aangewezen die worden gekenmerkt door "een groot aantal daden van zware criminaliteit", en anderzijds kunnen strategische plaatsen worden aangewezen die wegens hun aard (gebruik, kenmerken of symboliek) bescherming behoeven, met name door de invoering van de bewaring van gegevens op deze plaatsen, omdat zij het doelwit kunnen zijn van zware criminaliteit of blootgesteld kunnen worden aan bedreigingen van de nationale veiligheid.

Bepaling van de geografische gebieden

Afhankelijk van de veronderstellingen in paragraaf 3 wordt het geografische gebied gedefinieerd door:

— een of meer arrondissementen (§ 3, 1e lid, 1°, eerste streepje);

— een of meer politiezones (§ 3, 1e lid, 1°, tweede streepje);

— een of meer gemeenten (bijvoorbeeld in het kader van de kritieke infrastructuren);

— une adresse ou plusieurs adresses (par ex: une ambassade ou un domaine provincial).

Comme le paragraphe 5 le précise, le Roi déterminera les paramètres techniques qu'un opérateur de réseau mobile (1), et un opérateur de réseau fixe (2) utilisent pour limiter la conservation de données aux zones visées au paragraphe 3.

Le premier critère géographique: la conservation sur la base de lieux caractérisés par un nombre élevé d'actes de criminalité grave

Comme nous l'avons déjà énoncé, les données conservées sur la base de ce projet de loi sont très importantes au niveau de la réalisation de la politique criminelle. En effet, elles permettent notamment d'établir dans le cadre de crimes violents (meurtres, viols, enlèvements, carjacking), qui était actif dans la région autour des scènes de crimes, de pouvoir localiser le téléphone portable utilisé et le moment de son utilisation, ou encore d'identifier un téléphone portable utilisé au moment des faits (en utilisant par exemple la localisation basée sur les antennes). À l'identique, dans le cadre de recherches liées à un réseau d'auteurs, il est nécessaire pour les enquêteurs, de déterminer sur la base des données conservées, qui a été en contact avec qui et où se trouvent les lieux de rencontre possibles.

Il est dès lors tout à fait logique qu'un critère lié à la commission d'infractions soit retenu dans le présent projet. Il serait par contre non fondé et totalement arbitraire de choisir *a priori* de n'imposer la conservation que de certaines de données énumérées au paragraphe 2. En effet, comme les exemples énumérés ci-dessus le montrent, tant les données de localisation que celles du trafic sont nécessaires à la réalisation des enquêtes. Il va cependant de soi que, dans le cadre des requêtes faites aux opérateurs, le magistrat peut bien entendu cibler sa demande.

Afin de déterminer les lieux caractérisés par un haut taux de criminalité grave, pour lesquels une conservation des données de trafic et de localisation est prévue, le législateur a choisi de retenir les arrondissements judiciaires et/ou les zones de police où au moins 3 faits visés à l'article 90*ter*, §§ 2 à 4 du Code d'Instruction Criminelle par an et par 1 000 habitants sont constatés sur une moyenne de 3 ans.

Il ressort des différents avis reçus que des questions, des craintes et des incompréhensions relatives à ce premier critère subsistent. Il est dès lors essentiel d'expliquer davantage les différents aspects de ce critère tels que le

— een adres of verscheidene adressen (b.v. een ambassade of een provinciaal domein).

Zoals vermeld in paragraaf 5, zal de Koning de technische parameters bepalen die een operator van een mobiel netwerk (1), en een operator van een vast netwerk (2) gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones.

Het eerste geografische criterium: retentie op basis van plaatsen die worden gekenmerkt door een hoog aantal daden van zware criminaliteit

Zoals reeds aangehaald, zijn de gegevens die op basis van dit wetsontwerp bewaard worden van groot belang voor de uitvoering van het strafrechtelijk beleid. In het geval van geweldmisdrijven (moorden, verkrachtingen, ontvoeringen, carjackings) kunnen de bewaarde gegevens worden gebruikt om na te gaan wie actief was in de omgeving van de plaats van het misdrijf, om de gebruikte mobiele telefoon te lokaliseren en wanneer deze is gebruikt, of om nog een mobiele telefoon te identificeren die in gebruik was op het tijdstip van het misdrijf (bijvoorbeeld door gebruik te maken van locatiebepaling op basis van de antennes). Evenzo moeten de onderzoekers bij het onderzoek naar een dadernetwerk op basis van de bewaarde gegevens bepalen wie met wie contact heeft gehad en waar de mogelijke ontmoetingsplaatsen zijn.

Het is dan ook niet meer dan logisch dat een criterium dat verband houdt met het plegen van strafbare feiten in dit ontwerp wordt weerhouden. Anderzijds zou het ongegrond en volstrekt willekeurig zijn om *a priori* te kiezen voor het bewaren van slechts een deel van de gegevens die zijn opgesomd in paragraaf 2. Zoals uit de hierboven genoemde voorbeelden blijkt, zijn immers zowel locatiegegevens als verkeersgegevens noodzakelijk voor onderzoeken. Het spreekt voor zich dat de magistraat, in het kader van verzoeken aan operatoren, zijn verzoek uiteraard kan toespitsen.

Om de plaatsen die gekenmerkt worden door een hoog percentage ernstige criminaliteit te bepalen, waarvoor de bewaring van verkeers- en locatiegegevens voorzien wordt is, heeft de wetgever ervoor gekozen de gerechtelijke arrondissementen en/of politiezones te behouden waar gemiddeld over een periode van drie jaar, ten minste 3 feiten bedoeld in artikel 90*ter*, §§ 2 tot 4 van het Wetboek van Strafvordering per jaar en per 1 000 inwoners vastgesteld zijn.

Uit de verschillende ontvangen adviezen blijkt dat er ten aanzien van dit eerste criterium nog steeds vragen, twijfels en misverstanden bestaan. Het is dan ook van essentieel belang de verschillende aspecten van dit

choix de la méthode pour définir les zones à haut taux de criminalité, la durée de conservation des données selon le taux de criminalité, l'étendue géographique de la zone et la provenance des statistiques.

Le choix du seuil de 3 faits visés à l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle par an, par 1 000 habitants et sur une moyenne de 3 ans

Le recours aux constatations de faits visés à l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle s'explique par le fait que ces paragraphes reprennent la liste des formes de criminalité généralement considérées comme les plus graves.

L'article 90*ter* reprend notamment des infractions:

— qui sont liées à la criminalité grave contre les personnes: par exemple: attentat à la pudeur sur mineur et majeur et viol, enlèvement et recel de mineur, harcèlement par communications électroniques; ou

— qui sont liées à la criminalité organisée (par ex organisation criminelle, traite des êtres humains, incitation à la débauche, l'embauche en vue de la débauche, le proxénétisme et la tenue de maison de débauche ainsi que l'offre et la vente (et non la simple détention) de matériel pédopornographique);

— ou encore d'autres infractions particulièrement graves qui permettent de mettre en branle des méthodes spécifiques de recueil d'information (par exemple, infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes, vol et extorsion de matières nucléaires et protection physique des matières nucléaires).

La liste des infractions visées à l'article 90*ter*, §§ 2 à 4 est utilisée à plusieurs reprises dans le Code d'instruction criminelle comme seuil de l'exigence de proportionnalité en ce qui concerne les mesures d'enquête les plus attentatoires à la vie privée. C'est le cas, entre autres, pour:

— la recherche proactive (article 28*bis*, § 2);

— le blocage des comptes bancaires (article 46*quater*, § 2, alinéa 2);

— le contrôle visuel discret (article 46quinquis/89*ter*);

criterium nader toe te lichten, zoals de keuze van de methode voor het definiëren van zones met een hoge criminaliteit, de duur van de periode waarvoor gegevens worden bijgehouden op basis van de hoogte van de criminaliteit, de geografische omvang van de zone en de bron van de statistieken.

De keuze van de drempel van 3 feiten bedoeld in artikel 90*ter*, §§ 2 tot 4 van het Wetboek van strafvordering per jaar, per 1 000 inwoners en over een gemiddelde van 3 jaar

De reden waarom er beroep gedaan wordt op vastgestelde feiten bedoeld in artikel 90*ter*, §§ 2-4 van het Wetboek van Strafvordering wordt verklaard door het feit dat in deze paragrafen de vormen van criminaliteit worden opgesomd die over het algemeen als de ernstigste worden beschouwd.

Artikel 90*ter* omvat namelijk strafbare feiten:

— die verband houden met zware criminaliteit tegen personen: bijvoorbeeld aanranding van minderjarigen en volwassenen en verkrachting, ontvoering en verberging van minderjarigen, belaging via elektronische communicatie; of

— die verband houden met de georganiseerde criminaliteit (bijvoorbeeld criminele organisatie, mensenhandel, aanzetten tot ontucht, tewerkstelling met het oog op ontucht, pooierschap en het houden van een bordeel, en de aanbieding en verkoop (niet louter het bezit) van kinderpornografie);

— of andere bijzonder ernstige inbreuken die specifieke methoden voor het vergaren van informatie in beweging zetten (bijvoorbeeld inbreuken tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen en de door die systemen opgeslagen, verwerkte of doorgegeven gegevens, diefstal en afpersing van nucleair materiaal en fysieke beveiliging van nucleair materiaal).

De lijst van strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4 wordt in het Wetboek van strafvordering meerdere keren gebruikt als drempel voor de proportionaliteitsvereiste voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer. Dit is o.a. het geval voor:

— de proactieve recherche (artikel 28*bis*, § 2);

— het blokkeren van banktegoeden (artikel 46*quater*, § 2, tweede lid);

— de inkijkoperatie (artikel 46*quinquies*/89*ter*);

— l'infiltration (article 47*octies*);

— l'observation à l'aide de moyens techniques afin d'avoir une vue dans un domicile d'un médecin ou d'un avocat (article 56*bis*);

— l'anonymat complet des témoins (article 86*bis*);

— l'interception et la prise de connaissance de communications non accessibles au public ou la recherche secrète dans un système informatique (article 90*ter*);

— l'octroi de mesures de protection spéciales aux témoins menacés (article 104, § 2);

— l'octroi de mesures de protection spéciales aux personnes menacées qui exercent une fonction publique (article 111*quater*, § 1er, alinéa 2).

Pour l'application des mesures d'enquête les plus drastiques, la liste des infractions énumérées à l'article 90*ter*, §§ 2 à 4 est toujours utilisée.

Le législateur estime que se baser sur le nombre de faits qui sont actuellement considérés comme les plus graves est un bon indicateur pour déterminer les zones avec une forte criminalité.

À propos de ce critère statistique et du recours à l'article 90*ter*, l'Organe de contrôle de l'information policière (ci-après "COC") note dans le point 15 de son avis que "Le COC n'a pas de remarques particulières à ce sujet et comprend que les rédacteurs de l'avant-projet ont ainsi cherché au maximum à obtenir des critères objectifs en ligne avec la jurisprudence précitée de la Cour de Justice de l'UE. Il est évident que ce faisant, on tente également d'instaurer des critères réutilisables. Les descriptions territoriales des arrondissements judiciaires et des zones de police sont des descriptions connues avec lesquelles on peut rapidement se mettre au travail. Ladite "liste des écoutes" de l'art. 90*ter* C.i.cr. est, de lege lata, en droit belge le seul véritable critère utilisable pour pouvoir différencier lesdits "délits graves" de la criminalité ordinaire".

Dans son avis, l'APD déclare au point 121 "l'Autorité prend note du choix du demandeur d'utiliser cette liste pour définir ce qui relève de la criminalité grave". C'est une mauvaise interprétation de la volonté du législateur: en fait, le recours à cette liste a uniquement pour objectif de servir comme indicateur pour déterminer les zones avec un taux élevé de criminalité grave. Si la liste de l'article 90*ter*, §§ 2 à 4 reprend les infractions généralement considérées comme les plus graves, cela n'empêche pas que des infractions hors de cette

— de infiltratie (artikel 47*octies*);

— de observatie met gebruik van technische middelen om zicht te krijgen in de woning van een advocaat of een arts (artikel 56*bis*);

— de volledige anonimiteit van getuigen (artikel 86*bis*);

— de onderschepping en kennisname van communicatie die niet toegankelijk is voor het publiek en de geheime zoeking in een informaticasysteem (artikel 90*ter*);

— het toekennen van bijzondere beschermingsmaatregelen aan bedreigde getuigen (artikel 104, § 2);

— het toekennen van bijzondere beschermingsmaatregelen aan bedreigde personen die een openbaar ambt uitoefenen (artikel 111*quater*, § 1, tweede lid);

Voor het toepassen van de meest ingrijpende opsporingsmethoden wordt dus telkens teruggegrepen naar de lijst van strafbare feiten opgesomd in artikel 90*ter*, §§ 2 tot 4.

De wetgever is van mening dat het gebruik van het aantal feiten die momenteel als de meest ernstige worden beschouwd, een goede indicator is voor het bepalen van de zones met een hoge criminaliteit.

Met betrekking tot dit statistische criterium en het gebruik van artikel 90*ter* merkt het Controleorgaan op de politionele informatie (hierna "COC") in punt 15 van zijn advies het volgende op: "Het COC heeft hier geen bijzondere opmerkingen en begrijpt dat de stellers van het voorontwerp zo maximaal mogelijk hebben gezocht naar objectieve criteria in lijn met voormelde rechtspraak van het U Hof van Justitie. Dat daarbij getracht is ook praktisch haalbare criteria in te voeren ligt voor de hand. De territoriale omschrijvingen van de gerechtelijke arrondissementen en politiezones zijn gekende omschrijvingen waarmee men snel aan de slag kan. De zgn. "taplijst" van art. 90*ter* Sv. Is de lege lata naar Belgisch recht het enige echt bruikbare criterium om zgn. "zware misdrijven" te kunnen onderscheiden van "gewone criminaliteit"."

In zijn advies verklaart de GBA in punt 121: "De Autoriteit neemt nota van de keuze van de aanvrager om aan de hand van deze lijst te bepalen welke strafbare feiten onder de noemer "zware criminaliteit" vallen". Dit is een verkeerde interpretatie van de bedoeling van de wetgever: in feite is het gebruik van deze lijst alleen bedoeld als een indicator voor het bepalen van gebieden met een hoog aantal feiten van zware criminaliteit. Hoewel de lijst van artikel 90*ter*, §§ 2 tot en met 4, de strafbare feiten bevat die over het algemeen als de

liste pourraient également être estimées comme ayant un degré de gravité suffisant par rapport à l'ingérence qu'induit cette mesure de conservation.

La Cour de Justice de l'Union européenne ne donne pas de définition de la notion de "criminalité grave". Il n'existe pas non plus de définition autonome de la notion de "criminalité grave" dans le droit de l'Union. Il appartient aux États membres de l'Union européenne de le déterminer. Le droit pénal et la procédure pénale relèvent de la compétence des États membres. La qualification pénale peut donc varier entre les États membres en fonction des traditions, des priorités, de la politique pénale, de l'évolution de la criminalité et des développements sociaux.

Toutefois, dans ses conclusions relatives à l'arrêt Ministerio Fiscal du 2 octobre 2018, l'avocat général près la Cour de Justice, a donné quelques indications sur la manière dont la notion de criminalité grave pourrait être interprétée en droit national:

"La notion d'infractions graves a été employée par la Cour dans l'arrêt Digital Rights, parfois en combinaison avec la notion de "criminalité grave", en tant que critère de vérification de la finalité et de la proportionnalité de l'ingérence dans les droits fondamentaux susmentionnés qui était entraînée par des dispositions du droit de l'Union relatives aux données à caractère personnel, à savoir celles de la directive 2006/24". Il ajoute que "La Cour a par la suite fait usage de ces deux notions dans l'arrêt Tele2, en tant que même critère d'appréciation, mais concernant cette fois la conformité au droit de l'Union de dispositions adoptées par des États membres".

Pour l'avocat général, la notion de criminalité grave est une notion dynamique, qui se veut évolutive. Par exemple, il indique que la gravité d'une infraction pénale ne dépend pas seulement du niveau de la sanction. Le fait qu'un État membre prévoit un taux d'emprisonnement peu élevé, voire une peine alternative, n'enlève donc rien à la gravité intrinsèque du type d'infraction concerné. D'autres facteurs peuvent entrer en ligne de compte tels que le contexte de l'infraction présumée (caractère intentionnel, circonstances aggravantes, récidive, etc.), les intérêts de la société affectés par l'auteur de l'infraction, la nature et/ou le degré du préjudice subi par la victime de l'infraction, ou l'échelle des peines généralement applicable dans l'État membre concerné.

Sur ce sujet, le Conseil d'État français a estimé dans son arrêt du 21 avril 2021: "il ne résulte pas des énonciations de l'arrêt de la Cour de justice de l'Union européenne que le législateur serait tenu d'énumérer les infractions

ernstigste worden beschouwd, sluit dit niet uit dat ook strafbare feiten buiten deze lijst kunnen worden geacht een voldoende mate van ernst te hebben in verhouding tot de door deze gegevensbewaring teweeggebrachte inmenging.

Het Europese Hof van Justitie geeft geen definitie van het begrip "zware criminaliteit". Ook in het Unierecht bestaat er geen autonome definitie van het begrip "zware criminaliteit". Het is aan de lidstaten zelf van de Europese Unie om dit te bepalen. Het strafrecht en het strafprocesrecht behoren tot de bevoegdheid van de lidstaten. De strafrechtelijke kwalificatie kan zo verschillen tussen lidstaten onderling, in functie van tradities, prioriteiten, strafrechtelijk beleid, de evolutie van de criminaliteit en maatschappelijke ontwikkelingen.

In zijn conclusies over het arrest Ministerio Fiscal van 2 oktober 2018 heeft de advocaat-generaal bij het Hof van Justitie echter enkele aanwijzingen gegeven over de wijze waarop het begrip zware criminaliteit in het nationale recht kan worden uitgelegd:

"Het Hof in het arrest Digital Rights het begrip "ernstige criminaliteit", soms afgewisseld met het begrip "zware criminaliteit", heeft gebruikt als criterium ter beoordeling van het doel en de evenredigheid van de inmenging in de bedoelde grondrechten die werd veroorzaakt door Unierechtelijke bepalingen betreffende persoonsgegevens, te weten de bepalingen van Richtlijn 2006/24." Hij voegt daaraan toe dat "Het Hof heeft deze twee begrippen vervolgens als zelfde beoordelingscriterium gebruikt in het arrest Tele2, zij het in dit geval aangaande de verenigbaarheid met het Unierecht van door de lidstaten vastgestelde maatregelen".

Voor de advocaat-generaal is het begrip zware criminaliteit een dynamisch en evolutief begrip. Zo geeft hij aan dat de ernst van een strafbaar feit niet alleen afhangt van de hoogte van de straf. Het feit dat een lidstaat voorziet in een lage gevangenisstraf, of zelfs een alternatieve straf, doet dus niets af aan de intrinsieke ernst van het betrokken soort strafbaar feit. Er moet ook gekeken worden naar andere factoren, zoals de context van het vermeende strafbare feit (opzet, verzwarende omstandigheden, recidive, …), de belangen van de samenleving die door de dader geraakt worden, de aard en/of de omvang van de schade die het slachtoffer van het strafbare feit heeft geleden, of ook de in de betrokken lidstaat algemeen toepasselijke schaal van sancties.

In dit verband heeft de Franse Raad van State in zijn arrest van 21 april 2021 het volgende overwogen: "Uit de bewoordingen in het arrest van het Hof van Justitie van de Europese Unie volgt niet dat de wetgever verplicht zou

relevant du champ de la criminalité grave en se référant à des catégories strictement prédéfinies en droit interne. Le rattachement d'une infraction pénale à la criminalité grave a donc vocation à s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce. Une obligation de conservation généralisée et indifférenciée des adresses IP peut ainsi être imposée aux opérateurs, dès lors que les conditions d'accès à ces données par les services d'enquête sont fixées en fonction de la gravité des infractions susceptibles de le justifier, dans le respect du principe de proportionnalité, lequel fait partie des principes généraux du droit de l'Union européenne."

En Belgique, l'accès des autorités judiciaires aux données de trafic et de localisation à des fins de recherche, de détection et de poursuite d'infractions pénales d'une certaine gravité est réglementé par l'article 88*bis* du Code d'instruction criminelle. Outre des modalités procédurales et matérielles, des conditions d'accès y sont fixées dont le degré de gravité de l'infraction, qui justifie la mesure. Il y est, entre autres, prévu que le juge d'instruction puisse prendre la mesure uniquement s'il existe des indices sérieux que l'infraction est de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsqu'il estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité. Par ailleurs, le juge d'instruction doit indiquer dans une ordonnance motivée les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête.

Concernant le choix du seuil d'un minimum de 3 faits "90*ter*, §§ 2 à 4" par 1 000 habitants, le législateur a décidé de ne pas prendre un chiffre absolu qui serait identique pour tous ces lieux.

Afin de tenir compte du principe de proportionnalité, il est en effet préférable d'opérer pour chaque lieu une pondération propre à sa situation criminogène. Ce seuil de criminalité grave, calculé par 1 000 habitants permet donc de tenir compte de la réalité objective des phénomènes criminels au sein de chaque arrondissement, tout en permettant d'assurer une égalité de traitement pour l'ensemble de la population. En d'autres termes, ce critère permet de rencontrer le prescrit de la Cour de

zijn de strafbare feiten die onder de zware criminaliteit vallen, op te sommen onder verwijzing naar categorieën die in het nationale recht strikt vooraf zijn omschreven. De kwalificatie van een strafbaar feit als ernstig misdrijf moet dus concreet worden beoordeeld, onder toezicht van de strafrechter, in het licht van de aard van het gepleegde feit en van het geheel van feiten van de zaak. Aldus kan aan de operatoren een algemene en ongedifferentieerde verplichting tot bewaring van IP-adressen worden opgelegd, mits de voorwaarden voor toegang tot die gegevens door de opsporingsautoriteiten worden bepaald naar gelang van de ernst van de strafbare feiten die zulks kunnen rechtvaardigen, met inachtneming van het evenredigheidsbeginsel, dat een van de algemene beginselen van het recht van de Europese Unie is." (eigen vertaling)

In België is de toegang van gerechtelijke autoriteiten tot verkeers- en locatiegegevens met het oog op het onderzoeken, opsporen en vervolgen van strafbare feiten van een zekere ernst geregeld in artikel 88*bis* van het Wetboek van strafvordering. Naast de procedurele en materiële modaliteiten worden voorwaarden voor toegang vastgesteld, waaronder de mate van ernst van het strafbare feit, die de maatregel rechtvaardigt. Daarin is onder meer bepaald dat de onderzoeksrechter de maatregel enkel kan nemen wanneer er ernstige aanwijzingen zijn dat het strafbare feit een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kan hebben en wanneer hij van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen. Voorts moet de onderzoeksrechter in een met redenen omklede beschikking de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

Wat de keuze van de drempel van minimaal 3 feiten "90*ter*, §§ 2 tot 4" per 1 000 inwoners betreft, heeft de wetgever besloten geen absoluut cijfer te nemen dat voor al deze plaatsen identiek zou zijn.

Teneinde rekening te houden met het evenredigheidsbeginsel verdient het inderdaad de voorkeur elke plaats te wegen naar gelang van de criminogene situatie ervan. Deze drempel voor zware criminaliteit, berekend per 1 000 inwoners, maakt het dus mogelijk rekening te houden met de objectieve realiteit van de criminele fenomenen binnen elk arrondissement, en tegelijkertijd de gelijke behandeling van de gehele bevolking te waarborgen. Met andere woorden, dit criterium maakt

Justice et de la Cour constitutionnelle exigeant la mise en œuvre des critères objectifs et non discriminatoires.

En outre, un seuil annuel de 3 faits graves de la liste de l'article 90*ter*, §§ 2 à 4 par 1 000 habitants sur une moyenne de 3 ans permet de lisser les pics et les chutes de criminalité, qui seraient dus à des épiphénomènes et permet donc d'objectiver ce seuil.

La production annuelle de statistiques implique que ce critère est dynamique puisqu'il dépend des chiffres de criminalité repris soit au niveau d'un arrondissement, soit au niveau d'une zone de police. La période de référence de 3 ans permet d'avoir des statistiques suffisamment significatives tout en fournissant une image actuelle des chiffres de criminalité.

Ainsi, ce seuil, calculé par 1 000 habitants permet de tenir compte de la réalité divergente des phénomènes criminels au sein des différents arrondissements.

Illustrons ce propos:

Pour l'arrondissement le plus peuplé, soit l'arrondissement d'Anvers (1 869 730 habitants en 2019), ce seuil revient à dire qu'il faut qu'il y ait eu en moyenne sur les 3 dernières années 5 609 faits graves. Autrement formulé, sur les 3 dernières années, 16 827 faits graves se sont déroulés à Anvers.

Pour l'arrondissement de Bruxelles, (1 218 255 habitants en 2019), ce seuil revient à dire qu'il faut qu'il y ait eu, en moyenne sur les 3 dernières années 3 655 faits graves. En d'autres termes, sur les 3 dernières années, 10 965 faits graves se sont déroulés à Bruxelles.

Pour l'arrondissement le moins peuplé, Eupen (77 949 habitants en 2019), ce seuil implique qu'il y ait eu, en moyenne sur les 3 dernières années 234 faits graves, soit, sur un total de 3 ans, 702 faits graves.

Pour un arrondissement comme Charleroi (583 928 habitants en 2019) ou Mons (762 912 habitants en 2019) ceci implique qu'il y ait eu respectivement 1 752 et 2 889 faits en moyenne sur les 3 dernières années ou sur un total de 3 ans, 5 256 et 8667 faits graves.

Pour un arrondissement comme Namur par exemple (495 832 habitants en 2019), ceci implique qu'il y ait eu respectivement 1 487 faits en moyenne sur les 3 dernières années ou sur un total de 3 ans, 4 461 faits graves.

het mogelijk te voldoen aan de eisen van het Hof van Justitie en het Grondwettelijk Hof, die de toepassing van objectieve en niet-discriminerende criteria vereisen.

Bovendien, een jaarlijkse drempel van gemiddeld 3 ernstige strafbare feiten van de lijst van artikel 90*ter*, §§ 2 tot 4 per 1 000 inwoners over een periode van 3 jaar maakt het mogelijk pieken en dalen in de criminaliteit die aan tijdelijke fenomenen te wijten zouden zijn uit te vlakken en laat dus toe om de drempel te objectiveren.

De jaarlijkse productie van statistieken impliceert dat dit criterium dynamisch is, aangezien het afhankelijk is van de criminaliteitscijfers die hetzij op het niveau van een arrondissement, hetzij op het niveau van een politiezone worden geregistreerd. De referentieperiode van 3 jaar maakt het mogelijk voldoende betekenisvolle statistieken op te stellen en tegelijkertijd een actueel beeld van de criminaliteitscijfers te geven.

Zo laat deze drempel, berekend per 1 000 inwoners, toe om rekening te houden met de werkelijkheid van uiteenlopende criminele fenomenen in de verschillende arrondissementen.

Bijvoorbeeld:

In het dichtstbevolkte arrondissement Antwerpen (1 869 730 inwoners in 2019) houdt deze drempel in dat er in de afgelopen 3 jaar gemiddeld 5 609 zware feiten moeten zijn geweest. Met andere woorden, de voorbije 3 jaar vonden er in Antwerpen 16 827 zware feiten plaats.

In het gerechtelijk arrondissement Brussel (1 218 255 inwoners in 2019), betekent deze drempel dat er in de afgelopen drie jaar gemiddeld 3 655 zware feiten moeten zijn geweest. Met andere woorden, de afgelopen 3 jaar hebben er in Brussel 10 965 ernstige incidenten plaatsgevonden.

Voor het kleinste arrondissement, Eupen (77 949 inwoners in 2019) betekent de drempel dat er de voorbije 3 jaar gemiddeld 234 zware feiten, vastgesteld moeten zijn, of, op een totaal van 3 jaar, 702 zware feiten.

Voor Charleroi (583 928 inwoners in 2019) of Bergen (762 912 inwoners in 2019) ligt de drempel op respectievelijk gemiddeld 1 752 en 2 889 zware feiten gedurende de laatste 3 jaren of op een totaal van 3 jaar op 5 256 en 8 667 zware feiten.

Voor een arrondissement als Namen bijvoorbeeld (495 832 inwoners in 2019) ligt de drempel op respectievelijk gemiddeld 1 487 feiten gedurende de laatste 3 jaar of op een totaal van 3 jaar: 4 461 feiten.

Pour la Flandre occidentale (1 200 945 habitant en 2019), cela veut dire qu'il y ait eu, en moyenne sur les 3 dernières années 3 603 faits graves, ou sur les 3 dernières années, 10 808 faits graves.

Pour la Flandre orientale (1 525 255 habitant en 2019), cela veut dire qu'il y ait eu, en moyenne sur les 3 dernières années 4 576 faits graves ou sur les 3 ans dernières années, 13 728 faits graves.

Ces illustrations démontrent que le seuil de 3 faits de la liste de l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants correspond à un nombre élevé de faits de criminalité grave, comme illustré ci-dessus. Ce nombre élevé indique un enracinement de la criminalité grave au sein de l'arrondissement. Ce seuil a également un impact sur le sentiment d'insécurité de la population, et pour certaines infractions sur les attentes légitimes des victimes d'être assistées: qu'elle soit secourues mais également que les auteurs de l'infraction perpétrée à leur préjudice soient identifiés et poursuivis.

Ce seuil élevé est donc bien évidemment en étroite relation avec la capacité policière spécialisée nécessaire et *in fine* le nombre de demandes de collaboration qui seront introduites auprès des opérateurs.

Au niveau de l'arrondissement de Bruxelles capitale par exemple, où il y a en moyenne 16 859 infractions de la liste de l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle par an pour les 434 enquêteurs de la Police Judiciaire Fédérale, chaque enquêteur devrait en théorie traiter 39 faits par an.

Au niveau de l'arrondissement de Charleroi par exemple, où il y a en moyenne 9 532 infractions de la liste de l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle par an pour les 173 enquêteurs, chaque enquêteur devrait en théorie traiter 55 faits par an.

Sachant que:

— la valeur seuil ne tient compte que de l'enregistrement des faits de la liste de l'article 90*ter* qui ont été détectés par ou communiqués à la police et sur lesquels une capacité d'enquête est dédiée; et

— la capacité policière de recherche n'est bien entendu pas limitée aux enquêtes relatives aux faits de la liste de l'article 90*ter* mais à l'ensemble des missions de recherche spécialisées et *supra* locale;

— une enquête criminelle portant sur des faits graves peut parfois durer plusieurs mois (voir plusieurs années pour les cas véritablement complexes);

In West-Vlaanderen (1 200 945 inwoners in 2019) betekent dit dat er de voorbije 3 jaar gemiddeld 3 603 zware feiten, of gedurende de laatste 3 jaar 10 808 zware feiten, zouden moeten vastgesteld zijn.

Voor Oost-Vlaanderen (1 525 255 inwoners in 2019) komt de drempel gedurende de 3 voorbije jaren neer op gemiddeld 4 575 zware feiten of gedurende de laatste drie jaar op 13 728 ernstige feiten.

Deze illustraties tonen aan dat de drempel van 3 feiten van de lijst van artikel 90*ter*, §§ 2 tot 4 van het Wetboek van strafvordering per 1 000 inwoners beantwoordt aan een hoog aantal feiten van ernstige criminaliteit, zoals hierboven geïllustreerd. Dit hoge aantal wijst op een verankering van zware criminaliteit in het arrondissement. Deze drempel heeft ook gevolgen voor het onveiligheidsgevoel van de bevolking, en voor bepaalde misdrijven voor de legitieme verwachtingen van de slachtoffers om te worden bijgestaan: dat zij worden gered, maar ook dat de daders van het misdrijf dat tegen hen is gepleegd, worden opgespoord en vervolgd.

Deze hoge drempel hangt uiteraard nauw samen met de noodzakelijke gespecialiseerde politiecapaciteit en uiteindelijk ook met het aantal verzoeken om medewerking dat bij de operatoren zal worden ingediend.

In het arrondissement Brussel-Hoofdstad bijvoorbeeld, waar jaarlijks gemiddeld 16 859 misdrijven uit de lijst van artikel 90*ter*, §§ 2 tot 4 van het Wetboek van strafvordering worden gepleegd, voor de 434 speurders van de federale gerechtelijke politie, zou elke speurder theoretisch 39 feiten per jaar moeten behandelen.

In het arrondissement Charleroi bijvoorbeeld, waar de 173 speurders gemiddeld 9 532 inbreuken van artikel 90*ter*, §§ 2 tot 4 van het Wetboek van strafvordering per jaar moeten behandelen, zou elke speurder in theorie 55 feiten per jaar moeten behandelen.

Wetende dat:

— de drempelwaarde alleen rekening houdt met de registratie van feiten uit de lijst van artikel 90*ter* die door de politie zijn opgespoord of aan haar zijn meegedeeld en waarvoor een opsporingscapaciteit wordt ingezet; en

— de onderzoekscapaciteit van de politie uiteraard niet beperkt is tot het onderzoek van de feiten uit de lijst van artikel 90*ter*, maar tot alle gespecialiseerde en bovenlokale onderzoekstaken;

— een strafrechtelijk onderzoek naar ernstige feiten soms meerdere maanden (of zelfs jaren voor echt complexe zaken) kan duren;

— une seule enquête sur des faits graves demande la collaboration de plusieurs enquêteurs revêtant des spécialités différentes (ex: enquêteur spécialisé en matière informatique et digitale, enquêteur spécialisé en matière financière, enquêteur spécialisé en homicide, etc.);

— il existe un temps certain entre la découverte du fait lui-même (ex: la découverte du corps de la victime – préalablement signalée comme étant disparue) et les premières demandes en téléphonies dirigées vers un suspect potentiel;

— il existe, comme expliqué ci-dessus, un lien indéniable entre le nombre d'infractions constatées et le nombre d'infractions qui vont être commises dans cette zone;

— au plus le nombre de faits est élevé, au plus la charge sur les enquêteurs spécialisés est élevée et au plus les délais nécessaires pour arriver au moment de l'enquête où des requêtes pourront être adressées aux opérateurs sont longs; et

— au plus le nombre de faits est élevé, au plus le nombre de requêtes introduites auprès des autorités judiciaires compétentes sera élevé, avec son indéniable impact sur les délais de délivrance des autorisations légales.

Le seuil de 3 faits de la liste de l'article 90*ter*, §§ 2 à 4, par 1000 habitants indique donc qu'un pourcentage substantiel de la capacité d'enquête de la police judiciaire fédérale doit être réservé à ces faits vu l'enracinement de la criminalité organisée au sein de l'arrondissement.

Il est important de souligner que plus de 90 % des enquêtes portant sur la criminalité grave font appel à des données appelées de "téléphonie" et que, sauf de très rares exceptions, aucune enquête en matière de criminalité organisée ne peut se passer des données de téléphonie pour être menée à bien.

Pour répondre aux préoccupations de l'APD exprimées dans le point 122 de son avis 108/2021 du 28 juin 2021, le fait qu'un seuil de criminalité par 1 000 habitants ait été choisi et non un chiffre absolu par arrondissement/zone de police, et que ce seuil ne vise au sein de la catégorie des infractions graves, que les infractions les plus graves, soit les infractions visées à l'article 90*ter* et qu'il y ait des délais différenciés de conservation en fonction du taux de criminalité grave, permet précisément d'avoir un critère dynamique et proportionné.

— één enkel onderzoek naar ernstige feiten de samenwerking van meerdere rechercheurs met verschillende specialiteiten vereist (bijvoorbeeld computer- en digitaal rechercheur, financieel rechercheur, rechercheur moordzaken, enz.);

— er een bepaalde tijd verstrijkt tussen de ontdekking van het feit zelf (bijvoorbeeld de ontdekking van het lichaam van het slachtoffer – dat eerder als vermist was opgegeven) en de eerste telefonieonderzoeken naar een mogelijke verdachte;

— er, zoals hierboven uiteengezet, een duidelijk verband bestaat tussen het aantal overtredingen en het aantal overtredingen dat in dat gebied zal worden begaan;

— hoe groter het aantal feiten, hoe groter de last is voor gespecialiseerde onderzoekers en hoe langer de termijn zal zijn die nodig is om het punt van onderzoek te bereiken waar verzoeken aan operatoren kunnen worden gedaan; en

— hoe groter het aantal feiten, hoe groter het aantal verzoeken aan de bevoegde rechterlijke autoriteiten zal zijn, met een duidelijke impact op de tijd die nodig is om wettelijke machtigingen af te geven.

Het geeft de drempel van 3 feiten van de lijst van artikel 90*ter*, §§ 2 tot 4, per 1000 inwoners dus aan dat een aanzienlijk percentage van de onderzoekscapaciteit van de federale gerechtelijke politie aan deze feiten moet worden besteed, gezien het diepgewortelde karakter van de georganiseerde misdaad in het arrondissement.

Het is van belang erop te wijzen dat bij meer dan 90 % van de onderzoeken naar zware criminaliteit gebruik wordt gemaakt van zogenaamde "telefoniegegevens" en dat, op enkele uitzonderingen na, geen enkel onderzoek naar georganiseerde criminaliteit kan worden uitgevoerd zonder telefoniegegevens.

In antwoord op de bezorgdheid die de GBA heeft geuit in punt 122 van zijn advies 108/2021 van 28 juni 2021, zij opgemerkt dat het feit dat is gekozen voor een criminaliteitsdrempel per 1 000 inwoners en niet voor een absoluut cijfer per arrondissement/politiezone, en dat deze drempel alleen betrekking heeft op de ernstigste strafbare feiten binnen de categorie ernstige strafbare feiten, dat wil zeggen de in artikel 90*ter* bedoelde strafbare feiten, en dat er gedifferentieerde bewaartermijnen zijn naar gelang van de hoeveelheid van de strafbare feiten, het mogelijk maakt te beschikken over een dynamisch en evenredig criterium.

Cela permet également, comme nous l'avons déjà mentionné, d'objectiver un lien avec la population d'un arrondissement ou d'une zone de police: il n'y a de la conservation de données que s'il y a des signes objectifs que la criminalité grave s'est implantée de manière durable dans l'arrondissement ou la zone de police de sorte qu'il est nécessaire et proportionné dans une société démocratique de mettre en place des mécanismes permettant de lutter contre celle-ci.

Période de conservation proportionnelle au taux de criminalité

En outre, dans l'optique de tenir compte du principe de proportionnalité, la période de conservation des données est également modulée selon le seuil de faits criminels constatés, avec une durée maximale de 12 mois.

Au plus il y a une activité criminelle grave (selon l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle), au plus il y a, au sein de l'arrondissement, un enracinement des activités de criminalité organisée/grave et au plus, il est dès lors nécessaire de pouvoir investiguer le passé des communications, notamment pour établir les liens entre les différents groupes d'auteurs, dans le but de les démanteler ou, à tout le moins, de déstabiliser la criminalité organisée/grave.

De la sorte:

— Pour les arrondissements judiciaires où il y a sur une moyenne de 3 ans, à partir de 3 et jusque 4 faits visés à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle constatés par an par 1 000 habitants, le délai de conservation est de 6 mois.

— Pour les arrondissements judiciaires où il y a sur une moyenne de 3 ans, à partir de 5 et jusque 6 faits visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle constatés par an par 1 000 habitants, le délai de conservation est de 9 mois.

— Pour les arrondissements où il y a sur une moyenne de 3 ans, une moyenne égale ou supérieure à 7 faits visés à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle constatés par an par 1 000 habitants au cours des 3 dernières années, le délai de conservation est de 12 mois.

Délimitation géographique des zones

Au niveau de l'étendue géographique retenue, l'arrondissement judiciaire est le plus approprié pour tenir compte de la criminalité grave visée à l'article 90*ter* du Code d'instruction criminelle, vu que ce niveau correspond à la compétence d'un parquet du Procureur du Roi et

Het maakt ook, zoals al eerder vernoemd, een objectieve band met de bevolking van een arrondissement of politiezone mogelijk: gegevens worden alleen bewaard als er objectieve aanwijzingen zijn dat ernstige criminaliteit zich op een duurzame manier heeft ingeplant in het arrondissement of de politiezone, zodat het in een democratische samenleving noodzakelijk en evenredig is om mechanismen ter bestrijding daarvan in te voeren.

Bewaartermijn evenredig met de hoeveelheid criminaliteit

Bovendien, rekening houdend met het evenredigheidsbeginsel, wordt de termijn van de bewaarplicht veranderd volgens de drempel van vastgestelde strafbare feiten, met een maximale duur van 12 maanden.

Hoe meer zware criminaliteit (volgens artikel 90*ter*, §§ 2 tot 4 van het Wetboek van Strafvordering) hoe dieper de georganiseerde/criminele activiteiten in het arrondissement geworteld zijn, en dus hoe noodzakelijker het is om in de tijd terug te gaan, met name om verbanden te leggen tussen de verschillende dadergroepen, teneinde deze te ontmantelen of op zijn minst de georganiseerde/criminele activiteit te destabiliseren.

Dit betekent:

— Voor gerechtelijke arrondissementen waar er op basis van een gemiddelde van 3 jaar, vanaf 3 en tot 4 strafbare feiten sprake is zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering, per 1 000 inwoners per jaar, bedraagt de bewaartermijn 6 maanden.

— Voor gerechtelijke arrondissementen waar er op basis van een gemiddelde van 3 jaar, vanaf 5 en tot 6 strafbare feiten sprake is zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering, per 1 000 inwoners per jaar, bedraagt de bewaartermijn 9 maanden.

— Voor gerechtelijke arrondissementen waar sprake is van een gemiddelde gelijk aan of meer dan 7 inbreuken zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering, per 1 000 inwoners per jaar gedurende 3 jaar, bedraagt de bewaartermijn 12 maanden.

Geografische afbakening van de zones

Op het niveau van de geografische reikwijdte die wordt gehanteerd, is het arrondissementsniveau het meest geschikt om rekening te houden met de zware criminaliteit zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering, aangezien dit niveau overeenkomt met

donc à la réalisation d'une politique de répression. Les limites des arrondissements judiciaires sont d'ailleurs fixées par l'article 4 de l'annexe au Code judiciaire.

La structure de la police judiciaire fédérale suit en règle générale cette même organisation arrondissementale: il y a une direction Judiciaire d'enquête – appelée PJF – par arrondissement judiciaire, sauf pour l'arrondissement judiciaire du Hainaut qui a deux PJF (celles de Mons et Charleroi) et l'arrondissement judiciaire de Bruxelles qui a deux PJF (celles de Halle-Vilvorde et Bruxelles).

Or, c'est cette même PJF qui est chargée des enquêtes concernant les infractions les plus graves commis sur son arrondissement judiciaire; ce sont ces faits qui sont repris dans l'article 90*ter* du Code d'instruction criminelle.

Si ce seuil n'est pas atteint au niveau d'un arrondissement et que donc, il n'y a pas de raison objective de réaliser une conservation préventive des données de trafic et de localisation au sein de cet arrondissement, alors la conservation des données de trafic et de localisation se fait uniquement à plus petite échelle et au niveau de la/les zones de police dans laquelle/lesquelles, par 1 000 habitants par an au cours des 3 dernières années au moins 3 infractions visées à l'article 90*ter* du Code d'instruction criminelle ont été répertoriées. La délimitation des zones de police se trouve dans l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

À l'image de ce qui se passe au niveau arrondissemental, le délai de conservation est de 6 mois lorsque le nombre de faits visés à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an (sur une moyenne de 3ans) est de 3 ou 4, de 9 mois, lorsque le nombre est de 5 ou 6 et de 12 mois lorsqu'il y a au moins 7 faits visés à l'art. 90*ter* du Code d'instruction criminelle.

La délimitation géographique sur la base des arrondissements judicaires d'une part ou des zones de police d'autre part constitue un tout cohérent par rapport à la lutte concrète et quotidienne que mène tant les acteurs de la police que de ceux de la justice contre les phénomènes criminels , de sorte que, comme l'indique le C.O.C dans le point 17 de son avis "la description géographique de l'arrondissement et de la zone de police est rationnelle et logique en fonction de l'organisation étatique, judiciaire et policière.".

À cet égard, il faut aussi noter que les groupes d'auteurs sont, par ailleurs, très mobiles et se déplacent et

de bevoegdheid van een parket van een Procureur des Konings en dus met de uitvoering van een rechtshandhavingsbeleid. De grenzen van de gerechtelijke arrondissementen zijn overigens vastgelegd in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De structuur van de federale gerechtelijke politie volgt over het algemeen dezelfde arrondissementele organisatie: er is één Federale gerechtelijke Politie – FGP genoemd – per gerechtelijk arrondissement, behalve voor het gerechtelijk arrondissement Henegouwen, die twee FGP's heeft (Bergen en Charleroi) en het gerechtelijk arrondissement van Brussel, die ook twee FGP's heeft (Halle-Vilvoorde en Brussel).

Deze zelfde FGP is verantwoordelijk voor onderzoeken naar de ernstigste misdrijven die in zijn gerechtelijk arrondissement zijn gepleegd; dit zijn de feiten die zijn opgenomen in artikel 90*ter* wetboek van strafvordering.

Indien deze drempel niet wordt bereikt op het niveau van een arrondissement en er dus geen objectieve reden is om in dit arrondissement een preventieve bewaring van verkeers- en locatiegegevens op te leggen, worden de verkeers- en locatiegegevens alleen bewaard op kleinere schaal, zijnde het niveau van de politiezone, waar minstens 3 strafbare feiten, zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering, per 1 000 inwoners per jaar gedurende de voorbije 3 jaar zijn vastgesteld. De afbakening van de politiezones kan men overigens terugvinden in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

De bewaartermijn bedraagt, naar analogie met de regeling op vlak van de arrondissementen, 6 maanden wanneer het aantal feiten bedoeld in artikel 90*ter*, §§ 2 tot 4 van het Wetboek van strafvordering per 1 000 inwoners per jaar (op een gemiddelde van 3 jaar) 3 of 4 is, 9 maanden wanneer het aantal 5 of 6 is, en 12 maanden wanneer er tenminste 7 zware strafbare feiten zijn zoals bedoeld in art 90*ter* van het Wetboek van Strafvordering.

De geografische afbakening op basis van gerechtelijke arrondissementen enerzijds of politiezones anderzijds vormt ook een samenhangend geheel met betrekking tot de concrete en dagelijkse bestrijding van bepaalde criminele verschijnselen door zowel politie als justitie, zodat, zoals het COC in punt 17 van zijn advies aangeeft, "de geografische omschrijving van het arrondissement en de politiezone rationeel en logisch is met betrekking tot de gekende staatkundige, gerechtelijke en politionele organisatie".

In dit verband moet ook worden opgemerkt dat dadergroepen bovendien zeer mobiel zijn en zich verplaatsen,

que le crime organisé est par essence polycriminel. Se limiter d'office à certains lieux très ciblés au niveau local pour ce type de criminalité n'est pas approprié.

Dans cette optique, l'approche des "territoires criminels" doit être prise en compte. Le criminologue canadien Maurice Cusson a montré dans ses études qu'on peut considérer trois types de territoires criminels: les sanctuaires, les terrains de chasse et les lieux de plaisir. En matière de crime organisé, ces territoires criminels sont d'une importance capitale pour mener l'action publique et l'action policière.

Les sanctuaires sont les lieux où les criminels et leurs structures sont implantés.

S'il est clair que les organisations criminelles sont généralement implantées dans les agglomérations, ce n'est pas une généralité et par exemple les bandes criminelles de motards ont souvent tendance à implanter leurs Clubhouse (chapter) dans des zones reculées ou plus rurales (zones industrielles, cafés de village ou habitations isolées) mais sont susceptibles de se déplacer en fonction de la réaction policière/judiciaire et de la concurrence entre certaines organisations.

Les terrains de chasse sont les lieux où les groupes d'auteurs et les organisations criminelles commettent leurs faits. Il s'agit traditionnellement des informations qui ressortent des rapports statistiques annuels montrant la localisation temps-espace des phénomènes criminels.

Les activités des organisations criminelles et des groupes d'auteurs ne peuvent pas être limitées géographiquement au territoire d'une ou plusieurs communes. En effet, se priver de données de communications dans certaines zones serait une erreur fondamentale. Cela nous obligerait à prendre des mesures encore plus intrusives pour pouvoir suivre leurs agissements, leurs méfaits et démontrer pénalement les éléments constitutifs d'une organisation (Article 324*bis* Code pénal notamment).

Les lieux de plaisirs, ainsi nommés par Cusson, sont les endroits où le milieu criminel se retrouve et s'organise, où il "dépense" en partie ses gains criminels. Il s'agit d'établissements de l'Horeca, de salles de jeux clandestines, de bars à champagne ou d'établissements de prostitution. Beaucoup sont implantés dans les grandes villes et les agglomérations mais il est connu qu'un certain nombre se situent hors de celles-ci, le long de grandes nationales en pleine campagne (RN 3 entre Liège et Leuven, RN 5 entre Couvin et Charleroi, routes rurales en région frontalière du Tournai, …). Tous ces lieux sont donc susceptibles d'être liés d'une manière

en dat de georganiseerde criminaliteit in essentie polycrimineel is. Het lijkt niet juist om zich voor dit soort criminaliteit te beperken tot bepaalde zeer gerichte plaatsen op lokaal niveau.

In dat opzicht is het relevant de beschrijving van de "criminele gebieden" in gedachten te houden. De Canadese criminoloog Maurice Cusson heeft in zijn studies aangetoond dat er drie soorten criminele gebieden zijn: toevluchtsoorden, jachtgebieden en plaatsen van plezier. Wat de georganiseerde misdaad betreft, zijn deze criminele gebieden van het grootste belang voor het optreden van de overheid en de politie.

Toevluchtsoorden zijn de plaatsen waar criminelen en hun structuren zijn gevestigd.

Hoewel het duidelijk is dat criminele organisaties over het algemeen in stedelijke gebieden gevestigd zijn, is dit geen algemene regel en bijvoorbeeld motorbendes hebben vaak de neiging hun clubhuizen (chapter) in afgelegen of meer landelijke gebieden te vestigen (industriegebieden, dorpscafés of afgelegen woningen), maar zullen vermoedelijk verhuizen in functie van de politonele/gerechtelijke reacties en de concurrentie tussen bepaalde organisaties.

Jachtgebieden zijn de plaatsen waar dadergroepen en criminele organisaties hun feiten plegen. Dit is wat meestal naar voren komt uit de jaarlijkse statistische verslagen waarin de criminele fenomenen worden bestudeerd.

De activiteiten van criminele organisaties en dadergroepen mogen geografisch niet beperkt blijven tot het grondgebied van één of meer gemeenten. Het zou zodus een fundamentele vergissing zijn om communicatiegegevens in bepaalde gebieden te ontzeggen. Dit zou ertoe leiden dat er meer intrusieve maatregelen gebruikt zouden worden om hun daden en hun wandaden te kunnen volgen en de constitutieve elementen van een organisatie strafrechtelijk te kunnen aantonen (met name artikel 324*bis* Strafwetboek).

De plaatsen van plezier, zoals Cusson ze noemt, zijn de plaatsen waar het criminele milieu bijeenkomt en zich organiseert, waar zij een deel van haar criminele inkomsten "uitgeeft". Het zijn horecagelegenheden, clandestiene speelzalen, champagnebars en prostitutieinrichtingen. Een aantal daarvan zijn gelegen in de grote steden en gemeenten, maar het is bekend dat vele zich buiten deze steden en gemeenten bevinden, langs de hoofdwegen op het platteland (RN 3 tussen Luik en Leuven, RN 5 tussen Couvin en Charleroi, plattelandswegen in de grensstreek van Doornik, enz.). Al deze plaatsen zijn dus vermoedelijk op directe (het

directe (l'exemple des terrains de chasse) ou d'une manière indirecte (l'exemple des lieux de plaisir) à la commission d'infractions graves.

De manière fondamentale, le législateur estime que la zone ("*geographical area*") visée au point 150 de l'arrêt la Quadrature du net peut à l'issue de l'examen des statistiques de chaque arrondissement porter sur l'ensemble du territoire national s'il y a dans chacun de ces arrondissements un taux de criminalité élevé.

Le législateur souhaite conséquemment rappeler, eu égard au point 122 de l'avis n° 108/2021 de l'Autorité de protection des données du 28 juin 2021 que pour déterminer si ce critère respecte les critères de l'arrêt Quadrature du Net, le point 150 de l'arrêt indique qu'il faut en effet partir du seuil à partir duquel "les autorités nationales compétentes considèrent sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave". Un tel seuil, de nature dynamique et spécifique à chaque zone géographique, ne peut par nature être basé sur un nombre fixe déterminé sur la base des résultats obtenus pour l'ensemble des zones géographiques. En effet, un tel seuil servirait à soustraire tout ou partie des zones géographiques à la possibilité de réaliser une conservation des données sur la base de ce critère. Vu l'exigence du caractère dynamique de ce critère (les statistiques sont par essence évolutives), l'utilisation d'un seuil fixe et médian nécessiterait alors, chaque année, de le modifier pour s'assurer de soustraire un nombre prédéterminé de zones géographiques. Prendre comme point de départ supposé neutre l'entrée en vigueur de la loi, comme semble le suggérer l'APD dans le point 122 de son avis, n'a pas plus de fondement objectif.

Le législateur insiste sur le fait que ce qui est interdit sur la base du point 143 de l'arrêt La Quadrature Du Net, c'est de "prévoir la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation qui couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différentiation, limitation, ni exception ne soient opérées en fonction de l'objectif poursuivi".

Or, comme le Conseil d'État le souligne dans son avis 69/381.4 du 28 juin 2021, les différents délais de conservation permettent de "garantir la proportionnalité de la conservation au regard de l'importance de la criminalité dans l'arrondissement judiciaire ou la zone de police considérés (page 61, point 5)". En outre, chaque arrondissement/zone de police fait l'objet d'un examen

voorbeeld van de jachtgebieden) of indirecte (voorbeeld van de plaatsen van plezier) manier verbonden met het plegen van zware misdrijven.

In wezen is de wetgever van mening dat de in punt 150 van het arrest Quadrature du net bedoelde zone ("*geographical area*"), na bestudering van de statistieken voor elk arrondissement, het gehele nationale grondgebied kan omvatten indien in elk van deze arrondissementen een hoog misdaadcijfer wordt vastgesteld.

De wetgever wenst er derhalve met betrekking tot punt 122 van advies nr. 108/2021 van 28 juni 2021 van de gegevensbeschermingsautoriteit aan te herinneren dat, om te bepalen of dit criterium voldoet aan de criteria van het arrest Quadrature du Net, volgens punt 150 van dit arrest moet worden uitgegaan van de drempel waaronder "de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd". Een dergelijke drempel, die dynamisch en specifiek is voor elke geografisch zone, kan van nature niet worden gebaseerd op een vast cijfer dat wordt bepaald op basis van de voor alle geografische zones verkregen resultaten. Een dergelijke drempel zou er immers toe leiden dat alle of een deel van de geografische zones worden uitgesloten van de mogelijkheid om op basis van dit criterium gegevens te bewaren. Gezien het dynamische karakter van dit criterium (statistieken zijn per definitie evolutief) zou het gebruik van een vaste en mediane drempelwaarde immers vereisen dat deze elk jaar wordt gewijzigd om ervoor te zorgen dat een vooraf bepaald aantal geografische zones in mindering wordt gebracht. De inwerkingtreding van de wet als zogenaamd neutraal uitgangspunt nemen, zoals de GBA in punt 122 van zijn advies lijkt te suggereren, heeft geen objectieve grondslag.

De wetgever beklemtoont dat wat op grond van punt 143 van het arrest La Quadrature Du Net verboden is, erin bestaat te voorzien in "een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, die de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel".

Zoals de Raad van State in zijn advies 69/381.4 van 28 juni 2021 echter opmerkt, maken de verschillende bewaringstermijnen het mogelijk "de evenredigheid van de bewaring te garanderen ten aanzien van de omvang van de criminaliteit in het gerechtelijk arrondissement of de politiezone in kwestie" (blz. 152, punt 5). Bovendien wordt per gerechtelijk arrondissement/politiezone nagegaan of

visant à objectiver s'il y a ou non un seuil grave de criminalité.

C'est sans aucun doute aussi dans cette optique de validation de l'appréciation de la pertinence et de la proportionnalité du critère retenu que le COC ajoute dans son avis du 21 mai 2021, à propos de ce critère statistique repris à l'article 126/1, que "le COC n'a pas de remarques particulières à ce sujet et comprend que les rédacteurs de l'avant-projet ont ainsi recherché au maximum à obtenir des critères objectifs en ligne avec la jurisprudence précitée de l'UE de la Cour de Justice".

On ne peut dès lors nier qu'il existe une possibilité, sur la base de données statistiques, qui sont par définition dynamiques et évolutives, que des données doivent être conservées dans tous les arrondissements judiciaires, et donc pour l'ensemble du territoire. Cela signifierait qu'une conservation des données serait prévue pour l'ensemble du territoire.

Le service désigné par le Roi ne disposant d'aucune marge de manœuvre dans l'établissement de la liste des arrondissements judiciaires et/ou des zones de police qui seraient soumis à une obligation de conservation des données, le projet de loi prévoit une validation par le COC. Ce point est expliqué plus en détail ci-dessous dans la partie consacrée à l'origine des statistiques. En résumé, la direction de la police fédérale chargée de la gestion de la Banque de données Nationale Générale transmettra les statistiques à l'Organe de contrôle pour validation. Dans le cadre de cette validation, l'organe de contrôle déterminera également s'il doit ou non prévoir une conservation des données pour tous les arrondissements judiciaires et quelle période de conservation s'applique dans ces arrondissements judiciaires. Après validation, les statistiques et les périodes de conservation respectives sont envoyées au service désigné par le Roi. Ce service établit la liste et propose aux ministres de la Justice et de l'Intérieur de l'approuver. Dès que cet arrêté ministériel sera publié, la conservation des données pourra commencer.

Un arrêté ministériel déterminant la liste des arrondissements judiciaires et/ou des zones de police qui seraient soumis à une obligation de conservation des données, ainsi que les durées de conservation respectives, ne contient pas de nouvelles règles juridiques: il s'agit simplement d'une constatation ministérielle d'un résultat qui a été créé par l'application de critères fixés par la loi.

S'il existe une conservation de données d'au moins un an applicable à l'ensemble du territoire (avec ou sans

er al dan niet een hoge drempel voor zware criminaliteit bestaat.

Het is ongetwijfeld ook vanuit dit oogpunt van validering van de beoordeling van de relevantie en de evenredigheid van het weerhouden criterium dat het COC in zijn advies van 21 mei 2021 met betrekking tot dit in artikel 126/1 opgenomen statistische criterium toevoegt dat "het COC hierover geen bijzondere opmerkingen heeft en begrijpt dat de stellers van het voorontwerp zo maximaal mogelijk hebben gezocht naar objectieve criteria in lijn met de voormelde rechtspraak van het EU Hof van Justitie".

Het kan dus niet ontkend worden dat de mogelijkheid bestaat dat op basis van de statistische gegevens, die per definitie dynamisch en evolutief zijn, vastgesteld wordt dat gegevens bewaard moeten worden in alle gerechtelijke arrondissementen, en dus voor het gehele grondgebied. Dit zou dan betekenen dat er voor het volledige grondgebied een gegevensbewaring voorzien wordt.

Omdat de door de Koning aangewezen dienst over geen enkele beoordelingsbevoegdheid beschikt bij het opstellen van de lijst van gerechtelijke arrondissementen en /of politiezones die onder een gegevensbewaringsplicht zouden vallen, voorziet het wetsontwerp in een validatie door het COC. Dit wordt hieronder verder uitgelegd bij de herkomst van de statistieken. Kort gezegd komt het erop neer dat de directie van de federale politie die instaat voor het beheer van de Algemene Nationale Gegevensbank de statistieken zal overmaken aan het Controleorgaan met het oog op validatie ervan. Het Controleorgaan zal in het kader van deze validatie ook vaststellen of er al dan niet voor alle gerechtelijke arrondissementen een gegevensbewaring voorzien moet worden, en welke bewaartermijn geldt in deze gerechtelijke arrondissementen. Na de validatie worden de statistieken en de respectievelijke bewaartermijnen overgemaakt aan de door de Koning aangewezen dienst. Deze dienst stelt de lijst op en stelt voor aan de ministers van Justitie en Binnenlandse Zaken om deze lijst goed te keuren. Van zodra dit ministerieel besluit is gepubliceerd, kan de gegevensbewaring een aanvang nemen.

Een ministerieel besluit tot vaststelling van de lijst van gerechtelijke arrondissementen en/of politiezones waarop de gegevensbewaring betrekking heeft, samen met de respectievelijke bewaartermijnen bevat geen nieuwe rechtsregels: het is slechts een ministeriële vaststelling van een resultaat dat door toepassing van wettelijk vastgelegde criteria gecreëerd werd.

Indien er voor minstens een jaar een gegevensbewaring geldt voor het gehele grondgebied (al dan niet

délais de conservation différents), il n'est plus nécessaire que le service désigné par le Roi identifie également les zones géographiques visées aux points 3° à 5° du présent paragraphe: en effet, celles-ci sont alors déjà couvertes par l'obligation de conservation sur la base du critère statistique.

Provenance des statistiques

La production annuelle de statistiques implique que ce critère est dynamique puisqu'il dépend des chiffres de criminalité repris soit au niveau d'un arrondissement, soit au niveau d'une zone de police.

La période de référence de trois ans permet d'avoir des statistiques suffisamment significatives tout en fournissant une image actuelle des chiffres de criminalité.

En effet, l'addition sur un cycle significatif de 3 ans des faits graves permet précisément de mettre en exergue le caractère strictement nécessaire de la mesure puisque ce n'est qu'à l'issue d'une période significative, que l'on peut légitimement et de manière fondée conclure que les organisations criminelles se sont installées ou pas au niveau d'un arrondissement, soit au niveau d'une zone et qu'une capacité policière importante doit être dédiée à la lutte contre celle-ci.

D'autre part, et de manière plus fondamentale, le législateur interprète le caractère strictement nécessaire de la mesure visée au point 151 de l'arrêt de la Cour de Justice du 6 octobre 2020 comme une obligation de prévoir *a priori* un ou plusieurs critères préétablis ou, à défaut, une période pour évaluer la mesure de conservation ciblée de sorte qu'elle ne soit pas d'office d'application pour une durée indéterminée, malgré son caractère ciblé. Le fait que des statistiques soient annuellement produites, lesquelles enclenchent ou pas une conservation des données au terme d'une procédure validée par un Organe indépendant relevant du pouvoir législatif qui a reçu toutes les compétences nécessaires pour valider la production de ces statistiques et, le cas échéant les rectifier s'inscrit pleinement dans le cadre indiqué dans le point 151 de l'arrêt de la Cour de Justice du 6 octobre 2020.

Enfin, contrairement à ce que le Conseil d'État indique au point 6.2 de son avis du 28 juin 2021, la conservation de données est bien limitée vu que, si les seuils ne sont pas atteints au niveau des arrondissements judiciaires ou des zones de police, il n'y a pas de conservation. Il y a en outre une vérification annuelle pour voir si ces seuils sont atteints ou pas.

met verschillende bewaringstermijnen), is het niet meer nodig dat de door de Koning aangewezen dienst ook nog de geografische zones bedoeld in de punten 3° tot 5° van deze paragraaf identificeert: deze zijn dan immers al per definitie afgedekt door de bewaarplicht op basis van het statistische criterium.

Herkomst van de statistieken

Het jaarlijks bepalen van statistieken impliceert dat dit criterium dynamisch is, aangezien het afhangt van de criminaliteitscijfers die hetzij op het niveau van een arrondissement, hetzij op het niveau van een politiezone worden geregistreerd.

De referentieperiode van drie jaar maakt het mogelijk voldoende betekenisvolle statistieken op te stellen en tegelijkertijd een actueel beeld van de criminaliteitscijfers te geven.

De som van de ernstige feiten over een aanzienlijke periode van drie jaar maakt het precies mogelijk het strikt noodzakelijke karakter van de maatregel te benadrukken, aangezien pas aan het einde van een aanzienlijke periode op legitieme en valabele wijze kan worden geconcludeerd of criminele organisaties zich al dan niet in een wijk of een zone hebben gevestigd, en dat een aanzienlijke politiecapaciteit moet worden ingezet om deze te bestrijden.

Anderzijds, en meer fundamenteel, interpreteert de wetgever het strikt noodzakelijke karakter van de maatregel bedoeld in punt 151 van het arrest van het Hof van Justitie van 6 oktober 2020 als een verplichting om *a priori* te voorzien in een of meer vooraf vastgestelde criteria of, bij gebreke daarvan, een termijn voor de evaluatie van de gerichte bewaringsmaatregel, zodat deze niet automatisch van toepassing is voor onbepaalde tijd, ondanks zijn gerichte karakter. Het feit dat jaarlijks statistieken worden opgesteld, die al dan niet aanleiding kunnen geven tot gegevensbewaring aan het einde van een procedure die wordt gevalideerd door een onafhankelijk orgaan onder de wetgevende macht, die alle nodige bevoegdheden heeft gekregen om de opstelling van deze statistieken te controleren en zo nodig te corrigeren, is volledig in overeenstemming met het kader dat wordt voorgesteld in punt 151 van het arrest van het Hof van Justitie van 6 oktober 2020.

Tot slot is de gegevensbewaring, anders dan de Raad van State in punt 6.2 van zijn advies van 28 juni 2021 aangeeft, wel degelijk gelimiteerd, want als de drempels op het niveau van de gerechtelijke arrondissementen of politiezones niet worden bereikt, is er geen sprake van bewaring. Bovendien wordt jaarlijks gecontroleerd of deze drempels al dan niet worden bereikt.

L'arrêt Quadrature du Net du 6 octobre 2020 mentionne comme critère une "situation caractérisée par (…) un risque élevé de commission d'actes de criminalité grave".

Il s'agit donc de prendre comme point de référence la commission de telles infractions.

À cet égard, notons que les constatations d'infractions sont répertoriées au niveau national dans la Banque de données Nationale Générale, visée à l'article 44/7 de la loi sur la fonction de police.

Le point 6 de cet article mentionne en effet que cette banque de données sert à aider à "l'appui à la définition et à la réalisation de la politique policière et de sécurité".

Il faut bien être conscient que l'ensemble des faits criminels ne sont pas connus de la police (absence de plainte, non visibilité directe du phénomène, par exemple la traite ou le trafic d'êtres humains). Dès lors, les faits répertoriés dans la Banque de données Nationale Générale ne constituent qu'une partie limitée des phénomènes criminels au niveau des arrondissements et des zones de police.

L'APD suggère, au point 124 de son avis, de se baser sur les condamnations. Néanmoins, les condamnations sont prononcées pour une partie limitée de faits constatés et ne permettrait pas de donner une vision réelle du nombre élevé d'actes de criminalité grave, du sentiment d'insécurité qui y est lié, du nombre de victimes à assister et *in fine* du besoin objectif de recourir aux informations conservées par les opérateurs pour mener à bien les enquêtes.

De plus il est fondamental de considérer l'impact de la disponibilité des données de trafic et de localisation sur les condamnations et sur l'identification des auteurs. La conservation des données a comme objectif opérationnel premier d'identifier les auteurs d'infractions. Sans identification, il n'y aura pas de condamnation. La conservation des données et le nombre de requêtes introduites auprès des opérateurs est donc proportionnelle au nombre de faits à enquêter et non au nombre de condamnations.

En outre, si le critère du nombre de condamnations était pris en considération le lien temporel entre la nécessité de conserver les données et le fait risquerait d'être perdu. Les condamnations interviennent souvent plusieurs années après que les faits aient été commis.

Finalement, les condamnations sont répertoriées par rapport au domicile de l'auteur et non pas par rapport

Het arrest Quadrature du Net van 6 oktober 2020 vermeldt als criterium een "situatie die wordt gekenmerkt door (…) een hoog risico op het plegen van zware criminele feiten".

Het plegen van dergelijke strafbare feiten moet dus als referentiepunt genomen worden.

De vaststellingen van strafbare feiten worden op nationaal niveau geregistreerd in de Nationale Algemene Gegevensbank, bedoeld in artikel 44/7 van de Politiewet.

In punt 6 van dit artikel wordt ook vermeld dat deze gegevensbank het mogelijk maakt "de bepaling en de uitwerking van het politie- en veiligheidsbeleid te ondersteunen ".

Er moet op gewezen worden dat er een groot aantal feiten is die niet door de politie vastgesteld worden (geen klacht ingediend, onzichtbaarheid van het fenomeen, bijvoorbeeld mensenhandel/mensensmokkel). Hierdoor bevat de Algemene Nationale Gegevensbank slechts een beperkt deel van de criminele fenomenen die terug te brengen zijn tot het niveau van een gerechtelijk arrondissement en politiezone.

De GBA stelt in punt 124 van zijn advies voor om veroordelingen als basis te gebruiken. De veroordelingen hebben echter betrekking op een beperkt aantal vastgestelde feiten en zouden geen getrouw beeld geven van het grote aantal ernstige misdrijven, het daarmee samenhangende onveiligheidsgevoel, het aantal slachtoffers dat moet worden geholpen en uiteindelijk de objectieve noodzaak om de door de operatoren bijgehouden informatie te gebruiken om onderzoeken uit te voeren.

Voorts is het van fundamenteel belang om het effect van de beschikbaarheid van verkeers- en locatiegegevens op veroordelingen en op de identificatie van daders in ogenschouw te nemen. Het belangrijkste operationele doel van gegevensbewaring is het identificeren van daders. Zonder identificatie, zal er geen veroordeling zijn. De gegevensbewaring en het aantal verzoeken aan operatoren is dus evenredig met het aantal te onderzoeken feiten en niet met het aantal veroordelingen.

Bovendien zou, indien het criterium van de veroordeling in aanmerking zou worden genomen, het temporele verband tussen de noodzaak om de gegevens te bewaren en het feit verloren gaan. Veroordelingen vinden vaak pas jaren na de feiten plaats.

Tot slot, veroordelingen worden geregistreerd op de woonplaats van de dader en niet op de plaats waar de

au lieu où les faits ont été commis. Or, c'est bien sur le lieu où les faits ont été commis que les autorités judiciaires et les policiers chargés de l'enquête ont besoin d'information.

Concernant la préoccupation exprimée par l'APD dans le point 123 de son avis, chaque constat d'infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle fait l'objet d'un procès-verbal, qui est approuvé par le responsable hiérarchique du verbalisant. Ce dernier vérifie notamment si les éléments constitutifs de l'infraction sont présents. Ce mécanisme permet donc d'éviter que les chiffres soient artificiellement gonflés. En outre, ils seront également vérifiés par le COC, comme expliqué *infra*.

Le comptage des faits se déroule dans l'environnement statistique de la police fédérale, soit le Management Information System (le MIS). Des règles pour le comptage des faits 90*ter* à partir de la Banque de données Nationale Générale ont été mises en œuvre afin de garantir que celui-ci se déroule selon les règles de l'art. À titre d'exemple, pour s'assurer qu'une infraction visée à l'article 90*ter* du Code d'instruction criminelle ne soit comptée qu'une seule fois, seul le procès-verbal initial reprenant le fait 90*ter* est pris en compte et pas les procès-verbaux subséquents.

Concrètement, la direction de l'information et de l'ICT de la police fédérale réalisera une fois par an, les statistiques au niveau des arrondissements et le cas échéant, à l'intérieur de ces arrondissements au niveau des zones de police.

Ces statistiques sont soumises à la validation préalable de l'Organe de contrôle de l'information policière. En ce sens, le COC procède à un examen de la qualité des données et du respect de la procédure de production des statistiques. Cela vise notamment la vérification que les faits comptés sont bien des faits de la liste de l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle, qui ont eu lieu dans les 3 dernières années et qu'il n'y a pas de faits comptés plusieurs fois. Cette validation des statistiques annuelles par le COC est primordiale afin d'assurer la fiabilité des statistiques.

La validation des statistiques annuelles par le COC ne porte aucunement préjudice à l'exercice ultérieur des pouvoirs du COC à l'égard de la gestion de l'information et des données personnelles par la police, en ce compris concernant les processus et outils ayant mené à la production des statistiques préalablement validés par le COC.

feiten werden gepleegd. Het is echter over de plaats waar de feiten werden gepleegd dat de gerechtelijke autoriteiten en de politie die met het onderzoek zijn belast, informatie nodig hebben.

Voor wat betreft de bezorgdheid die de GBA in punt 123 van zijn advies heeft geuit, wordt voor elk vastgesteld strafbaar feit zoals bedoeld in artikel 90*ter*, §§ 2 tot en met 4, van het Wetboek van strafvordering een proces-verbaal opgemaakt, dat wordt goedgekeurd door de hiërarchisch verantwoordelijke van de verbalisant, die onder meer nagaat of de constitutieve elementen van het strafbare feit aanwezig zijn. Dit mechanisme voorkomt dus dat de cijfers kunstmatig worden opgeblazen. Bovendien zullen deze cijfers worden geverifieerd, zoals hieronder aangegeven, door het COC.

De telling van de feiten vindt plaats in de statistische omgeving van de federale politie, namelijk het Management Information System (MIS). Er werden regels ingevoerd voor het tellen van 90*ter*-feiten uit de Nationale Algemene Gegevensbank om ervoor te zorgen dat dit op een state-of-the-art manier gebeurt. Om er bijvoorbeeld voor te zorgen dat een strafbaar feit als bedoeld in artikel 90*ter* van het Wetboek van strafvordering slechts één keer wordt meegerekend, wordt alleen rekening gehouden met het eerste proces-verbaal dat het 90*ter*-feit bevat, en niet met latere processen-verbaal.

Concreet zal de Directie Informatie en ICT van de federale politie één keer per jaar statistieken opmaken op het niveau van de arrondissementen en, indien nodig, binnen deze arrondissementen op het niveau van de politiezones.

Deze statistieken moeten vooraf gevalideerd worden door het Controleorgaan op de politionele informatie. In dit verband onderzoekt het COC de kwaliteit van de gegevens en de naleving van de procedure voor de productie van de statistieken. Dit houdt onder meer in dat wordt nagegaan of de getelde feiten wel degelijk feiten zijn uit de lijst van artikel 90*ter*, §§ 2 tot 4 van het Wetboek van Strafvordering, die in de loop van de laatste 3 jaar hebben plaatsgevonden, en of er geen feiten zijn die meermaals zijn geteld. Deze validering van de jaarlijkse statistieken door het COC is van essentieel belang om de betrouwbaarheid van de statistieken te garanderen.

De validering van de jaarlijkse statistieken door het COC doet geen afbreuk aan de latere uitoefening van de bevoegdheden van het COC met betrekking tot het beheer van informatie en persoonsgegevens door de politie, met inbegrip van de processen en instrumenten die tot de productie van de eerder door het COC gevalideerde statistieken hebben geleid.

Étant donné que les statistiques ne constituent pas des données personnelles, le COC ne dispose pas en soi de compétences spécifiques à cet égard. Par conséquent, le présent projet de loi prévoit explicitement de doter le COC, au fin de l'exercice de cette nouvelle tâche, de toutes les compétences initialement attribuées en matière de protection des données par le titre 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et ce, afin de déterminer formellement que les statistiques sont adéquates, pertinentes et limitées à ce qui est nécessaire à chaque fois qu'elles sont élaborées. Ainsi, le COC pourrait, par exemple, prendre des mesures correctrices telles qu'un avertissement indiquant qu'un traitement n'est actuellement pas conforme en termes de protection des données ou constater que certains faits n'ont pas été pris en compte dans les statistiques alors qu'ils devraient être inclus ou, à l'inverse éviter des doublons. En ce sens, le COC pourrait indiquer que d'autres paramètres (localisation) doivent être examinés afin d'éviter des doublons.

Afin de permettre au COC de procéder à la validation des statistiques endéans le délai d'un mois, la direction visée à l'article 44/11 de la loi sur la fonction de police lui fournit l'ensemble des documents nécessaires et requis par le COC dans les plus brefs délais et au plus tard, dans le délai fixé par ce dernier. Les données nécessaires comprennent tout document jugé utile par le COC aux fins de cette validation tel que la documentation sur la méthodologie poursuivie et sur la qualité des données, ces documents permettant notamment la vérification de l'encodage sur la base de l'article 90*ter* et de la pertinence de la méthodologie afin d'éviter les doublons.

Le COC dispose d'un délai d'un mois afin de procéder à cette validation et d'en informer la direction visée à l'art. 44/11 de la loi sur la fonction de police. La validation peut être liée à des conditions ou peut aller de pair avec un ordre de se mettre en règle dans un délai fixé. À titre d'exemple, le COC peut valider les statistiques tout en demandant à la direction compétente de procéder, pour les prochaines statistiques, à une amélioration ou une adaptation de la méthodologie poursuivie.

Lorsque le COC a informé la direction susmentionnée de sa validation, en ce compris lorsque cette validation est conditionnée à une amélioration ou adaptation pour les futures statistiques, cette dernière transmet lesdites statistiques au service désigné par le Roi. Par contre, en l'absence de validation par le COC dans le délai d'un mois à dater de la transmission des statistiques, celles-ci ne peuvent être transmises au service désigné

Aangezien de statistieken geen persoonsgegevens zijn, beschikt het COC op zich niet over specifieke bevoegdheden ter zake. Bijgevolg voorziet huidig wetsontwerp met het oog op de uitoefening van deze nieuwe taak, uitdrukkelijk in de toekenning aan het COC van alle bevoegdheden die oorspronkelijk op het gebied van gegevensbescherming werden toegekend door titel 7 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens betreffende deze statistieken, zodat formeel vastgesteld kan worden dat de statistieken toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is, en dit telkens wanneer zij worden opgesteld. Zo kan het COC bijvoorbeeld corrigerende maatregelen nemen, zoals een waarschuwing dat een verwerking momenteel niet in overeenstemming is met de gegevensbeschermingsvoorschriften of dat bepaalde feiten niet in aanmerking zijn genomen in de statistieken terwijl dat wel het geval zou moeten zijn, of, omgekeerd, het voorkomen van doublures. In die zin zou het COC kunnen aangeven dat andere parameters (locatie) moeten worden bestudeerd om overlappingen te voorkomen.

Om het COC in staat te stellen de statistieken binnen de termijn van één maand te valideren, verstrekt de in artikel 44/11 van de wet op het politieambt bedoelde directie haar zo spoedig mogelijk en uiterlijk binnen de door haar vastgestelde termijn alle door de COC gevraagde documenten. De noodzakelijke gegevens omvatten elk document dat door de COC nuttig wordt geacht voor validatiedoeleinden, zoals documentatie over de gebruikte methodologie en over de kwaliteit van de gegevens. Deze documenten maken het met name mogelijk de codering op basis van artikel 90*ter* van het Wetboek van strafvordering en de relevantie van de methodologie te verifiëren om overlappingen te voorkomen.

Het COC beschikt over een termijn van één maand om deze validatie uit te voeren en de in artikel 44/11 van de wet op het politieambt bedoelde directie te informeren. Aan de validatie kunnen voorwaarden worden verbonden of zij kan vergezeld gaan van een bevel om binnen een bepaalde termijn aan de eisen te voldoen. Het COC kan bijvoorbeeld de statistieken valideren en tegelijkertijd de bevoegde directie verzoeken de methodologie voor toekomstige statistieken te verbeteren of aan te passen.

Wanneer het COC de voornoemde directie in kennis heeft gesteld van zijn validering, ook wanneer aan deze validering een voorwaarde verbonden is voor een verbetering of een aanpassing voor toekomstige statistieken, geeft deze directie deze statistieken door aan de door de Koning aangewezen dienst. Indien het COC de statistieken echter niet binnen een maand na de toezending ervan valideert, kunnen zij niet worden toegezonden aan de

par le Roi. En conséquence, une conservation des données ciblée de manière géographique sur la base de lieux caractérisés par un nombre élevé d'actes de criminalités graves ne peut être effectuée.

Comme l'indique l'Organe de contrôle au point 11 de son avis du 21 mai 2021, il reçoit une nouvelle compétence importante qui est directement en rapport avec le thème de la conservation des données et de leur utilisation dans le cadre de la fonction de police judiciaire puisque le COC est chargé d'une forme de contrôle *a priori* des statistiques provenant de la Banque de données Nationale Générale.

Pour répondre aux considérations mentionnées dans le point 16 de l'avis de l'Organe de contrôle, il est tout à fait possible d'isoler dans la Banque de données Nationale Générale des services de police, les faits visés à l'article 90*ter* du Code d'instruction criminelle, de sorte que la production annuelle de statistiques est tout à fait possible.

Il nous paraît aussi important de souligner:

— d'une part que la direction de la police fédérale chargée de la gestion quotidienne de la B.N.G. dispose d'un service qui s'occupe exclusivement de la politique criminelle et qui a donc en son sein les profils requis en matière de gestion; et

— d'autre part que la méthodologie usitée en matière de production de statistiques est documentée sur le site de la police fédérale (*http://www.stat.policefederale.be*).

Ceci implique que les statistiques produites sur la base des données de la Banque de données Nationale Générale sont réalisées avec tout le professionnalisme requis.

Le deuxième critère porte sur le niveau de la menace terroriste ou extrémiste (échelle de 1 à 4, variant de faible à très grave).

Il s'agit, dans cette hypothèse, de réaliser une conservation générale ou ciblée, des données visées au § 2, au sens où, ces données ne sont conservées que lorsque et aussi longtemps que le niveau de la menace terroriste et extrémiste sur ce lieux atteint un niveau 3. Dès lors qu'un niveau de la menace atteint le niveau 3 (menace possible et vraisemblable) et, *a fortiori*, 4 (menace sérieuse et imminente), une conservation des données visées au § 2 sur les zones géographiques visées est réalisée. Il peut dans certains cas (évaluation générale de la menace de niveau 3 ou 4) s'agir de l'ensemble du territoire.

door de Koning aangewezen dienst. Bijgevolg kan geen geografisch gerichte gegevensbewaring plaatsvinden op basis van plaatsen die worden gekenmerkt door een groot aantal ernstige strafbare feiten.

Zoals het Controleorgaan in punt 11 van zijn advies van 21 mei 2021 aangeeft, krijgt het een belangrijke nieuwe bevoegdheid die rechtstreeks verband houdt met de bewaring van gegevens en het gebruik ervan in het kader van de gerechtelijke politie, aangezien het COC verantwoordelijk is voor een vorm van *a priori* controle van de statistieken van de Algemene Nationale Gegevensbank.

In antwoord op de overwegingen vermeld in punt 16 van het advies van het Controleorgaan, is het heel goed mogelijk om in de Algemene Nationale Gegevensbank van de politiediensten de feiten bedoeld in artikel 90*ter* van het Wetboek van Strafvordering te isoleren, zodat de jaarlijkse productie van statistieken absoluut mogelijk is.

Het is ook belangrijk erop te wijzen:

— enerzijds dat de directie van de federale politie die belast is met het dagelijks beheer van de A.N.G. beschikt over een dienst die zich uitsluitend bezighoudt met strafrechtelijk beleid en dus over de vereiste beheersprofielen beschikt; en

— anderzijds dat de methodologie die bij de opstelling van de statistieken wordt gevolgd, gedocumenteerd is op de website van de federale politie (*http://www.stat.policefederale.be*).

Dit houdt in dat de statistieken opgesteld op basis van de gegevens van de Algemene Nationale Gegevensbank, worden opgesteld volgens de regels van de kunst en met de nodige professionaliteit.

Het tweede criterium heeft betrekking op het dreigingsniveau inzake terrorisme of extremisme (schaal van 1 tot 4, gaande van laag naar zeer ernstig).

In dit geval gaat het om algemene of gerichte opslag van de in § 2 bedoelde gegevens, in die zin dat deze gegevens alleen worden bewaard wanneer en zolang het niveau van de terroristische en extremistische dreiging op deze plaats een niveau 3 bereikt. Zodra het dreigingsniveau het niveau 3 (mogelijke en waarschijnlijke dreiging) en *a fortiori* het niveau 4 (ernstige en onmiddellijke dreiging) bereikt, worden de in § 2 bedoelde gegevens opgeslagen in de betrokken geografische zones. In sommige gevallen (algemene beoordeling van de dreiging van niveau 3 of 4) kan dit het hele grondgebied zijn.

Dans ce dernier cas, dès lors que la menace en matière de terrorisme ou d'extrémisme est grave ou très grave, il est nécessaire d'activer une conservation de données pour par ce niveau 3 ou 4 et ce, aussi longtemps que le niveau 3 ou le niveau 4 perdure. En effet même si une évaluation passe du niveau 4 vers le niveau 3, une conservation généralisée et indifférenciée doit être maintenue pour faire face à la menace qui reste réelle et actuelle.

Ce niveau des menaces 3 ou 4 est établi par un Organe indépendant des services qui utilisent les données des opérateurs

Dans la pratique, l'Organe de Coordination pour l'Analyse de la Menace (OCAM) reçoit les informations permettant de faire les analyses générale et spécifique. Ces données proviennent des différents services d'appui. L'OCAM détermine de manière indépendante le niveau de la menace visé à l'article 8 de sa loi organique (Loi du 10 juillet 2006 relative à l'analyse de la menace).

L'OCAM remplit son rôle en toute indépendance. Cette indépendance est également bien fondée. Les deux ministres de tutelle (Justice et Intérieur) veillent uniquement à l'organisation et à l'administration générale de l'OCAM (article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace), mais c'est l'OCAM qui est responsable des évaluations de la menace (voir art. 8 de la loi). Ces évaluations sont communiquées aux membres du Conseil national de sécurité, à toute une série d'autres services, ainsi qu'au parquet et au membre compétent du Collège des procureurs. En d'autres termes, les évaluations vont directement au gouvernement et aux partenaires de l'OCAM, sans passer d'abord par les ministres de tutelle. Ces derniers sont, bien entendu, également destinataires des évaluations de la menace, mais sur un pied d'égalité avec les autres destinataires.

Les informations et les renseignements provenant des services d'appui sur lesquels l'OCAM se base, ne parviennent qu'à l'OCAM et ne sont pas disponibles pour les ministres de tutelle. Ainsi, les ministres de tutelle n'ont jamais une vision complète du contexte des évaluations de l'OCAM et ne peuvent donc pas les influencer ou les diriger. C'est d'autant plus vrai pour les informations classifiées ou sous embargo envoyées à l'OCAM.

On peut également se référer aux conclusions de la commission d'enquête parlementaire sur les attentats terroristes de 2016, qui insistent à plusieurs reprises sur la nécessité de maintenir l'OCAM en tant qu'organe indépendant: "L'Organe de coordination pour l'analyse de la menace a pour mission d'effectuer des évaluations stratégiques et ponctuelles sur les menaces terroristes

Met andere woorden, zodra de dreiging van terrorisme of extremisme ernstig of zeer ernstig is, is het noodzakelijk om de gegevensbewaring voor de geografische zones die onder dit niveau 3 of 4 vallen, te activeren, en dit zolang de dreiging niveau 3 of niveau 4 voortduurt. Immers, zelfs indien een evaluatie van niveau 4 naar niveau 3 gaat, moet de bewaring algemeen en ongedifferentieerd blijven om het hoofd te kunnen bieden aan de dreiging die reëel en actueel blijft.

Dit niveau van bedreiging 3 of 4 wordt vastgesteld door een instantie die onafhankelijk is van de diensten die de gegevens van de operatoren gebruiken

In de praktijk ontvangt het coördinatieorgaan voor dreigingsanalyse (OCAD) informatie die toelaat om algemene en specifieke analyses te doen. Deze gegevens zijn afkomstig van de verschillende ondersteunende diensten. Het OCAD beslist zelfstandig over het dreigingsniveau zoals bedoeld in artikel 8 van haar organieke wet (wet van 10 juli 2006 betreffende de dreigingsanalyse).

Het OCAD vervult zijn rol in alle onafhankelijkheid. Die onafhankelijkheid is ook goed onderbouwd. De twee voogdijministers (Justitie en Binnenlandse Zaken) waken over de organisatie en het algemene bestuur van het OCAD (artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging), maar het is het OCAD dat verantwoordelijk is voor de dreigingsevaluaties (zie art 8 van de wet). Deze evaluaties worden meegedeeld aan de leden van de Nationale Veiligheidsraad, en een hele reeks andere diensten, plus het parket en het bevoegde lid van het College van procureurs-generaal. De evaluaties gaan met andere woorden rechtstreeks naar de regering en de partners van het OCAD, zonder eerst te passeren bij de voogdijministers. Die zijn uiteraard ook bestemming van de dreigingsevaluaties, maar ten gelijke titel van de andere bestemmelingen.

De informatie en de inlichtingen van de ondersteunende diensten waarop het OCAD zich beroept, komen enkel bij het OCAD terecht, en staan niet ter beschikking van de voogdijministers. De voogdijministers hebben dus nooit een volledig zicht op context van de evaluaties van het OCAD, en kunnen dus de evaluaties niet beïnvloeden of sturen. Dit geldt des te meer voor geclassificeerde inlichtingen of inlichtingen die onder embargo worden toegestuurd aan het OCAD.

Er kan ook verwezen worden naar de conclusies van de parlementaire onderzoekscommissie naar de terroristische aanslagen van 2016, waar herhaaldelijk wordt aangedrongen op de nood om OCAD te handhaven als een onafhankelijk orgaan: "Het Orgaan voor de Coördinatie en Analyse van de Dreiging maakt analyses en strategische evaluaties over terroristische en

et extrémistes à l'encontre de la Belgique. Ce travail repose essentiellement sur l'analyse des informations transmises par d'autres services, notamment les services de renseignement, la police, l'Office des étrangers et les Affaires étrangères. L'OCAM fixe le niveau d'alerte et suggère les mesures à prendre en cas de relèvement du niveau d'alerte. Les évaluations d'alerte sont destinées aux diverses autorités politiques, administratives et judiciaires qui assument la responsabilité de la sécurité. Celles-ci doivent prendre les mesures appropriées afin d'écarter toute menace détectée. L'OCAM est placé sous l'autorité des ministres de l'Intérieur et de la Justice. Ce n'est pas un service de renseignement, il n'a pas de compétences opérationnelles et n'est pas intégré dans un autre service de sécurité, comme c'est le cas dans certains autres pays. La commission d'enquête estime important que l'OCAM puisse continuer à effectuer l'analyse d'alerte en toute indépendance."

Sur la base de ces constatations, la commission d'enquête a conclu qu'il n'était pas approprié que l'OCAM soit rattaché au Centre de crise.

Bien entendu, l'OCAM doit, sur la base des informations reçues par les services d'appui revoir *in concreto*, le niveau de la menace. En pratique, cette évaluation a lieu une fois par mois.

Afin de répondre à une remarque du Conseil d'État (point 7.2. de l'avis 69.381/4), il a été ajouté au texte qu'il s'agit des zones géographiques déterminées par l'Organe de Coordination pour l'Analyse de la Menace. Le Conseil d'État précise à juste titre qu'un niveau de menace peut être déterminé à l'égard d'une personne, d'un groupe ou d'un événement, et que dans la mesure où la détermination du niveau de menace concerne une personne ou un groupe limité, la menace ne peut pas toujours être localisée géographiquement. En effet, le projet de loi ne traite que des cas où elle peut être localisée dans une zone géographique. Cela est désormais également prévu explicitement dans le texte. La conservation des données s'appliquera à la zone géographique couverte par le niveau de la menace, et qui est déterminée de manière précise par l'OCAM, et ne visera jamais des individus ou des groupes spécifiques.

Dans le même temps, on ne peut nier qu'il existe une possibilité que le niveau de la menace soit fixé au niveau 3 pour l'ensemble du territoire. Cela signifierait qu'une conservation générale et indifférenciée des données serait prévue pour l'ensemble du territoire. Par analogie avec ce qui est prévu pour les services de renseignement, l'obligation de conservation des données devra dans ce cas être confirmée par arrêté royal. En l'absence d'un tel arrêté royal dans un délai d'un mois

extremistische dreigingen in en tegen België. Het doet dat vooral op basis van inlichtingen die het krijgt van andere diensten zoals de veiligheidsdiensten, de politie, de dienst Vreemdelingenzaken en Buitenlandse Zaken. Het OCAD bepaalt het dreigingsniveau en het suggereert welke maatregelen er moeten komen bij een verhoogde dreiging. De dreigingsevaluaties zijn bestemd voor de diverse politieke, administratieve en gerechtelijke overheden die verantwoordelijkheid dragen op het vlak van veiligheid. Zij moeten de gepaste maatregelen nemen om een gedetecteerde dreiging af te wenden. Het OCAD staat onder gezag van de ministers van Binnenlandse Zaken en Justitie. Het is geen inlichtingendienst, het heeft geen operationele bevoegdheden en het is ook niet, zoals in sommige andere landen wel het geval is, geïntegreerd in een andere veiligheidsdienst. De onderzoekscommissie vindt het belangrijk dat het OCAD de dreigingsanalyse onafhankelijk kan blijven maken."

Op basis van deze bevindingen concludeerde de onderzoekscommissie dat het dus niet aangewezen was om het OCAD bij het Crisiscentrum te voegen.

Uiteraard moet het OCAD, op basis van de door de ondersteunende diensten ontvangen informatie, het niveau van de dreiging *in concreto* herevalueren. In de praktijk wordt één keer per maand een evaluatie gemaakt.

Om tegemoet te komen aan een opmerking van de Raad van State (punt 7.2. van het advies 69.381/4) werd aan de tekst toegevoegd dat het gaat om de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse. De Raad van State stelt terecht dat een dreigingsniveau vastgesteld kan worden ten aanzien van een persoon, een groepering of een gebeurtenis, en dat in zoverre de vaststelling van het dreigingsniveau betrekking heeft op een persoon of een beperkte groepering, kan de dreiging niet altijd geografisch worden gelokaliseerd. Het wetsontwerp gaat inderdaad alleen over die gevallen waarin de dreiging lokaliseerbaar is in een geografisch gebied. Dit wordt nu ook expliciet bepaald in de tekst. De gegevensbewaring zal gelden voor het geografische gebied waarop het dreigingsniveau betrekking heeft en dat door OCAD nauwkeurig wordt bepaald, en zal nooit gericht zijn op bepaalde personen of groeperingen.

Tegelijk kan niet ontkend worden dat de mogelijkheid bestaat dat het dreigingsniveau op niveau 3 bepaald wordt voor het gehele grondgebied. Dit zou dan betekenen dat er voor het volledige grondgebied een algemene en ongedifferentieerde gegevensbewaring voorzien wordt. Naar analogie met wat voorzien is bij de inlichtingendiensten, zal de bewaarplicht in dit geval bevestigd moeten worden bij Koninklijk besluit. Bij ontstentenis van een dergelijk Koninklijk besluit binnen de maand nadat de

après la prise de décision, l'obligation de conserver les données prend fin et les opérateurs doivent supprimer les données qui ont déjà été conservées à cette fin.

Un tel arrêté royal confirme donc que les règles légales en vigueur sont applicables à une situation concrète, à savoir qu'il ressort de l'évaluation de la menace qu'une obligation de conservation s'applique à l'ensemble du territoire. En d'autres termes, aucune nouvelle règle de droit n'est créée. L'arrêté royal ne fait que ratifier une situation existante, et n'est donc pas un arrêté "réglementaire" au sens de l'article 3, § 1er des lois coordonnées sur le Conseil d'État. Toutefois, le législateur estime utile d'introduire cette ratification par le Roi, comme une garantie supplémentaire pour les opérateurs, qui disposent ainsi d'un point de référence juridique.

La conservation des données de localisation et de trafic dans les zones stratégiques (§ 3, points 3 à 5)

Les points 3 à 5 du paragraphe 3 sont aussi entièrement nouveaux et traitent de la limitation de l'obligation de conservation sur la base de critères géographiques. La Cour de Justice de l'Union européenne a jugé qu'une mesure prévoyant la conservation de données relatives au trafic et de données de localisation peut être définie sur la base d'un critère géographique, notamment s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave, ou que ces zones peuvent être la cible de menaces graves contre la sécurité publique.

Ce risque s'analyse notamment en termes de probabilité ou d'impact. Vu le caractère stratégique des zones reprises dans ces points, l'impact des actes de criminalité est d'office élevé.

Les points 3° à 5° énumèrent d'une part, les critères génériques qui peuvent être pris en compte dans la détermination des zones géographiques et mentionnent d'autre part, les zones géographiques qui répondent à ces critères tout en laissant par ailleurs au Roi, par arrêté délibéré en Conseil des ministres, la possibilité d'ajouter d'autres lieux stratégiques qui correspondent à ces critères. Il est d'emblée important de souligner que l'article en projet reprend les critères mentionnés par la Cour de justice tels que les lieux fréquentés par un grand nombre de personnes ou les lieux stratégiques, tels que les aéroports, les gares ferroviaires ou les gares de péage (§ 150 de l'arrêt du 6 octobre 2020). Ces critères sont précisés dans le présent article.

beslissing genomen is, zal de bewaarplicht komen te vervallen, en moeten de operatoren de tot dan toe en met dit doel bewaarde gegevens vernietigen.

Een dergelijk Koninklijk besluit bevestigt dus dat de bestaande wettelijke regels toepasselijk zijn op een concrete situatie, namelijk dat op basis van het dreigingsniveau blijkt dat een bewaarplicht geldt voor het gehele grondgebied. er worden m.a.w. geen nieuwe rechtsregels gecreëerd. Het Koninklijk besluit bekrachtigt slechts een bestaande situatie, en is geen "reglementair" besluit in de zin van artikel 3, § 1 van de gecoördineerde wetten op de Raad van State, omdat het geen rechtsregel formuleert De wetgever acht het echter wel nuttig om deze bekrachtiging door de Koning in te voeren, als een extra garantie voor de operatoren die zo een juridisch houvast hebben.

Bewaring van verkeers- en locatiegegevens op basis van strategische zones (§ 3, punten 3 tot 5)

De punten 3 tot 5 van paragraaf 3 zijn eveneens nieuw en hebben betrekking op de beperking van de bewaarplicht op basis van geografische criteria. Het Europees Hof van Justitie heeft geoordeeld dat een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens kan worden ingesteld op basis van een geografische criterium, met name indien op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat in een of meer geografische gebieden een groot risico bestaat op het voorbereiden of plegen van ernstige criminaliteit, of dat er plaatsen zijn waar de bewaring van gegevens als preventieve maatregel noodzakelijk is omdat zij het doelwit kunnen zijn van ernstige bedreigingen van de openbare veiligheid.

Dit risico wordt geanalyseerd in termen van waarschijnlijkheid of impact. Gezien het strategische karakter van de zones die onder deze punten vallen, is de impact van criminele daden automatisch groot.

De punten 3° tot 5° sommen enerzijds de algemene criteria op die in aanmerking kunnen worden genomen bij de bepaling van de geografische gebieden en vermelden anderzijds de geografische gebieden die aan deze criteria voldoen. De Koning kan hiernaast, bij een in Ministerraad overlegd besluit, andere strategische locaties die aan deze criteria voldoen, toevoegen. Dit ontwerp-artikel herneemt de door het Europees Hof van Justitie uitdrukkelijk genoemde criteria, zoals plaatsen die door een groot aantal mensen worden bezocht of strategische locaties, zoals luchthavens, spoorwegstations of tolstations (§ 150 van het arrest van 6 oktober 2020). Deze criteria worden in dit artikel nader omschreven.

Un seul critère est nécessaire pour établir qu'il faille à titre préventif réaliser une conservation de données sur un lieu.

Il faut d'emblée noter que, dès lors qu'un lieu est affecté à d'autres destinations, la conservation à titre préventif des données de trafic et de localisation sur ce lieu à titre de lieu stratégique (X) s'arrête, sauf, bien entendu s'il peut toujours constituer un autre lieu stratégique (Y). C'est d'ailleurs dans cette optique qu'il est stipulé que les autorités compétentes informent sans délai le NTSU des modifications de la destination des lieux.

Pour établir, ces lieux, le législateur s'est basé sur les intérêts à protéger visés à l'article 3 de la loi du 11 décembre 1998 relative à la classification et aux habilitations et avis de sécurité, soit:

— la défense de l'intégrité du territoire national et des plans de défense militaire;

— l'accomplissement des missions des forces armées;

— la sûreté intérieure de l'État, y compris dans le domaine de l'énergie nucléaire, et la pérennité de l'ordre démocratique et constitutionnel;

— la sûreté extérieure de l'État et les relations internationales de la Belgique;

— le potentiel scientifique et économique du pays;

— tout autre intérêt fondamental de l'État;

— la sécurité des ressortissants belges à l'étranger;

— le fonctionnement des organes décisionnels de l'État;

— la sécurité des témoins protégés;

— les matières nucléaires.

Le législateur a également tenu compte des missions des services de renseignement définies aux articles 7 et 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Sur cette base, le législateur a identifié toutes les zones présentant un lien avec ces intérêts.

Een plaats moet aan minstens één criterium voldoen om vast te stellen dat de bewaring van gegevens noodzakelijk is als preventieve maatregel.

Er dient onmiddellijk te worden opgemerkt dat, zodra een locatie een andere bestemming krijgt, de bewaring van verkeers- en locatiegegevens over deze locatie als strategische locatie (X) ophoudt, tenzij het door haar aard parallel ook nog een andere strategische locatie (Y) is. In dit verband is bepaald dat de bevoegde autoriteiten de NTSU in kennis moeten stellen van bestemmingswijzigingen van de plaatsen.

Om deze plaatsen vast te stellen, heeft de wetgever zich gebaseerd op de te beschermen belangen bedoeld in artikel 3 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, namelijk:

— de verdediging van de onschendbaarheid van het nationaal grondgebied en van de militaire defensieplannen;

— de vervulling van de opdrachten van de strijdkrachten;

— de inwendige veiligheid van de Staat, met inbegrip van het domein van de kernenergie, en het voortbestaan van de democratische en grondwettelijke orde;

— de uitwendige veiligheid van de Staat en de internationale betrekkingen van België;

— het wetenschappelijk en economisch potentieel van het land;

— elk ander fundamenteel belang van de Staat;

— de veiligheid van de Belgische onderdanen in het buitenland;

— de werking van de besluitvormingsorganen van de Staat;

— de veiligheid van beschermde getuigen;

— de nucleaire materies.

De wetgever hield ook rekening met de opdrachten van de inlichtingendiensten zoals omschreven in de artikelen 7 en 11 van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Op deze basis heeft de wetgever alle zones geïdentificeerd die een band hebben met deze belangen.

Pour ce qui concerne les zones particulièrement exposées à des risques élevés de criminalité grave, le législateur se réfère tout d'abord à des risques élevés de commission d'infractions visées à l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle.

Les risques élevés de criminalité grave se justifient sur la base de l'endroit où les faits sont finalement commis mais également sur la base des lieux où s'organisent ces actes graves, où transitent les membres des organisations criminelles qui les commentent ou d'autres lieux charnières pour la mise en place du processus de criminalité ou leur organisation opérationnelle.

Les lieux suivants sont repris comme critère permettant de réaliser une conservation de données de trafic et de localisation car ils constituent des zones particulièrement exposées à la commission d'actes de criminalité grave ou parce qu'ils sont exposés à des menaces pour la sécurité nationale:

— les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2., 3°, 4° et 5° de la Code de la Navigation; les gares ferroviaires, les stations de métro et de pré-métro; les aéroports:

Les lieux où il y a un transport de passagers sont en effet susceptibles d'être la cible d'actes de criminalité grave comme les attentats de Bruxelles en 2016 l'ont démontré (attentat à l'aéroport de Zaventem et à la station de métro de Maelbeek). Les aéroports et les ports sont bien entendu aussi des lieux où, par exemple, le trafic des êtres humains est organisé, ou encore l'import de stupéfiants. Il est certain à cet égard que ce n'est pas uniquement les grands aéroports/ports qui doivent être visés puisque, précisément dans le but de tenter d'échapper à un contrôle, des ports et des aéroports plus modestes sont parfois choisis comme zone pour commettre des infractions graves, par les organisations criminelles. Enfin, les gares et les alentours des gares sont également des lieux de rendez-vous entre groupes criminels, se rendant coupables de trafic de stupéfiants, leur importation et ensuite leur distribution.

Les bâtiments de l'administration des douanes et accises. Il s'agit de bâtiments dans lesquels des biens saisis sont entreposés. Il peut s'agir de quantité parfois élevée de drogues, d'armes ou de biens de valeur. Ces lieux sont dès lors particulièrement exposés à la commission d'actes de criminalité grave.

Les prisons: ces lieux représentent aussi un risque élevé au niveau de préparation d'actes d'évasion et parfois de trafic et de consommation de stupéfiants.

Met betrekking tot zones waar het risico op zware criminaliteit bijzonder groot is, verwijst de wetgever in de eerste plaats naar het grote risico op het plegen van de in artikel 90*ter*, §§ 2 tot 4 van het Wetboek van strafvordering bedoelde strafbare feiten.

Het hoge risico van zware criminaliteit wordt gerechtvaardigd op grond van de plaats waar de feiten uiteindelijk worden gepleegd, maar ook op grond van de plaatsen waar deze ernstige feiten worden georganiseerd, waar de leden van de criminele organisaties die zich ermee bezighouden, zich ophouden of andere belangrijke plaatsen voor het opzetten van het criminele proces of de operationele organisatie ervan.

De volgende plaatsen zijn opgenomen als criterium voor de bewaring van verkeers-en locatiegegevens omdat het zones zijn die bijzonder vatbaar zijn voor het plegen van zware criminaliteit of omdat zij blootstaan aan bedreigingen van de nationale veiligheid:

— de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2., 3°, 4° en 5° van het Scheepvaartwetboek, treinstations, metro- en pre-metrostations; luchthavens:

Plaatsen waar personenvervoer plaatsvindt, kunnen immers het doelwit zijn van criminele handelingen, zoals de aanslagen in Brussel in 2016 hebben aangetoond (aanslag op de luchthaven van Zaventem en het metrostation van Maelbeek). Luchthavens en havens zijn natuurlijk ook plaatsen waar mensenhandel wordt georganiseerd, of nog de invoer van drugs. Het is duidelijk dat in dit verband niet alleen grote luchthavens/havens moeten worden aangepakt, want juist in een poging om aan de controle te ontsnappen, worden kleinere havens en luchthavens soms gekozen door criminele organisaties. Tot slot zijn de stations en hun omgeving ook ontmoetingsplaatsen voor criminele groepen, die zich schuldig maken aan drugshandel, de invoer en vervolgens de distributie van drugs.

De gebouwen van de administratie Douane en Accijnzen. Dit zijn gebouwen waar in beslag genomen goederen worden opgeslagen. Het kan soms gaan om grote hoeveelheden drugs, wapens of waardevolle goederen. Deze plaatsen zijn derhalve bijzonder kwetsbaar voor het plegen van zware criminaliteit.

De gevangenissen: deze plaatsen vormen ook een verhoogd risico wat betreft (de voorbereiding van) ontsnappingen, drugshandel en -gebruik.

Les armuriers et les centres de tir: vu que ces lieux concentrent une quantité d'armes et de munitions, il est nécessaire de faire une conservation des données sur ces lieux.

Par ailleurs, le législateur a lui-même identifié à travers différent(e)s lois ou arrêtés royaux ces lieux stratégiques qui doivent faire l'objet d'une attention et d'une protection particulières car une atteinte à ces lieux aurait d'office une répercussion majeure au niveau de la sécurité nationale et parce qu'elles sont exposées à des risques élevés de criminalité grave.

— Il s'agit premièrement des sites nucléaires. Une attaque sur un site nucléaire constituerait en soi un incident grave qui nécessite le déclenchement de plans d'urgence, notamment pour porter secours à la population. En fonction de l'ampleur des dégâts, les intérêts vitaux de la population peuvent être touchés.

— Deuxièmement, vu les activités liées à la manipulation, la fabrication, l'emploi ou le stockage de substances dangereuses, les entreprises SEVESO peuvent, bien entendu, elles aussi constituer une cible "privilégiée" d'attentats ou d'actes malveillants. Un attentat sur un tel site constitue immédiatement une menace grave pour la sécurité nationale.

— Il s'agit troisièmement des communes dans lesquelles il y a une ou plusieurs infrastructures critiques telles que visées à l'article 1er la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et ses arrêtés d'exécution. Vu le lien entre ces infrastructures critiques et la production et les transports vitaux d'énergie, les points de jonction vitaux des transports, les maillons indispensables des systèmes de paiement électronique et des réseaux de communications électroniques, une atteinte à celles-ci constitue ipso facto une menace pour la sécurité nationale. En pratique, les infrastructures critiques peuvent être définies de manière large. Pour assurer dans ce cas une mise en œuvre proportionnée de l'article 126/1, on prendra en compte pour l'application de cet article les seuls éléments critiques du réseau (notion que l'on retrouve par exemple à l'article 8, alinéa 1er, 3°, de l'arrêté royal du 27 mai 2014 portant exécution dans le secteur des communications électroniques de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques).

Comme les adresses spécifiques des infrastructures critiques font l'objet d'une classification au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, elles ne peuvent pas en tant que telles être communiquées aux opérateurs. Par contre les communes qui hébergent

Wapenkamers en schietcentra: aangezien op deze plaatsen een hoeveelheid wapens en munitie wordt geconcentreerd, is het noodzakelijk gegevens over deze plaatsen te bewaren.

De wetgever heeft zelf, door middel van verschillende wetten of koninklijke besluiten, deze strategische locaties aangewezen die speciale aandacht en bescherming moeten krijgen, omdat een aanval op deze locaties automatisch grote gevolgen zou hebben voor de nationale veiligheid.

— Ten eerste, zijn er de nucleaire sites. Een aanval op een nucleaire site zou op zich een ernstig incident vormen dat de activering van noodplannen vereist, met name om de bevolking te redden. Afhankelijk van de omvang van de schade kunnen de vitale belangen van de bevolking worden aangetast.

— Ten tweede kunnen de SEVESO-bedrijven, gezien hun activiteiten gelieerd aan de behandeling, de productie, het gebruik of de opslag van gevaarlijke stoffen, ook een "geprivilegieerd" doelwit vormen voor aanslagen of kwaadwillige handelingen. Een aanslag op zo'n site vormt onmiddellijk een ernstige bedreiging voor de nationale veiligheid.

— Ten derde gaat het om de gemeenten waarbinnen zich één of meerdere kritieke infrastructuren bevinden zoals bedoeld in artikel 1 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren en zijn uitvoeringsbesluiten. Door het verband tussen deze kritieke infrastructuren en vitale energieproductie en -vervoer, vitale verkeersknooppunten, onmisbare schakels in elektronische betalingssystemen en elektronische communicatienetwerken, vormt een inbreuk hierop ipso facto een bedreiging voor de nationale veiligheid. In de praktijk kunnen kritieke infrastructuren ruim worden gedefinieerd. Om in dit geval een evenredige toepassing van artikel 126/1 te verzekeren, zullen enkel de kritieke elementen van het netwerk in aanmerking worden genomen voor de toepassing van dit artikel (een begrip dat onder meer terug te vinden is in artikel 8, eerste lid, 3°, van het koninklijk besluit van 27 mei 2014 tot uitvoering in de sector elektronische communicatie van artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren).

Aangezien de specifieke adressen van kritieke infrastructuur geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, kunnen zij niet als zodanig aan de operatoren worden meegedeeld. De gemeenten waar deze kritieke infrastructuren zich bevinden zijn

ces infrastructures critiques font l'objet d'une diffusion restreinte et peuvent dès lors sur la base du principe du besoin d'en connaître être communiquées aux opérateurs via le service désigné par le Roi, soit le service NTSU.

— Quatrièmement, les infrastructures des opérateurs étatiques qui assurent les communications en situation de crise telles les réseaux ASTRID ou BINII, doivent, comme l'intitulé le mentionne, offrir en cas de crise, une possibilité pour l'État de maintenir une communication de crise. Si ces infrastructures sont touchées, il n'y a potentiellement plus de communication étatique de crise, ce qui a immédiatement une répercussion grave au niveau de la sécurité nationale.

Prévoir une conservation des données s'appliquant à toute l'infrastructure ASTRID reviendrait *de facto* à recréer une data rétention nationale généralisée, puisque ce réseau spécifique fournit des capacités de communication aux services de secours et d'urgence dans toute la Belgique.

Toutefois, vu la nature des communications supportées par le réseau Astrid et leur importance pour l'aide aux victimes, la coordination des services d'urgence et d'intervention, il est essentiel que celui-ci bénéficie, au moins pour ses composants centraux critiques, d'une protection supplémentaire permettant de protéger son infrastructure.

L'infrastructure qui soutient les services ASTRID (le réseau de radiocommunication, le réseau de rappel de personnes (paging), BLM, les centres d'appels d'urgence, etc.) est composée de divers équipements critiques dans le sens fonctionnel du terme. Ils sont répartis sur tout le territoire.

Il s'agit du siège social d'ASTRID (centre de supervision des systèmes, du site de *Disaster Recovery*), des Centres de Données Centraux (CDC), des Centres de Données Provinciaux (PDC, généralement localisés avec les CIC et NCU112) et des mâts radio.

Le texte proposé par le législateur concerne donc uniquement le siège social d'ASTRID, les 2 centres de données centraux et les 12 centres de données provinciaux. Ces derniers sont composés des centres dispatching CIC et des Centres 112. Pour des raisons opérationnelles, plusieurs CIC provinciaux sont logés dans les mêmes lieux que les centres 112. De ce fait, ils ne sont que 12 sur le territoire belge.

Le raisonnement employé pour ASTRID s'applique par analogie au système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7 de l'arrêté

echter onderworpen aan een behandeling op niveau "beperkte verspreiding" en kunnen zij dus, op basis van het "need-to-know"-beginsel, aan de operatoren worden meegedeeld via de door de Koning aangewezen dienst, namelijk de NTSU.

— Ten vierde moeten de infrastructuren van staatsbedrijven die de communicatie in crisissituaties waarborgen, zoals het ASTRID- of het BINII-netwerk, de staat, zoals de titel vermeldt, de mogelijkheid bieden om de crisiscommunicatie in crisissituaties in stand te houden. Indien deze infrastructuren worden aangetast, is er potentieel geen crisiscommunicatie van de staat meer mogelijk, hetgeen onmiddellijk ernstige gevolgen heeft voor de nationale veiligheid.

Het voorzien van de verplichting tot gegevensbewaring voor de hele ASTRID-infrastructuur zou *de facto* neerkomen op een algemene nationale gegevensbewaring, aangezien dit specifieke netwerk de nood- en reddingsdiensten in heel België communicatiecapaciteit biedt.

Gezien de aard van de door het ASTRID-netwerk ondersteunde communicatie en het belang ervan voor slachtofferhulp, coördinatie van nooddiensten en interventiediensten, is het echter van essentieel belang dat het ASTRID-netwerk, althans voor zijn kritische kerncomponenten, over aanvullende bescherming beschikt om zijn infrastructuur veilig te stellen.

De infrastructuur ter ondersteuning van de ASTRID-diensten (het radiocommunicatie-netwerk, het oproepnetwerk van personen (paging), de BLM, de alarmcentrales, …) bestaat uit verschillende uitrustingen die van cruciaal belang zijn in de functionele zin van het woord. Ze zijn over het hele grondgebied verspreid.

Het gaat om de zetel van de NV ASTRID (het systeemtoezichtcentrum, de site van *Disaster Recovery*), de centrale datacentra (CDC), de provinciale datacentra (PDC, gewoonlijk gevestigd bij de CIC's en NCU112) en de zendmasten.

De door de wetgever voorgestelde tekst heeft dus alleen betrekking op het hoofdkantoor van ASTRID, de 2 centrale datacentra en de 12 provinciale datacentra. Deze laatste zijn samengesteld uit de dispatchcentra en de 112 Centra. Om operationele redenen zijn verschillende provinciale CIC's gehuisvest op dezelfde locaties als de 112 centra. Er zijn er dus maar 12 op het Belgische grondgebied.

De redenering die wordt gebruikt voor ASTRID is van overeenkomstige toepassing op het beveiligde en versleutelde communicatie- en informatiesysteem

royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace.

Ce système est utilisé pour la communication d'informations entre l'OCAM et les services d'appui. Le nom et la structure du système sont susceptibles d'évoluer dans le temps.

Les éléments critiques de ce système sont à ce jour 2 centres de données centraux et 6 nœuds de communication Bemilnet.

— Enfin, les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de services essentiels constituent eux aussi des "lieux cybers" qui peuvent faire l'objet d'attaques ciblées lesquelles auraient une répercussion sur la sécurité nationale.

Un autre critère concerne la menace grave potentielle au sein de la zone pour les intérêts vitaux du pays ou les besoins essentiels de la population.

Ce que l'on entend par intérêts vitaux ou besoins essentiels est subdivisé en 6 catégories, dont 4 sont extraites du plan d'urgence cybernétique: l'ordre public, le potentiel scientifique et économique du pays, la souveraineté nationale et les institutions établies par la Constitution et les lois, et l'intégrité du territoire national. La cinquième catégorie est le transport et la sixième, reprise de l'article 23.1.e du RGPD concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale.

La potentialité de la menace désigne des dangers dont l'existence n'est pas au moment où elle est appréhendée, établie ou dont la probabilité n'est pas encore démontrée.

Au niveau de l'ordre public, deux catégories de zones sont déterminées dans l'article en projet. Il s'agit des zones neutres (exemple zone neutre de Bruxelles) soit le périmètre au sein duquel il est interdit de manifester et des cabinets ministériels. Vu que ces zones englobent les lieux de pouvoir, la violation de ces zones entraîne un risque élevé que certaines structures de pouvoir ne puissent plus se réunir et prendre les mesures adéquates.

En termes de potentiel scientifique et économique, la menace est, par exemple, automatiquement grave lorsqu'elle concerne la recherche universitaire ou scientifique dans les vastes domaines de la micro- et de la

bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging.

Dit systeem wordt gebruikt voor de communicatie van informatie tussen OCAD en de ondersteunde diensten. De naam en structuur van het systeem kunnen in de loop of tijd veranderen.

De kritische elementen van dit systeem zijn momenteel 2 datacentra en 6 Bemilnet-communicatieknooppunten.

— Ten slotte, de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen, zijn ook "cyberplaatsen" die het voorwerp kunnen zijn van gerichte aanvallen die gevolgen zouden hebben voor de nationale veiligheid.

Een ander criterium betreft de mogelijke ernstige bedreiging binnen het gebied voor de vitale belangen van het land of de essentiële behoeften van de bevolking.

Wat wordt verstaan onder vitale belangen of essentiële behoeften is onderverdeeld in zes categorieën, waarvan er vier zijn overgenomen uit het cybernoodplan: de openbare orde, het wetenschappelijk en economisch potentieel van het land, de nationale soevereiniteit en de bij de grondwet en de wetten opgerichte instellingen, en de integriteit van het nationale grondgebied. De vijfde categorie is het transport en de zesde, overgenomen uit artikel 23.1.e van de AVG behelst de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid.

De mogelijkheid van de dreiging heeft betrekking op gevaren waarvan het bestaan nog niet is vastgesteld of waarvan de waarschijnlijkheid nog niet is aangetoond.

Wat de openbare orde betreft, worden in het ontwerpartikel twee categorieën van zones bepaald. Dit is de neutrale zone , (bijvoorbeelde neutrale zone van Brussel), dat wil zeggen de zone waarbinnen betogingen verboden zijn en de ministeriële kabinetten. Aangezien deze zones de machtscentra omvatten, houdt de schending van deze zones een groot risico in dat bepaalde machtsstructuren niet meer kunnen vergaderen en geen passende maatregelen meer kunnen nemen.

Wat betreft het wetenschappelijk en economisch potentieel is de dreiging bijvoorbeeld automatisch ernstig wanneer zij betrekking heeft op academisch of wetenschappelijk onderzoek op de brede wetenschapsdomeinen

nanoélectronique, de la biotechnologie et de la technologie à large bande. Il s'agit donc notamment des "centres de recherche stratégiques" reconnus par la Région flamande et des "centres de recherches agréés" reconnus par la Région wallonne.

La liste des personnes morales belges dont le potentiel économique et/ou scientifique doit être protégé est établie par les 2 services PES (potentiel économique et scientifique) des services de renseignement lesquels, sur la base de leur loi organique, ont comme mission la protection du potentiel scientifique et économique du pays (articles 7, 1° et 11, § 1er, c) de la loi organique des services de renseignement et de sécurité).

Cette liste est établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la sécurité sur proposition des ministres de la Justice et de la Défense et approuvée par le Conseil national de sécurité.

En ce qui concerne les transports, les autoroutes constituent un réseau de transport essentiel de notre pays, grâce auquel l'approvisionnement doit pouvoir être assuré en cas d'urgence.

Les autoroutes sont également des lieux où s'exercent toute une série d'actes de criminalités spécifiques, mais également des lieux qui interviennent comme voies de fuite pour des groupes criminels qui viennent de les commettre: car-jacking, home jacking, bande itinérante, hold-up.

Les parkings publics attenants sont également inclus: C'est autour de ces parkings que régulièrement (quasi journalièrement) se rassemblent des groupes de victimes de traite des êtres humains, dans l'attente d'une prise en charge par une organisation criminelle qui exploite la prise en charge du transit de ces personnes vers d'autre pays.

C'est le lieu où le transporteur va s'arrêter avant de les prendre en charge.

Les parkings d'autoroutes reviennent régulièrement comme lieux où des membres d'organisations criminelles se rencontrent, ont des rendez-vous, échangent des stupéfiants contre payement, etc.

Ces lieux ne sont donc pas répertoriés comme le lieu final de l'exécution de l'infraction grave, mais bien comme un lieu essentiel à la criminalité. Il est dès lors indispensable de pouvoir obtenir des informations pour éviter que des actes criminels ne s'exécutent ou le cas

van micro- en nano-elektronica, biotechnologie en breedbandtechnologie. Daardoor worden hiermee de "strategische onderzoekscentra" bedoeld zoals erkend door het Vlaams gewest, alsook de "centres de recherches agréés" zoals erkend door het Waals Gewest.

De lijst van de Belgische rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel moet worden beschermd, wordt opgesteld door de twee diensten EWP (economisch en wetenschappelijk potentieel) van de inlichtingendiensten die, op grond van hun organieke wet, tot taak hebben het wetenschappelijk en economisch potentieel van het land te beschermen (artikelen 7, 1° en 11, § 1, c) van de organieke wet inzake de inlichtingen- en veiligheidsdiensten).

Deze lijst wordt wordt opgesteld door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid op voorstel van de ministers van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad.

Wat betreft het transport vormen de autosnelwegen een essentiële netwerk van transport in ons land, waarlangs de bevoorrading in noodsituaties moet kunnen verzekerd worden.

De autosnelwegen zijn ook plaatsen waar een hele reeks specifieke criminele daden wordt gepleegd, maar ook plaatsen die fungeren als ontsnappingsroute voor criminele groepen die zich er net aan schuldig hebben gemaakt: carjacking, homejacking, rondtrekkende bendes, hold-ups.

Ook de bijhorende openbare parkeerterreinen vallen hieronder: het is rond deze parkeerterreinen dat zich regelmatig (bijna dagelijks) groepen slachtoffers van mensenhandel verzamelen, wachtend om te worden opgehaald door een criminele organisatie die de doorvoer van deze personen naar andere landen exploiteert.

Het is ook de plaats waar de transporteur zal stoppen alvorens deze personen mee te nemen.

Parkeerterreinen van autosnelwegen worden regelmatig gebruikt als plaatsen waar leden van criminele organisaties elkaar ontmoeten, afspraken maken, drugs uitwisselen tegen betaling, enz.

Deze plaatsen worden dus niet op de lijst geplaatst als de uiteindelijke plaats van uitvoering van het ernstige misdrijf, maar als een sleutelplaats voor de criminaliteit. Daardoor is het van essentieel belang om informatie te kunnen inwinnen om te voorkomen dat deze strafbare

échéant pour identifier les personnes qui font partie des organisations criminelles qui s'en rendent coupables.

Au niveau de la souveraineté nationale et des institutions établies par la Constitution, les lois, les décrets ou les ordonnances, l'ensemble des lieux suivants peuvent faire l'objet d'une menace potentielle et grave. La menace est d'office grave lorsqu'elle touche les lieux qui symbolisent la souveraineté nationale et les institutions établies par la Constitution, les lois, les décrets ou ordonnances.

Il s'agit premièrement des différents parlements du pays et qui sont visés au chapitre II et IV de la Constitution. À ce titre, il s'agit aussi de protéger les assemblées législatives au niveau communal et provincial. En effet, il s'agit d'offrir une protection uniforme à tous les élus qui représentent la nation. Les maisons communales sont dès lors également mentionnées. Cela concerne non seulement l'hôtel de ville sensu stricto, mais aussi les bâtiments de l'administration municipale. Il s'agit des lieux où sont prises des décisions politiques, et où sont produits les documents administratifs originaux (cartes d'identité, passeports, actes d'état civil, permis de conduire, etc.).

Il s'agit deuxièmement de protéger le Roi et donc concrètement de permettre de réaliser une conservation de données de trafic et de localisation près du palais royal et des domaines royaux qui font d'ailleurs l'objet d'autres protections spécifiques.

Il s'agit troisièmement d'apporter une protection d'une part aux bâtiments du pouvoir judiciaire, soit aux cours et tribunaux du pouvoir judiciaire visés au chapitre VI de la Constitution et au Conseil d'État visé au chapitre VII de la Constitution. L'ensemble des juridictions et les bâtiments de l'ordre judiciaire: dans le cadre de la tenue de procès, ces lieux constituent l'objet de menaces. Pour prévenir ces menaces ou enquêter, une conservation de données sur ces lieux est nécessaire, et ce, même en dehors de la tenue d'un procès, vu que ces lieux symbolisent la Justice et sont donc susceptibles de faire l'objet d'actes de criminalité grave. Ce point ne vise pas uniquement les juridictions de l'ordre judiciaire dans la mesure où les autres bâtiments qui accueillent du personnel de l'ordre judiciaire sont également susceptibles d'être la cible d'attentats. Le Conseil d'État a fait remarquer à juste titre que cette zone était placée sous deux catégories différentes dans l'avant-projet, ce qui pouvait prêter à confusion. Le législateur choisit de maintenir les bâtiments du pouvoir judiciaire au point 4°.

feiten worden gepleegd of, zo nodig, om de personen te identificeren die deel uitmaken van de criminele organisaties die ervoor verantwoordelijk zijn.

Wat betreft de nationale soevereiniteit en de instellingen die bij de grondwet en wetten, decreten of verordeningen zijn opgericht, kunnen alle volgende plaatsen aan een potentiële en ernstige bedreiging worden blootgesteld. De dreiging is automatisch ernstig wanneer zij plaatsen treft die symbool staan voor de nationale soevereiniteit en de instellingen die zijn opgericht bij de grondwet of bij wetten, decreten of verordeningen.

Dit zijn in de eerste plaats de verschillende parlementen van het land waarnaar in de hoofdstukken II en IV van de Grondwet wordt verwezen. In dit verband gaat het er ook om de wetgevende vergaderingen op gemeentelijk niveau te beschermen. Het gaat er immers om alle verkozen vertegenwoordigers van de natie een uniforme bescherming te bieden. Daarom worden ook de gemeentehuizen vernoemd. Het gaat hier niet alleen om het stadhuis sensu strictu, maar ook om de gebouwen van de gemeentelijke administratie. Dit zijn plaatsen waar politieke beslissingen worden genomen, en waar originele administratieve documenten geproduceerd worden (identiteitskaarten, paspoorten, akten van de burgerlijke stand, rijbewijzen, …).

In de tweede plaats gaat het om de bescherming van de koning en gaat het er dus concreet om verkeers- en locatiegegevens op te slaan in de buurt van het koninklijk paleis en de koninklijke domeinen, die ook een andere specifieke bescherming genieten.

Ten derde gaat het om de bescherming van de gebouwen van de rechterlijke macht, d.w.z. de rechtbanken en gerechtshoven van de rechterlijke macht bedoeld in hoofdstuk VI van de Grondwet en de Raad van State bedoeld in hoofdstuk VII van de Grondwet. De hoven en rechtbanken en de gebouwen van de rechterlijke macht: in het kader van de procesvoering zijn deze plaatsen blootgesteld aan dreigingen. Om deze dreigingen te voorkomen of om onderzoek te voeren, is het noodzakelijk gegevens over deze plaatsen bij te houden, zelfs buiten het kader van een proces, aangezien deze plaatsen symbool staan voor justitie en dus ook het voorwerp kunnen zijn van ernstige criminaliteit. Het is niet voldoende om enkel de hoven en rechtbanken als mogelijk doelwit te hernemen, aangezien ook andere gebouwen waarin justitieel personeel is gehuisvest, vatbaar zijn voor aanslagen. De Raad van State wees er terecht op dat deze zone onder twee verschillende categorieën werd geplaatst in het voorontwerp, wat voor verwarring zou kunnen zorgen. De wetgever kiest ervoor om de gebouwen van de rechterlijke macht onder punt 4° te behouden.

Il s'agit aussi des protéger les corps qui représentent la force publique au sens du titre VI de la Constitution, soit la police et les militaires. Comme il s'agit de protéger des lieux avec une menace grave et potentielle, la protection porte respectivement sur les postes de police et les domaines militaires. Les bâtiments affectés à la police fédérale et à la police locale sont en effet de lieux qui représentent la puissance publique de l'État et dans lesquels des armes et munitions, des uniformes ou des biens saisis dont notamment de la drogue, sont stockés. Du matériel technologique spécifique est aussi stocké dans certaines unités de police. À ces titres, ils peuvent bien entendu constituer la cible d'attentat, d'actes de violence ou de vols, comme cela a déjà été le cas par le passé (postes de police de Verviers et de Charleroi). Cela s'applique également à la Sûreté de l'État. Le Conseil d'État a fait remarquer à juste titre que cette zone était placée sous deux catégories différentes dans l'avant-projet, ce qui pouvait prêter à confusion. Le législateur choisit de conserver les bâtiments destinés à la police fédérale et locale et à la Sûreté de l'État sous le point 4°.

Les domaines militaires sont des zones particulièrement exposées à des menaces pour la sécurité nationale et à la commission d'actes de criminalité grave. En effet, sont stockés dans les domaines militaires des armes, des munitions, des explosifs, des systèmes d'armes, du matériel à haut potentiel technologique, du matériel, des documents et des systèmes informatiques classifiés, du matériel pour assurer la sécurité aérienne, … Ces éléments font l'objet de convoitise de la part notamment de certains mouvements extrémistes et de services de renseignement étrangers. Seules les communes seront communiquées et pas les sites précis. Ceci s'explique par la sensibilité des quartiers militaires. En effet, nombreux sont classifiés. Il n'est donc pas envisageable de donner un point précis sur une carte à tous les opérateurs. Pour rappel, l'article 120*ter* du Code pénal punit quiconque fera des photos dans un rayon de 10km autour d'établissements militaires. Vu ce caractère sensible, couvrir les communes dans lesquelles se trouvent des domaines militaires est proportionné. Le Conseil d'État a fait remarquer à juste titre que cette zone était placée sous deux catégories différentes dans l'avant-projet, ce qui pouvait prêter à confusion. Le législateur choisit de conserver les communes dans lesquelles se trouvent des domaines militaires sous le point 4°.

Au niveau de l'intégrité du territoire national, les communes frontalières doivent être soumises à une conservation des données. En cas d'attaque ou d'invasion, ces communes constituent des lieux stratégiques pour la souveraineté nationale. Les communes frontalières ont été retenues comme zones géographiques dans la

Tenslotte gaat het om de bescherming van de organen die de openbare macht vertegenwoordigen in de zin van Titel VI van de Grondwet, namelijk de politie en het leger. Aangezien het gaat om de bescherming van plaatsen met een ernstige en potentiële dreiging, betreft de bescherming respectievelijk politiebureaus en militaire domeinen. De gebouwen toegewezen aan de federale en lokale politie zijn plaatsen die de openbare macht van de Staat vertegenwoordigen en waar wapens en munitie of in beslag genomen goederen, met inbegrip van drugs, worden opgeslagen. Specifiek technologisch materiaal is eveneens opgeslagen bij bepaalde politieeenheden. Als zodanig kunnen zij uiteraard het doelwit van aanslagen zijn, zoals in het verleden reeds het geval is geweest (politiebureaus van Verviers en Charleroi). Dit geldt in dezelfde mate voor de Veiligheid van de Staat. De Raad van State wees er terecht op dat deze zone onder twee verschillende categorieën werd geplaatst in het voorontwerp, wat voor verwarring zou kunnen zorgen. De wetgever kiest ervoor om de gebouwen bestemd voor de federale en de lokale politie en voor de Veiligheid van de Staat onder punt 4° te behouden.

Militaire domeinen zijn gebieden die in het bijzonder blootstaan aan bedreigingen voor de nationale veiligheid en aan het plegen van ernstige strafbare feiten. Wapens, munitie, explosieven, wapensystemen, uitrusting met een hoog technologisch potentieel, geclassificeerd materiaal, documenten en computersystemen, uitrusting voor het waarborgen van de veiligheid van het luchtverkeer, enz. liggen namelijk opgeslagen in militaire zones. Deze elementen zijn begeerd door bepaalde extremistische bewegingen en buitenlandse inlichtingendiensten. Alleen de gemeenten zullen worden meegedeeld en niet de precieze locaties. Dit is te wijten aan de gevoeligheid van militaire kwartieren. Inderdaad, velen van hen zijn geclassificeerd. Het is dus niet mogelijk om alle operatoren een precies punt op een kaart te geven. Ter herinnering: artikel 120*ter* van het Wetboek van Strafrecht stelt eenieder strafbaar die foto's neemt binnen een straal van 10 km van militaire inrichtingen. Gezien deze gevoelige aard is het evenredig de gemeenten waarin zich militaire domeinen bevinden, in het toepassingsgebied op te nemen. De Raad van State wees er terecht op dat deze zone onder twee verschillende categorieën werd geplaatst in het voorontwerp, wat voor verwarring zou kunnen zorgen. De regering kiest ervoor om de gemeenten waar zich militaire domeinen bevinden onder punt 4° te behouden.

Wat de nationale territoriale integriteit betreft, zijn de grensgemeenten onderworpen aan de verplichting tot gegevensbewaring. In geval van een aanval of invasie zijn deze gemeentes van strategisch belang voor de nationale soevereiniteit. De grensgemeenten zijn in de gerichte bewaring in aanmerking genomen als geografische

conservation ciblée, étant donné que la pratique montre que des groupes d'individus (bandes urbaines, organisations criminelles, etc.) venant de l'étranger commettent des infractions pénales en Belgique comme l'organisation de trafic de stupéfiants, des coups et blessures, vols de voiture et conduite dangereuse ("Joy riding") et que des groupes d'individus résidant en Belgique passent la frontière pour commettre de telles infractions.

Enfin, les hôpitaux et la BNB, respectivement pour le domaine de la santé et le domaine économique, sont des zones vitales pour les besoins essentiels de la population. Hacker des hôpitaux par exemple constituerait une menace grave pour ces intérêts.

Le dernier critère concerne la menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national.

Ce critère nécessite peu d'explications: la Belgique est le siège d'un certain nombre d'institutions internationales qui, en raison de leur nature, peuvent faire l'objet de menaces graves. Il s'agit en premier lieu des bâtiments affectés à l'Union européenne, des bâtiments et infrastructures affectés à l'OTAN, des bâtiments des institutions de l'Espace économique européen et des bâtiments des Nations Unies. Selon ce critère, les bâtiments des ambassades et des représentations diplomatiques situés en Belgique sont également considérés comme des zones nécessitant la conservation de données.

Le Conseil d'État demande au point 4.2.3. de son avis 69.381/4 de fixer dans la loi ou dans un arrêté royal les critères concrets et techniques à prendre en compte pour définir le périmètre de la zone de manière telle que les zones relevant d'une même catégorie soient définies selon la même méthodologie. Pour le 1er critère, soit les arrondissements judiciaires et les zones de police, la loi définit précisément leur contour. Pour le second critère, c'est à chaque fois l'OCAM qui indiquera dans son analyse la délimitation géographique précise. Pour les critères 3° à 5°, Le Roi déterminera par type de zone, l'étendue du périmètre.

Le législateur a donc prévu:

— que les zones géographiques sont juridiquement définies soit dans le présent projet de loi, soit dans un arrêté royal;

— que le périmètre de ces zones est précisé soit dans la loi, soit dans un arrêté royal;

gebieden aangezien uit de praktijk blijkt dat groepen van individuen (stadsbendes, criminele organisaties, enz.) vanuit het buitenland in België strafbare feiten komen plegen, zoals de organisatie van drugshandel, slagen en verwondingen, autodiefstal en gevaarlijk rijden ("joyriding") en dat groepen van individuen die in België verblijven de grens oversteken om daar zulke inbreuken te plegen.

Ten slotte zijn in de gezondheidssector, de ziekenhuizen en in de economische en financiële sector, de NBB van vitaal belang voor de basisbehoeften van de bevolking. Het hacken van ziekenhuizen, bijvoorbeeld, zou een ernstige bedreiging voor deze belangen vormen.

Het laatste criterium betreft de mogelijke ernstige bedreiging voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen.

Dit criterium behoeft weinig uitleg: België is de zetel van een aantal internationale instellingen die vanwege hun aard mogelijke ernstige bedreigingen kunnen ondervinden. Het gaat hier in eerste instantie om de gebouwen bestemd voor de Europese Unie, de gebouwen en de infrastructuren bestemd voor de NAVO, de gebouwen van de instellingen van de Europese Economische Ruimte, en de gebouwen van de Verenigde Naties. Onder dit criterium worden ook de gebouwen van de ambassades en van de diplomatieke vertegenwoordigingen die zich in België bevinden beschouwd als een zone waarvoor een gegevensbewaring noodzakelijk is.

In punt 4.2.3. van zijn advies 69.381/4 vraagt de Raad van State dat in de wet of in een koninklijk besluit de concrete en technische criteria worden vastgesteld die in aanmerking genomen moeten worden om de omvang van de zone te bepalen, opdat de zones die tot eenzelfde categorie behoren volgens dezelfde methodologie bepaald zouden worden. Voor het eerste criterium, namelijk de gerechtelijke arrondissementen en de politiezones, beschrijft de wet precies hun draagwijdte. Wat het tweede criterium betreft, is het OCAM die in zijn analyse de precieze geografische afbakening zal aangeven. Voor de criteria 3° tot 5° bepaalt de Koning voor elk type zone de omvang van de perimeter.

De wetgever heeft dus voorzien:

— dat de geografische zones juridisch gedefinieerd worden hetzij in de wet, hetzij bij Koninklijk besluit;

— dat de perimeter van deze zones gepreciseerd wordt in de wet of in een koninklijk besluit;

— que les autorités débitrices d'informations, c'est-à-dire, celles qui doivent fournir les données qui correspondent aux définitions des lieux sont précisées dans un arrêté royal;

— que la liste des lieux dressée sur ces bases est approuvée par les ministres de la Justice, de l'Intérieur et de la Défense (voir *infra*).

Dans le point 125 de son avis, l'APD indique qu' "l'autorité souligne que le législateur doit bien veiller, au cours de la délibération précédant le vote, à apprécier la nécessité et la proportionnalité de la sélection des différents lieux retenus" et qu'"il importe, en tout état de cause, que cette sélection de lieux n'aboutisse pas à réintroduire, de facto, une obligation de conservation indifférenciée des données d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique".

Le site internet de l'Autorité de protection des données indique à propos du principe de proportionnalité que "le principe de proportionnalité qui est défini dans le RGPD est le principe en vertu duquel on ne peut traiter que des données personnelles adéquates, pertinentes et non excessives au vu de la finalité pour laquelle elles ont été obtenues". Ceci est repris à l'article 5, 1°, c du RGPD. À cet égard, le législateur insiste sur le caractère différencié et objectif, en fonction des intérêts supérieurs identifiés à l'article 126/1, de la conservation des données mise en place. Les types et catégories de données pertinentes adéquates et non excessives sont précisées dans l'arrêté royal qui exécutera l'article 126/1.

Par ailleurs, l'APD, aux points 125 et 126 de son avis, a rappelé l'importance du principe de nécessité et de proportionnalité dans la définition des lieux visés. En ce sens, chaque lieu déterminé a fait l'objet d'un examen approfondi et justifié de manière détaillée ci-dessus. Il n'est pas apparu néanmoins possible de déterminer une proportion fixe en termes de pourcentage d'utilisateurs visés qui serait considérée comme trop importante. En effet, il n'existe pas en tant que tel un "nombre d'or" en matière de conservation des données qui représenterait la proportionnalité absolue et maximale de la population visée (par exemple 91, 61 ou 41 pour cent de la population).

Le législateur est intimement convaincu que c'est le caractère à la fois général et indifférencié de la conservation des données qui est rejeté dans les arrêts de la Cour de Justice, précisément parce qu'une telle conservation générale et indifférenciée ne permet pas de "répondre à des critères objectifs, établissant un rapport entre les

— dat de autoriteiten die verantwoordelijk zijn voor het verstrekken van informatie, d.w.z. die de gegevens moeten verstrekken die overeenkomen met de definities van de zones, in een koninklijk besluit worden vermeld;

— dat de lijst van de zones opgesteld op deze basis goedgekeurd wordt door de ministers van Justitie, Binnenlandse Zaken en Defensie (zie verder).

In punt 125 van zijn advies bepaalt de GBA dat "de Autoriteit benadrukt dat de wetgever er bij de beraadslaging die de stemming voorafgaat op moet toezien dat de noodzaak en evenredigheid van de keuze van de verschillende weerhouden plaatsen wordt beoordeeld" en dat "Het is in ieder geval van belang dat deze keuze van locaties niet leidt tot de feitelijke herinvoering van een verplichting om de gegevens van een te groot deel van de gebruikers van elektronische communicatie in België te bewaren".

Op de website van de Gegevensbeschermingsautoriteit staat met betrekking tot het evenredigheidsbeginsel het volgende: "Het evenredigheidsbeginsel dat is vastgelegd in de AVG is het beginsel dat stelt dat alleen gepaste, relevante en niet-overdreven persoonsgegevens, ten opzichte van het doel waarvoor ze worden verkregen, kunnen worden verwerkt." Dit is opgenomen in artikel 5, 1°, c van de AVG. In dit verband benadrukt de wetgever het gedifferentieerde en objectieve karakter van de gegevensbewaring overeenkomstig de in artikel 126/1 genoemde dwingende belangen die moeten worden gevrijwaard. De soorten en categorieën van gegevens die gepast, relevant en niet-overdreven zijn, worden nader omschreven in het koninklijk besluit dat artikel 126/1 zal uitvoeren.

Voorts heeft de GBA in de punten 125 en 126 van zijn advies herinnerd aan het belang van het noodzakelijkheids- en het evenredigheidsbeginsel bij de bepaling van de betrokken plaatsen. In die zin is elke vastgestelde locatie grondig onderzocht en hierboven uitvoerig verantwoord. Het bleek echter niet mogelijk een vast percentage te bepalen van het aantal gebruikers dat onder de regeling zou vallen en dat als te hoog zou worden beschouwd. Er is immers geen "gouden getal" als zodanig voor gegevensbewaring dat het absolute en maximale aandeel van de geviseerde bevolking zou vertegenwoordigen (bijvoorbeeld 91, 61 of 41 % van de bevolking).

De wetgever is er vast van overtuigd dat juist het algemene en ongedifferentieerde karakter van de bewaring van gegevens in de arresten van het Hof van Justitie wordt verworpen, net omdat een dergelijke algemene en ongedifferentieerde bewaring het niet mogelijk maakt om "te voldoen aan objectieve criteria, waarbij een

données à conserver et l'objectif poursuivi". Tel n'est pas le cas dans les points 3° à 5° prévus au § 3 de l'article 126/1 où à chaque fois un intérêt supérieur justifiant la conservation préventive des données est identifié. Le législateur a souhaité justifier de manière précise les raisons pour lesquelles l'obligation de conservation ciblée pour chacune des zones visées est considérée comme nécessaire et proportionnée.

Eu égard à l'arrêt de la Cour de Justice européenne du 6 octobre 2020, le législateur insiste encore une fois sur le caractère proportionné du système mis en place dans ce projet de loi, portant sur une conservation ciblée des données relatives au trafic et des données de localisation, aux fins de la lutte contre la criminalité grave, de la sauvegarde de la sécurité nationale et de la prévention des menaces graves contre la sécurité publique, sur la base d'éléments objectifs et non discriminatoires au moyen d'un critère géographique.

Délégation au Roi

Pour répondre à une remarque dans le point 4.2.4. de l'avis du Conseil d'État, le législateur confirme que le Roi n'a pas de marge d'appréciation pour déterminer des zones géographiques additionnelles. Une zone additionnelle doit absolument correspondre à un des critères prévus au § 3 points 3°à 5°.

Enfin, pour répondre à la remarque du Conseil d'État dans le point 4.3.1. de l'avis, le législateur tient à préciser qu'il n'est pas requis de faire un accord de coopération, avec les Régions et/ou les Communautés, relatifs aux autorités compétentes débitrices d'informations: les Communautés et Régions ne font que livrer de l'information (des listes et éventuellement des mises à jour) sans que ces niveaux de pouvoir doivent exercer une nouvelle compétence (prendre une décision ou exercer un pouvoir d'appréciation). En d'autres termes, c'est la compétence fédérale qui prime ici, à savoir la réalisation d'une liste de lieux stratégiques à protéger dans un objectif de sécurité.

Carte transmise aux opérateurs par le service NTSU pour identifier les zones soumises à une conservation de données à titre préventif

Les lieux ou catégories de lieux visés dans la loi (§ 3 point 1° à 5°) et, le cas échéant, dans l'Arrêté royal sont reportés sur une carte par la NTSU au moins une fois par an. Cette carte, ainsi que, le cas échéant, les délais de conservation spécifique, seront transmis par le service NTSU aux opérateurs pour qu'ils puissent, en pratique, respecter l'obligation de conservation ciblée que la loi leur impose.

verband wordt gelegd tussen de te bewaren gegevens en het nagestreefde doel". Dit is niet het geval in de punten 3 tot en met 5 van artikel 126/1, waar voor elk geval een hoger belang wordt vastgesteld dat de preventieve bewaring van gegevens rechtvaardigt. De wetgever heeft nauwkeurig willen motiveren waarom de verplichting tot gerichte bewaring voor elk van de betrokken zones noodzakelijk en evenredig wordt geacht.

Gelet op het arrest van het Europees Hof van Justitie van 6 oktober 2020, benadrukt de wetgever nogmaals de evenredigheid van het in dit wetsontwerp opgezette systeem voor de gerichte bewaring van verkeers- en locatiegegevens, met het oog op de bestrijding van zware criminaliteit, de vrijwaring van de nationale veiligheid en de voorkoming van ernstige bedreigingen van de openbare veiligheid, op basis van objectieve en niet-discriminerende elementen door middel van een geografisch criterium.

Machtiging aan de Koning

In antwoord op een opmerking in punt 4.2.4. van het advies van de Raad van State, bevestigt de wetgever dat de Koning niet over enige appreciatiemarge beschikt om bijkomende geografische zones vast te stellen. Een bijkomende zone moet absoluut beantwoorden aan een van de criteria van § 3, punten 3° tot en met 5°.

Ten slotte wenst de wetgever, in antwoord op de opmerking van de Raad van State in punt 4.3.1. van het advies, te verduidelijken dat het niet nodig is een samenwerkingsakkoord te sluiten met de Gewesten en/of de Gemeenschappen over de bevoegde autoriteiten die de informatie moeten verstrekken: de Gemeenschappen en de Gewesten verstrekken enkel informatie (lijsten en eventuele actualiseringen) zonder dat deze bevoegdheidsniveaus een nieuwe bevoegdheid moeten uitoefenen (een beslissing nemen of een appreciatiebevoegdheid uitoefenen). Met andere woorden, het is de federale bevoegdheid die hier voorrang heeft, namelijk het opstellen van een lijst van strategische plaatsen die met het oog op de veiligheid moeten worden beschermd.

Kaart die door de NTSU-dienst aan de operatoren wordt toegezonden om de zones aan te duiden waarvoor preventieve gegevensbewaring geldt

De in de wet (§ 3, punten 1° tot 5°) en, desgevallend in het koninklijk besluit, bedoelde plaatsen of categorieën van plaatsen worden minstens eenmaal per jaar door de NTSU in kaart gebracht. Deze kaart en eventuele specifieke bewaartermijnen zullen aan de operatoren worden verzonden, zodat zij in de praktijk de verplichting tot gerichte bewaring kunnen nakomen die de wet hun oplegt.

Tant les lieux précisés dans la loi que ceux indiqués dans l'Arrêté royal doivent être aussi précis que possible, ne laissant à la NTSU aucune marge d'appréciation. De cette manière, la carte sur laquelle ces lieux seront reportés est un simple acte matériel d'exécution, sans contenu juridique propre. Cette carte ne doit donc pas être publiée.

Ceci dit, le fait que les catégories de zones géographiques doivent être déterminées de manière précise et objective, n'implique pas que la loi ou l'Arrêté royal identifie très précisément quels sont les lieux répondant à ces catégories. C'est notamment le cas pour le critère relatif aux statistiques. Cette catégorie est précise et objective, mais il est indispensable de disposer de statistiques, qui ne sont pas publiques, à ce sujet, pour déterminer quelles sont concrètement les zones géographiques visées. La recherche de ces statistiques n'implique toutefois aucun pouvoir d'appréciation. Il s'agit seulement de recueillir et d'appliquer des données pertinentes.

En pratique, ce sera le service NTSU de la police fédérale qui transmettra au moins annuellement la carte aux opérateurs. Ce service est déjà le canal de communication entre les autorités requérantes (autorités judiciaires, services de renseignements, etc.) et les opérateurs qui doivent effectuer les réquisitions.

Concrètement, c'est ce service qui, sur la base des critères fixés par la loi et des lieux qui y sont énumérés, ainsi que ceux éventuellement mentionnés dans l'Arrêté royal, établira la carte des lieux spécifiques dans lesquels s'applique l'obligation de conservation des données par les opérateurs.

Afin que le service NTSU puisse exécuter ses missions, chaque autorité compétente devra transmettre à échéance déterminée par le Roi les données opérationnelles nécessaires pour réaliser la carte. Cependant dès qu'une zone change de finalité (destination), cette autorité a aussi l'obligation de communiquer ce changement sans délai au NTSU.

Afin d'assurer l'homogénéité de la méthode de travail, le service désigné par le Roi peut se faire assister dans la réalisation de sa mission par l'Institut Géographique National. À cette fin, un protocole de collaboration peut être signé entre le service désigné par le Roi et l'Institut Géographique National.

L'Institut Géographique National (IGN) a été créé par la loi du 8 juin 1976. L'article 3*bis* de cette loi, telle que remplacée par la loi du 15 décembre 2011 transposant la directive 2007/2/CE du Parlement européen et du

Zowel de in de wet als de in het koninklijk besluit genoemde plaatsen moeten zo nauwkeurig zijn, dat de NTSU geen beoordelingsmarge heeft. Zo is de kaart waarop deze plaatsen zullen worden ingevuld een louter materiële uitvoeringshandeling, zonder eigen juridische inhoud. De kaart hoeft dus niet te worden gepubliceerd.

Dat de categorieën van geografische gebieden op precieze en objectieve wijze moeten worden vastgesteld, impliceert evenwel niet dat de wet of het koninklijk besluit zeer nauwkeurig vaststelt welke plaatsen onder deze verschillende categorieën vallen. Dit is met name het geval voor het criterium inzake statistieken. Deze categorie is nauwkeurig en objectief, maar het is van essentieel belang over statistieken te beschikken, die niet noodzakelijk openbaar zijn, om te kunnen bepalen welke geografische zones daadwerkelijk onder de regeling vallen. Het zoeken naar dergelijke statistieken impliceert evenwel geen discretionaire bevoegdheid. Het is alleen een kwestie van relevante gegevens te verzamelen en toe te passen.

In de praktijk zal het de dienst NTSU van de federale politie zijn die minstens jaarlijks de kaart aan de operatoren zal overmaken. Deze dienst is reeds het communicatiekanaal tussen de verzoekende autoriteiten (gerechtelijke autoriteiten, inlichtingendiensten, enz.) en de operatoren die de opvorderingen moeten doen.

Concreet is het deze dienst die, op basis van de door de wet vastgestelde criteria en de daarin opgesomde plaatsen, alsmede de plaatsen die eventueel in het Koninklijk Besluit worden vermeld, de kaart zal opstellen van de specifieke plaatsen waar de verplichting tot het bewaren van gegevens door de operatoren geldt.

Opdat de NTSU-dienst zijn taken kan uitvoeren, moet elke bevoegde autoriteit de operationele gegevens die nodig zijn om de kaart op te stellen, vóór een door de Koning vastgestelde datum indienen. Zodra een gebied echter zijn bestemming wijzigt, is deze autoriteit ook verplicht deze wijziging onverwijld aan de NTSU mee te delen.

Teneinde de homogeniteit van de werkwijze te verzekeren, kan de door de Koning aangewezen dienst zich laten bijstaan in zijn opdracht door het Nationaal Geografisch Instituut. Daartoe kan een samenwerkingsprotocol ondertekend worden tussen de door de Koning aangewezen dienst en het Nationaal Geografisch Instituut.

Het Nationaal Geografisch Instituut (NGI) werd opgericht bij wet van 8 juni 1976. Artikel 3*bis* van die wet, zoals vervangen door de wet van 15 december 2011 tot omzetting van de Richtlijn 2007/2/EG van het Europees

Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne, stipule que l'une des missions du IGN est "d'établir et d'exploiter une infrastructure d'information géographique au sein de laquelle des réseaux de compilations identifiables de données géographiques et d'applications informatiques sur ces données géographiques peuvent être rendus opérationnels. L'IGN est largement reconnu comme une source authentique de bases de données topographiques et d'informations géographiques numériques.

Le Conseil d'État a noté au point 7.4. de l'avis qu'il ne peut être exclu qu'une situation se présente dans laquelle, en raison des matières pour lesquelles elles sont compétentes, plusieurs autorités seraient compétentes pour un même type de zone. Le législateur est d'avis que, si tel était le cas, les compétences respectives de ces autorités seraient complémentaires plutôt que de se superposer.

Le Conseil d'État note au paragraphe 4.2.3. que la détermination du périmètre des zones ainsi que leur inscription sur la liste ou leur retrait de celle-ci, conditionnent l'obligation imposée aux opérateurs de conserver les données y afférentes, et que ces décisions doivent être à tout le moins approuvées par une autorité unique, aux fins d'assurer le respect du principe d'égalité. Le Conseil d'État ajoute dans la note de bas de page 27 que, le cas échéant, à condition que la méthode de calcul ait été préalablement fixée par le législateur ou par le Roi, il pourrait être envisagé de charger un ou plusieurs ministres de cette détermination.

Il était déjà prévu que ce soit le Roi qui détermine l'étendue du périmètre pour les zones prévues aux points 3° à 5° du présent paragraphe. Or, le législateur prévoit également dans le projet de loi que les ministres de la Justice, de l'Intérieur et de la Défense doivent donner leur approbation à la liste des zones géographiques soumises à l'obligation de conservation des données et à la durée de cette conservation, annuellement et lors de toute modification de la liste (c'est-à-dire chaque ajout d'une zone à la liste et/ou chaque suppression d'une zone de la liste). Une disposition similaire est déjà prévue dans d'autres lois: voir, par exemple, l'article 44/5 de la loi sur la fonction de police, où c'est le ministre de l'Intérieur qui établit une liste de phénomènes et de groupements sur la base d'une proposition des services opérationnels. Ce faisant, le législateur répond à l'observation du Conseil d'État. Ce n'est qu'après cette approbation que le service désigné par le Roi peut communiquer aux opérateurs la

Parlement en de Raad van 14 maart 2007 tot oprichting van een infrastructuur voor ruimtelijke informatie in de Gemeenschap, voorziet dat één van de opdrachten van het NGI eruit bestaat "een geografische informatie-infrastructuur op te richten en uit te baten waarin netwerken van identificeerbare verzamelingen geografische gegevens en computertoepassingen op deze geografische gegevens operationeel kunnen worden gemaakt". Het NGI is algemeen erkend als authentieke bron voor topografische databanken en digitale geografische informatie.

De Raad van State heeft in punt 7.4. van het advies op dat het niet uit te sluiten valt dat zich een situatie voordoet waarin verschillende overheden op grond van de aangelegenheden waarvoor ze bevoegd zijn, voor eenzelfde soort zone bevoegd zouden zijn. De wetgever is van mening dat, als dit al het geval zou zijn, de respectievelijke bevoegdheden van deze autoriteiten eerder complementair dan overlappend zullen zijn.

De Raad van State merkt in punt 4.2.3. op dat het bepalen van de omvang van de zones, het opnemen van zones op de lijst en het schrappen van zones van de lijst van doorslaggevend belang zijn voor de verplichting die aan de operatoren opgelegd wordt om de daarmee verband houdende gegevens te bewaren, en dat deze beslissingen op zijn minst goedgekeurd moeten worden door één enkele overheid, om ervoor te zorgen dat het gelijkheidsbeginsel in acht genomen wordt. De Raad van State voegt er in voetnoot 27 aan toe dat in voorkomend geval en mits de berekeningsmethode vooraf door de wetgever of door de koning vastgesteld is, één of meer ministers ermee belast kunnen worden die zones vast te stellen.

Eerder werd al voorzien dat het de Koning zal zijn die de omvang van de perimeter zal bepalen, voor de zones bedoeld in de punten 3° tot 5° van deze paragraaf. Nu voorziet de wetgever eveneens in het wetsontwerp dat de ministers van Justitie, Binnenlandse Zaken en Defensie jaarlijks én bij elke wijziging van de lijst (daarmee wordt bedoeld: elke toevoeging van een zone op de lijst en/of elke schrapping van een zone van de lijst) hun goedkeuring moeten geven aan de lijst van geografische zones die onderworpen zijn aan een gegevensbewaringsplicht en de bewaringstermijnen. Een gelijkaardige regeling is al voorzien in andere wetgevingen: zie bijvoorbeeld artikel 44/5 van de wet op het politieambt, waar het de minister van Binnenlandse Zaken is die een lijst van fenomenen en groeperingen aanlegt op basis van een voorstel van operationele diensten. Daarmee komt de wetgever tegemoet aan de opmerking van de Raad van State. Het is pas na deze goedkeuring dat de dienst

liste des zones géographiques soumises à l'obligation de conservation des données.

L'arrêté ministériel précité fixant la liste des zones géographiques et les délais de conservation n'est pas publié in extenso au *Moniteur belge*, mais il est publié par mention, comme prévu par l'article 56, § 1, quatrième alinéa, des lois sur l'emploi des langues en matière administrative, coordonnées le 18 juillet 1966. En effet, l'arrêté ministériel contient des informations sensibles dont on peut déduire quelles sont les zones géographiques soumises à une obligation de conservation, et surtout quelles sont les zones géographiques qui ne le sont pas. Sur cette base, les auteurs potentiels d'infractions pénales pourraient se déplacer vers des zones où il n'y a pas d'obligation de conservation de données. Les opérateurs, qui doivent bien entendu prendre connaissance de la liste des zones géographiques et des périodes de conservation respectives, sont informés par le service désigné par le Roi. Cette approche est d'ailleurs conforme à ce que le Conseil d'État a relevé dans son avis n° 69.160/4 du 6 mai 2021 sur un avant-projet de loi introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G.

La liste des zones géographiques soumises à l'obligation de conservation des données est également transmise à l'Organe de contrôle de l'information policière et au Comité permanent R, chacun pour ce qui concerne ses propres compétences. Toutefois, la liste des bâtiments destinés à des personnes morales dont le potentiel économique et scientifique doit être protégé, comme prévu au § 3, premier alinéa, 4°, b), n'est soumise qu'au Comité permanent R.

Alors que le Comité R est compétent pour contrôler le fonctionnement général des services de renseignement et de sécurité et donc également les listes qu'ils transmettent au service désigné par le Roi, ce n'est pas le cas de l'Organe de contrôle de l'information policière, dont la compétence se limite au contrôle du traitement des données à caractère personnel par les services de police. Chaque organe de contrôle intervient dans le cadre de ses compétences. Ainsi, si l'Organe de contrôle de l'information policière estime qu'il ne se justifie pas qu'une zone géographique soit retenue dans la liste au regard des risques élevés de criminalité grave, cette zone géographique sera néanmoins maintenue si elle se justifie au regard des menaces contre la sécurité nationale. Les deux organismes de contrôle peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner que certaines zones géographiques soient retirées de la liste.

aangewezen door de Koning de lijst van geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, kan meedelen aan de operatoren.

Het hierboven vernoemde ministerieel besluit tot vaststelling van de lijst van geografische zones en van de bewaringstermijnen wordt niet in extenso bekendgemaakt in het *Belgisch Staatsblad*, maar wel via vermelding, zoals voorzien in artikel 56, § 1, vierde lid, van de wetten op het gebruik van de talen in bestuurszaken, gecoördineerd op 18 juli 1966. Het ministerieel besluit bevat immers gevoelige informatie waaruit afgeleid kan worden in welke geografische zones een bewaringsplicht geldt, en vooral in welke geografische zones dat niet het geval is. Op basis daarvan zouden potentiële daders van strafbare feiten kunnen uitwijken naar zones waar geen bewaringsplicht geldt. De operatoren, die uiteraard kennis moeten nemen van de lijst van geografische zones en de respectievelijke bewaartermijnen, worden op de hoogte gebracht door de door de Koning aangewezen dienst. Deze benadering komt overigens overeen met wat de Raad van State ook heeft opgemerkt in advies nr. 69.160/4 van 6 mei 2021 inzake een voorontwerp van wet tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten.

De lijst van de geografische zones die onderworpen zijn aan de gegevensbewaringsplicht wordt ook overgemaakt aan het Controleorgaan op de politionele informatie en aan het Vast Comité I, elk voor wat betreft hun eigen bevoegdheden. Echter, de lijst van gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden, voorzien in § 3, eerste lid, 4°, b), wordt alleen overgemaakt aan het Vast Comité I.

Terwijl het Comité R bevoegd is om de algemene werking van de inlichtingen- en veiligheidsdiensten te controleren en dus ook de lijsten die zij doorgeven aan de door de Koning aangewezen dienst, geldt dit niet voor het Controleorgaan op de politionele informatie, waarvan de bevoegdheid beperkt is tot de controle van de verwerking van persoonsgegevens door de politiediensten. Elk toezichthoudend orgaan treedt op binnen het kader van zijn bevoegdheden. Indien het Controleorgaan op de politionele informatie dus van oordeel is dat een geografische zone vanwege het hoge risico op zware criminaliteit niet op de lijst behoeft te worden geplaatst, zal deze zone niettemin gehandhaafd blijven indien dit gerechtvaardigd is met betrekking tot de bedreigingen van de nationale veiligheid. Beide controle-instanties kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of bevelen dat bepaald geografische zones van de lijst geschrapt worden.

Le Comité R exerce à l'égard de cette liste ses compétences en matière de contrôle de données non personnelles, à savoir un rôle d'avis, incluant la possibilité d'émettre des recommandations. Tant le Comité R que l'Organe de contrôle de l'information policière peuvent procéder à un examen de la qualité des données et du respect de la procédure d'établissement des listes visées au présent paragraphe et notamment la vérification que les zones sont bien reprises de manière stricte et exacte et que certaines zones ne sont pas reprises plusieurs fois.

Il faut aussi noter que selon la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, l'IBPT est chargé du contrôle du respect entre autres de la loi télécom. Cette compétence générale de contrôle n'implique cependant pas que l'IBPT soit amené à contrôler le respect des obligations que l'article 126/1 met à charge des autorités.

Pour répondre à une remarque du Conseil d'État, le projet de loi ne prévoit plus que la loi du 11 avril 1994 relative à la publicité de l'administration ne s'applique pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article.

Par conséquent, l'accès à ces informations et notamment à la liste des zones géographiques se fera conformément à la loi du 11 avril 1994 relative à la publicité de l'administration, en tenant compte notamment de l'article 6, § 1er, de cette loi qui dispose que l'autorité administrative rejette la demande de consultation, d'explication ou de communication sous la forme de copie d'un document administratif si elle a constaté que l'intérêt de la publicité ne l'emporte pas notamment sur la protection de la sécurité de la population ou de l'ordre public, ou encore, de la sûreté ou de la défense nationales.

Le projet de loi prévoit néanmoins une obligation de secret pour toute personne (autorités compétentes, opérateurs, autres) qui, en raison de sa fonction, a connaissance de ces informations ou prête son concours à la mise en œuvre de l'article 126/1, avec référence à la peine prévue à l'article 458 du code pénal.

Paragraphe 4

L'alinéa 1er prévoit que les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone.

Lors de la consultation publique relative à l'avant-projet de loi, certains opérateurs ont indiqué que des directives étaient nécessaires concernant un certain

Met betrekking tot deze lijst oefent het Comité I zijn controlebevoegdheden inzake niet-persoonsgebonden gegevens uit, namelijk een adviserende rol, met inbegrip van de mogelijkheid om aanbevelingen te doen. Zowel het Comité I als het Controleorgaan op de politionele informatie kunnen de kwaliteit van de gegevens en de naleving van de procedure voor het opstellen van de in dit lid bedoelde lijsten onderzoeken, en met name nagaan of de velden strikt en juist zijn ingevuld en of bepaalde velden niet meer dan eens zijn ingevuld.

Er zij tot slot op gewezen dat volgens de wet van 17 januari 2003 betreffende het statuut van de regulator van de Belgische post- en telecommunicatiesector, het BIPT belast is met het toezicht op de naleving van onder meer de telecomwet. Deze algemene controlebevoegdheid houdt evenwel niet in dat het BIPT moet controleren of de verplichtingen die artikel 126/1 aan de autoriteiten oplegt, worden nageleefd.

Om te beantwoorden aan een opmerking van de Raad van State schrijft het wetsontwerp niet langer voor dat de wet van 11 april 1994 betreffende de openbaarheid van bestuur niet van toepassing is op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel.

Bijgevolg zal de toegang tot deze informatie en dus tot de lijst van geografische zones geschieden overeenkomstig de wet van 11 april 1994 betreffende de openbaarheid van bestuur, met name rekening houdende met artikel 6, § 1, van deze wet, dat bepaalt dat de administratieve overheid de vraag om inzage, uitleg of mededeling in afschrift van een bestuursdocument afwijst wanneer zij heeft vastgesteld dat het belang van de openbaarheid niet opweegt tegen de bescherming van de veiligheid van de bevolking of van de openbare orde, de veiligheid of de verdediging van het land.

Niettemin wordt in het wetsontwerp een geheimhoudingsplicht ingeschreven voor eenieder (bevoegde autoriteiten, operatoren, anderen) die uit hoofde van hun functie kennis heeft van deze informatie of meewerkt aan de uitvoering van artikel 126/1, met verwijzing naar de bestraffing voorzien in artikel 458 van het Strafwetboek.

Paragraaf 4

In het eerste lid is bepaald dat de operatoren de verkeersgegevens moeten bewaren van alle oproepingen of communicaties zonder resultaat vanuit of naar een geografisch gebied als bedoeld in lid 3.

Tijdens de openbare raadpleging over het voorontwerp van wet hebben sommige operatoren aangegeven dat er richtlijnen nodig waren in verband met een aantal

nombre de cas pratiques d'application de l'article 126/1. Afin de donner suite à cette demande, ainsi qu'à la préoccupation de l'Autorité de protection des données concernant le respect du principe de minimisation des données (consid. 129), il a été apporté plusieurs précisions à l'article 126/1, § 4.

L'exemple suivant permet d'illustrer l'alinéa 1er du paragraphe 4. Une personne qui se trouve dans une zone soumise à une conservation de données en vertu de l'article 126/1 appelle une personne qui se trouve dans une zone qui n'est pas soumise à une telle conservation en vertu du même article. Dans ce cas, les données de communication ou de l'appel infructueux doivent être conservées, telles que le numéro de l'appelant et de l'appelé et la durée de la communication (en cas de communication). En pratique, les données de trafic de l'appel sortant de la zone soumise à conservation de données seront conservées, mais pas les données de trafic de l'appel entrant dans la zone qui n'est pas soumise à une telle conservation.

Par contre, les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement ne doivent être conservées que pour l'appelant (pas pour l'appelé, étant donné que ce dernier se trouve dans une zone qui n'est pas soumise à une conservation de données).

Par ailleurs, il a précisé à l'alinéa 2 que lorsque l'opérateur n'est pas en mesure de localiser l'équipement terminal concerné de façon plus précise que sa localisation sur le territoire national, l'opérateur doit procéder à la conservation des données lorsque l'ensemble du territoire national est soumis à une obligation. En effet, dans cette hypothèse, il peut être déduit avec certitude que les données doivent être conservées, indépendamment de la zone géographique précise. En revanche, en l'absence de cette information, la durée de conservation applicable ne peut être déduite, de sorte que la durée la plus courte doit être retenue conformément au principe de minimisation des données. *A contrario*, lorsque l'ensemble du territoire national n'est pas soumis à une obligation de conservation, il ne peut être déduit avec certitude que les données doivent être conservées. En conséquence, dans cette dernière hypothèse, l'opérateur ne doit pas conserver ces données.

L'exemple suivant permet d'illustrer l'alinéa 3 du paragraphe 4. Une personne commence une communication électronique dans une zone qui n'est pas soumise à une conservation de données en vertu de l'article 126/1,

praktische gevallen van de toepassing van artikel 126/1. Om aan dit verzoek tegemoet te komen, alsmede aan de bezorgdheid van de gegevensbeschermingsautoriteit met betrekking tot de naleving van het beginsel van minimalisering van de gegevensverwerking (overweging 129), zijn in artikel 126/1, § 4, verscheidene verduidelijkingen aangebracht.

Aan de hand van het volgende voorbeeld kan het eerste lid van paragraaf 4 geïllustreerd worden. Een persoon die zich in een gebied bevindt dat onderworpen is aan een gegevensbewaring krachtens artikel 126/1, belt naar een persoon die zich in een gebied bevindt dat niet onderworpen is aan zo'n bewaring krachtens hetzelfde artikel. In dat geval moeten de communicatiegegevens of de gegevens van de oproep zonder resultaat worden bewaard, zoals het nummer van de beller en van de opgebelde persoon en de duur van de communicatie (als er communicatie is geweest). In de praktijk zullen de verkeersgegevens van de oproep die uitgaat van het gebied dat onderworpen is aan gegevensbewaring bewaard worden, maar niet de verkeersgegevens van de oproep naar de zone die niet aan een dergelijke bewaring is onderworpen.

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst, alsook met betrekking tot de locatie van die apparatuur moeten daarentegen enkel worden bewaard voor de beller (niet voor de opgebelde persoon, aangezien die laatste zich bevindt in een gebied dat niet onderworpen is aan een gegevensbewaring).

Voorts wordt in lid 2 verduidelijkt dat wanneer de operator de betrokken eindapparatuur niet preciezer kan lokaliseren dan de lokalisatie ervan op het nationale grondgebied, de operator de gegevens moet bewaren wanneer voor het gehele nationale grondgebied een bewaarplicht geldt. In dit geval kan immers met zekerheid worden geconcludeerd dat de gegevens moeten worden bewaard, ongeacht het precieze geografische gebied. Bij gebreke van deze informatie kan de toepasselijke bewaringstermijn echter niet worden afgeleid, zodat overeenkomstig het beginsel van minimalisering van de gegevens de kortste termijn moet worden gehanteerd. Anderzijds kan uit het feit dat niet voor het gehele nationale grondgebied een bewaarplicht geldt, niet met zekerheid worden afgeleid dat de gegevens moeten worden bewaard. In het laatste geval behoeft de operator de gegevens dus niet te bewaren.

Aan de hand van het volgende voorbeeld kan het derde lid van paragraaf 4 geïllustreerd worden. Een persoon start een elektronische communicatie in een gebied dat niet onderworpen is aan gegevensbewaring

se déplace dans une zone qui est soumise à une telle conservation et y continue la communication et finalement se rend dans une zone qui n'est pas soumise à une telle conservation de données et y termine la communication. Dans ce cas, les données de trafic doivent être conservées par les opérateurs étant donné que l'utilisateur final s'est trouvé à un moment donné de la communication dans une zone soumise à une conservation de données. La solution contraire permettrait à des personnes mal intentionnées de contourner la législation (en commençant une communication dans une zone qui n'est pas soumise à une conservation de données).

Par contre, dans le même exemple, les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement ne doivent être conservées que pour ce qui concerne le passage de l'utilisateur final dans une zone soumise à une conservation de données.

Pour les fournisseurs de services de communication fournis via Internet, l'alinéa 5 prévoit qu'ils peuvent utiliser les données de localisation de leurs utilisateurs finaux dont ils disposent pour déterminer s'ils doivent conserver les métadonnées sur ces utilisateurs. Les données de localisation dont disposent ces fournisseurs sont diverses, mais il s'agit souvent de données de localisation très précises, allant jusqu'à la précision des systèmes de positionnement par satellite.

Au point 129 de l'avis de l'APD, on peut lire ce qui suit:

"129. Le nouvel article 126/1 § 4, dernier alinéa prévoit que "Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques". Cette disposition est problématique au regard du principe de minimisation des données et, plus fondamentalement, du principe de la proportionnalité qui doit régir toute mesure de conservation des données. Elle risque, en effet, d'aboutir à une conservation des données qui aille au-delà de ce qui est nécessaire et proportionné au regard des objectifs poursuivis par cette conservation. Le principe de proportionnalité, tel qu'il est interprété par la CJUE, s'oppose à ce que les opérateurs puissent conserver, en exécution de l'article 126/1 de la loi télécom, les données de trafic relatives à des communications qui

krachtens artikel 126/1, verplaatst zich naar een gebied dat wel aan zo'n bewaring onderworpen is en zet daar de communicatie voort en begeeft zich uiteindelijk naar een gebied dat niet onderworpen is aan een dergelijke gegevensbewaring en beëindigt daar de communicatie. In dat geval moeten de communicatiegegevens en de gegevens van de oproepen zonder resultaat door de operatoren worden bewaard aangezien de eindgebruiker zich op een bepaald moment van de communicatie in een gebied bevond dat onderworpen is aan een gegevensbewaring. De tegenovergestelde oplossing zou personen met slechte bedoelingen de mogelijkheid bieden om de wetgeving te omzeilen (door een communicatie te beginnen in een gebied dat niet aan een gegevensbewaring onderworpen is).

In datzelfde voorbeeld moeten de gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst, alsook met betrekking tot de locatie van die apparatuur daarentegen enkel worden bewaard wat betreft de doortocht van de eindgebruiker door een gebied dat onderworpen is aan een gegevensbewaring.

Voor de aanbieders van communicatiediensten die via internet worden geleverd voorziet deze bepaling dat zij gebruik kunnen maken van de lokalisatiegegevens die ze van hun eindgebruikers hebben om te bepalen of ze metadata over deze gebruikers moeten bijhouden. De lokalisatiegegevens die deze aanbieders hebben is divers, maar vaak gaat het om zeer precieze lokalisatiegegevens, tot de precisie van satellietplaatsbepalingssystemen toe.

In punt 129 van het advies van de GBA kunnen we het volgende lezen:

"129. Het nieuwe artikel 126/1 § 4, laatste lid bepaalt als volgt: "Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden." Deze bepaling is problematisch gezien het beginsel van minimale gegevensverwerking en, maar fundamenteel, het evenredigheidsbeginsel waaraan elke maatregel tot bewaring van de gegevens moet voldoen. Ze dreigt immers te leiden tot een bewaring van de gegevens die verder gaat dan wat strikt noodzakelijk en evenredig is voor de beoogde doelen. Het feit dat de operatoren, in uitvoering van artikel 126/1 van de telecomwet, de verkeersgegevens mogen bewaren die betrekking hebben op communicaties die buiten de door de bepaling afgebakende geografische zones worden gevoerd, is in

sont effectuées en dehors des zones géographiques délimités par ladite disposition. Il en est d'autant plus ainsi que ces zones géographiques sont déjà déterminées de manière très large dans l'avant-projet de loi et que l'obligation de conservation des données s'impose, non seulement, aux communications "originaires" de ces zones, mais également aux communications vers ces zones. L'avant-projet de loi sera revu afin supprimer la possibilité offerte aux opérateurs de pouvoir conserver des données au-delà des zones géographiques dans lesquelles l'avant-projet de loi impose une obligation de conservation s'ils ne leur pas techniquement pas possible de circonscrire la conservation des données à ces zones."

Ce point de l'avis n'a pas été suivi pour les raisons suivantes:

Premièrement, il n'est techniquement pas possible pour un opérateur de circonscrire parfaitement la conservation de données de trafic à une zone géographique déterminée dans la loi. Pour prendre un exemple pratique, la portée d'une antenne qui couvre la zone géographique ne va pas s'arrêter exactement à la limite de la zone. Si l'avis de l'APD était suivi, cela signifierait qu'une conservation ciblée sur base géographique ne serait pas possible, alors que la Cour de Justice européenne admet ce type de conservation.

Deuxièmement, il n'est pas proportionné d'exiger des opérateurs de déplacer tout leur matériel (par exemple une antenne pour un opérateur mobile) pour qu'ils ne couvrent très précisément que les zones géographiques identifiées dans le présent projet. Une telle obligation de résultat serait disproportionnée en ce qu'elle ne permettrait pas aux opérateurs, tel que mentionné dans le RGPD, e.a. aux articles 25 et 32, de prendre en considération, dans le cadre de la mise en place de mesures techniques et organisationnelles afin de garantir un niveau de protection des données adéquat de "l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement" que "les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques".

Pour ce qui concerne les services de téléphonie mobile classique (non voice-over-IP), les opérateurs peuvent déterminer la position géographique approximative en fonction de l'antenne, car celle-ci est un élément nécessaire dans un réseau mobile. Chaque utilisateur final doit être localisé afin d'établir une connexion et de permettre la communication. Il n'est cependant pas possible, sur la base de ces seules données, d'établir la position géographique de façon plus précise que le périmètre couvert par l'antenne concernée.

strijd met het evenredigheidsbeginsel. Bovendien zijn die geografische zones in het voorontwerp van wet zeer ruim bepaald en geldt de verplichting tot bewaring van de gegevens niet alleen voor de communicaties "afkomstig" van deze zones, maar ook voor de communicaties naar deze zones. Het voorontwerp van wet moet worden herzien om de mogelijkheid te schrappen die de operatoren wordt geboden om gegevens te bewaren van buiten de geografische zones waarbinnen het voorontwerp van wet voorziet in een bewaarplicht wanneer het voor hen technisch niet mogelijk is om de gegevensbewaring te beperken tot die zones."

Dit punt van het advies werd niet gevolgd, om de volgende redenen:

Ten eerste is het voor een operator technisch niet mogelijk om de bewaring van verkeersgegevens perfect te beperken tot een bij wet vastgesteld geografisch gebied. Om een praktisch voorbeeld te nemen: het bereik van een antenne die het geografisch gebied bestrijkt, zal niet precies stoppen bij de grens van het gebied. Indien het advies van de GBA gevolgd zou worden, zou dit betekenen dat geografisch gerichte bewaring niet mogelijk is, terwijl het Europese Hof van Justitie dergelijke bewaring toestaat.

Ten tweede is het niet evenredig om van operatoren te verlangen dat zij al hun apparatuur (b.v. een antenne voor een mobiele operator) verplaatsen om zeer precies alleen de geografische zones te bestrijken die in het huidige ontwerp worden genoemd. Een dergelijke resultaatsverplichting zou onevenredig zijn omdat zij de operatoren, zoals vermeld in de artikelen 25 en 32 van de AVG, niet de mogelijkheid zou bieden om bij de invoering van technische en organisatorische maatregelen om een passend niveau van gegevensbescherming te waarborgen, rekening te houden met "de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking", alsook met "met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen".

Voor wat betreft de klassieke (niet-voice-over-IP) mobiele telefoondiensten kunnen de operatoren de geografische positie bij benadering bepalen op basis van de antenne, omdat dit een noodzakelijk gegeven is in een mobiel netwerk. Elke eindgebruiker moet namelijk kunnen worden gelokaliseerd om een verbinding op te stellen en communicatie mogelijk te maken. Op basis van deze gegevens alleen is het echter niet mogelijk de geografische positie nauwkeuriger vast te stellen dan de omtrek die door de betrokken antenne wordt bestreken.

En outre, les opérateurs ne peuvent pas utiliser une période de conservation différente pour les données qu'ils collectent par antenne. Il en va de même pour les services vocaux fixes: dans le cadre de l'agrégation choisie, ils ne peuvent plus faire de distinction entre les données des clients qui leur sont associés. Toutes les données sont conservées pendant la même période, indépendamment du client. Conformément au principe de minimisation des données, la durée retenue doit donc être la plus courte.

Enfin, le dernier alinéa du paragraphe 4 précise encore que lorsqu'en application du présent article, différentes durées de conservation sont applicables à des mêmes données, les opérateurs conservent les données pendant la durée la plus courte.

Paragraphe 5

Le paragraphe 5 de l'article 126/1 contient un certain nombre de délégations au Roi. Ces délégations sont facultatives. En d'autres termes, les arrêtés d'exécution énumérés ici ne sont pas obligatoires et ne sont donc pas nécessaires à l'entrée en vigueur de la loi. Ces délégations concernent les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées au paragraphe 3, la liste des différentes autorités compétentes pour les matières visées au paragraphe 3, premier alinéa, points 2° à 5°, et les modalités de communication des informations par les autorités compétentes vers le service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er.

Comme expliqué plus haut, la loi prévoit également que le Roi peut déterminer des zones géographiques supplémentaires qui ne sont pas encore couvertes par les points du § 3, 3° à 5° de l'article 126/1, pour autant qu'elles répondent aux critères légaux. La conservation des données peut alors également être prévue dans ces zones géographiques supplémentaires. En réponse au point 125 de l'avis de l'Autorité de protection des données, le législateur rappelle que le Roi ne dispose d'aucune marge d'appréciation: il ne peut ajouter des zones géographiques que dans la mesure où elles répondent aux critères de la loi. Le dernier alinéa du paragraphe 5 stipule, en ce qui concerne cet arrêté royal, qu'il doit être renouvelé tous les trois ans, et qu'en l'absence de renouvellement, l'obligation de conservation en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal. Cela met un frein

Operatoren kunnen bovendien voor de gegevens die ze per antenne verzamelen geen verschillende bewaartermijn hanteren. Hetzelfde geldt voor vaste spraakdiensten: binnen de gekozen aggregatie kunnen ze geen verder verschil maken tussen de gegevens van klanten die daarmee geassocieerd worden. Alle gegevens worden bewaard voor dezelfde periode onafhankelijk van de klant. In overeenstemming met het beginsel van minimalisering van de gegevens moet de gekozen duur derhalve zo kort mogelijk zijn.

Tot slot wordt in het laatste lid van paragraaf 4 gespecificeerd dat wanneer op grond van dit artikel verschillende bewaringstermijnen van toepassing zijn op dezelfde gegevens, de operatoren de gegevens gedurende de kortste termijn moeten bewaren.

Paragraaf 5

Paragraaf 5 van artikel 126/1 bevat een aantal delegaties aan de Koning. Het gaat hier om optionele delegaties. Dat wil zeggen dat de hier opgesomde uitvoeringsbesluiten niet verplicht zijn en dus ook niet noodzakelijk zijn voor een inwerkingtreding van de wet. Het gaat om de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones, de lijst van de verschillende autoriteiten die bevoegd zijn voor de in paragraaf 3, eerste lid, punten 2° tot en met 5° bedoelde aangelegenheden, en de procedures voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de procedures voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen.

Zoals hoger uitgelegd voorziet de wet ook dat de Koning bijkomende geografische zones kan bepalen die nog niet onder de punten in § 3, 3° tot 5° van artikel 126/1 staan, voor zover deze beantwoorden aan de wettelijke criteria. In deze bijkomende geografische zones kan dan ook een gegevensbewaring voorzien worden. Als antwoord op punt 125 van het advies van de Gegevensbeschermingsautoriteit wijzen de stellers van het ontwerp op het feit dat de Koning geen enkele appreciatiebevoegdheid heeft: hij kan slechts geografische zones toevoegen voor zover zij voldoen aan de wettelijke criteria. Het laatste lid van paragraaf 5 bepaalt m.b.t. tot dit Koninklijk besluit dat het elke drie jaar hernieuwd moet worden, en dat bij ontstentenis van een hernieuwing de verplichting tot bewaring voor wat deze bijkomende geografische zones betreft vervalt, en dit tot een nieuw koninklijk besluit van kracht wordt. Hiermee wordt een rem gezet op de mogelijke uitbreiding van de

à l'éventuelle extension des zones géographiques par arrêté royal et à la continuation de la conservation des données dans ces zones.

Paragraphe 6

Évaluation de la loi et de l'arrêté royal

Après l'avis du Comité de coordination du Renseignement et de la Sécurité (CCRS) et des autorités de protection des données compétentes, les ministres compétents établiront un rapport qui sera soumis à la Chambre des représentants. L'objet de ce rapport est de vérifier s'il est nécessaire d'adapter les dispositions de la loi ou de l'arrêté royal. Dans le cadre de ce rapportage annuel, il appartient aux ministres compétents de décider de le faire ou non. Une attention particulière sera portée au caractère objectif et non discriminatoire des zones géographiques. Le point 126 de l'avis de l'Autorité de protection des données indique que le rapport d'évaluation devrait contenir quelques éléments d'information supplémentaires. En réponse à ce commentaire, il a été ajouté que le pourcentage du territoire national couvert par la conservation des données devrait également être inclus dans le rapport. Cependant, il n'est pas possible d'inclure le pourcentage de la population dans le rapport: cela n'est pas possible pour la conservation de données basée sur un critère géographique. S'il est possible de déterminer le nombre de personnes vivant dans une zone géographique donnée, il n'est pas possible de suivre le nombre de personnes entrant temporairement dans ces zones.

Le Comité de coordination est choisi comme organe d'avis car il représente les besoins des services opérationnels en matière d'utilisation des métadonnées de téléphonie.

Composition de ce Comité

Le Comité de coordination pour le renseignement et la sécurité visé par l'arrêté royal du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du Renseignement et de la Sécurité et du Comité de coordination du Renseignement et de la Sécurité compte les membres permanents suivants: l'administrateur général de la sûreté de l'État, le chef du service général de renseignement et de sécurité des forces armées, le directeur de l'organe de coordination de l'évaluation des menaces, le commissaire général de la police fédérale, le directeur général du centre national de crise du service public fédéral de l'intérieur, le président du comité exécutif du service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement, un membre du collège

geografische zones bij Koninklijk besluit en op het voortbestaan van de gegevensbewaring binnen deze zones.

Paragraaf 6

Evaluatie van de wet en van het koninklijk besluit

Na het advies van het Coördinatiecomité Inlichtingen en Veiligheid en de bevoegde gegevensbeschermingsautoriteiten, zullen de bevoegde ministers een verslag opmaken dat aan de Kamer van volksvertegenwoordigers wordt voorgelegd. Het doel van het verslag is na te gaan of het nodig is de bepalingen in de wet of het koninklijk Besluit aan te passen. In het kader van deze jaarlijkse verslaggeving is het aan de bevoegde ministers om daartoe al dan niet over te gaan. Bijzondere aandacht zal worden besteed aan het objectieve en niet-discriminerende karakter van de geografische gebieden. In punt 126 van het advies van de Gegevensbeschermingsautoriteit wordt gesteld dat het evaluatieverslag een aantal extra informatie-elementen moet bevatten. In antwoord op deze opmerking werd aan het artikel toegevoegd dat het percentage van het nationale grondgebied waarop de gegevensbewaring van toepassing is ook opgenomen moet worden in het verslag. Daarentegen is het niet mogelijk om ook het percentage van de bevolking op te nemen in het verslag: dit is immers niet mogelijk voor de bewaring op grond van een geografisch criterium. Waar het eventueel wel mogelijk zou zijn om na te gaan hoeveel personen er binnen een bepaalde geografische zones gevestigd zijn, is het echter niet mogelijk om bij te houden hoeveel personen tijdelijk deze zones betreden.

Het coördinatiecomité is gekozen als adviesorgaan omdat het de behoeften van de operationele diensten bij het gebruik van telefoniemetagegevens vertegenwoordigt.

Samenstelling van dit comité

Het Coördinatiecomité Inlichtingen en de Veiligheid, zoals bedoeld in het Koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid heeft de volgende permanente leden: de administrateur-generaal van de Veiligheid van de Staat, de chef van de Algemene Dienst inlichting en veiligheid van de Krijgsmacht, de directeur van het Coördinatieorgaan voor de dreigingsanalyse, de commissaris-generaal van de Federale Politie, de directeur-generaal van het Nationaal Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, de voorzitter van het directiecomité van de Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking,

des procureurs généraux désigné par le collège, le procureur fédéral et le chef de la défense.

Comme déjà expliqué ci-dessus, le dernier alinéa du paragraphe 5 de cet article prévoit que l'arrêté royal qui y est prévu doit être renouvelé tous les trois ans. La période de trois ans semble raisonnable: d'ici là, trois rapportages annuels auront en principe été réalisés, permettant une vision claire des avantages et inconvénients de l'arrêté royal qui aurait été adopté.

Le délai de trois ans n'empêche évidemment pas que l'arrêté royal puisse être révisé plus tôt. En même temps, un renouvellement triennal ne signifie pas nécessairement que le contenu de l'arrêté royal va changer de manière substantielle. Il convient également de rappeler que toute modification de l'arrêté royal doit être soumise à l'Autorité de protection des données pour avis.

Selon le législateur, le rapportage annuel avec possibilité de renouvellement de l'arrêté royal, est conforme aux conditions imposées par la Cour de justice.

Art. 10 (modification à l'article 127)

Le paragraphe 2 de l'article 127 est modifié, dès lors que les règles en matière de système de cryptographie sont dorénavant reprises à l'article 107/5.

Art. 11 (insertion de l'article 127/1)

Introduction pour les paragraphes 1 à 4 et 6

Objet des paragraphes 1 à 5

L'article 127/1 est une disposition commune aux articles 122, 123, 126, 126/1 et 127. Les paragraphes 1 à 4 de l'article 127/1 indiquent les finalités de conservation des données conservées en vertu des articles 126, 126/1 et 127, à savoir les données d'identification et les métadonnées conservées par les opérateurs pour les autorités sur la base de la loi télécom. Ces paragraphes n'indiquent pas les finalités de conservation pour les données conservées sur la base des articles 122 et 123 (les données de trafic et de localisation conservées par les opérateurs pour leurs propres besoins et dans l'intérêt de leurs abonnés), dès lors que ces finalités sont déjà prévues dans ces articles (facturation, marketing, lutte contre la fraude, etc.). Les paragraphes 1 à 4 de l'article 127/1 fixent aussi les finalités pour la fourniture aux autorités de données

een lid van het College van procureurs-generaal dat door het College wordt aangewezen, de federaal procureur en de Chef Defensie.

Zoals hiervoor al uitgelegd, voorziet het laatste lid van paragraaf 5 van dit artikel dat het daar voorziene koninklijk besluit om de drie jaar hernieuwd moet worden. De termijn van drie jaar lijkt redelijk: op dat moment zijn er in principe al drie jaarlijkse evaluaties gedaan, waardoor er een duidelijke visie kan zijn op de verdiensten en de gebreken van het koninklijk besluit dat zou zijn aangenomen. eventuele wijzigingen te implementeren.

De termijn van drie jaar verhindert uiteraard niet dat er vroeger kan herzien worden. Tegelijk betekent een driejaarlijkse hernieuwing niet noodzakelijk dat de inhoud van het koninklijk besluit grondig zal veranderen. Er moet ook rekening gehouden worden met het feit dat elke wijziging van het koninklijk besluit voor advies voorgelegd moet worden aan de Gegevensbeschermingsautoriteit.

De jaarlijkse verslaggeving met mogelijkheid tot hernieuwing van het koninklijk besluit, is volgens de wetgever in lijn met wat het Hof van Justitie als voorwaarden oplegt.

Art. 10 (wijziging aan artikel 127)

Paragraaf 2 van artikel 127 wordt gewijzigd, aangezien de regels inzake versleutelingssysteem voortaan opgenomen zijn in artikel 107/5.

Art. 11 (invoeging van artikel 127/1)

Inleiding voor de paragrafen 1 tot 4 en 6

Voorwerp van de paragrafen 1 tot 5

Artikel 127/1 is een bepaling die gemeenschappelijk is aan de artikelen 122, 123, 126, 126/1 en 127. De paragrafen 1 tot 4 van artikel 127/1 vermelden de doeleinden van bewaring van de gegevens die worden bewaard krachtens de artikelen 126, 126/1 en 127, met name de identificatiegegevens en de metagegevens bewaard door de operatoren voor de autoriteiten op basis van de telecomwet. Deze paragrafen vermelden niet de doeleinden van bewaring voor de gegevens die worden bewaard krachtens de artikelen 122 en 123 (de verkeers- en locatiegegevens bewaard door de operatoren voor hun eigen behoeften en in het belang van hun abonnees), aangezien deze doeleinden reeds zijn gedefinieerd in die artikelen (facturering, marketing, bestrijding van fraude, enz.). De paragrafen 1 tot 4 van artikel 127/1 bepalen ook de doeleinden voor de verstrekking aan de autoriteiten

conservées par les opérateurs en vertu des articles 122, 123, 126, 126/1 et 127.

L'article 127/1 régit uniquement les demandes adressées par les autorités aux opérateurs pour obtenir des données. Il ne s'applique pas aux situations dans lesquelles les données sont transmises à une autorité par l'une des parties à la communication ou demandées par une autorité à l'une des parties. Entre notamment dans cette dernière hypothèse, la situation où une partie transmet à une autorité ses métadonnées à des fins de plainte, de règlement d'un litige ou d'une instruction d'office.

L'article 127/1 ne s'applique pas non plus lorsqu'un opérateur transmet des données anonymes à un tiers. Les données doivent être rendues anonymes conformément aux exigences du RGPD et doivent être rendues anonymes par rapport aux personnes physiques et morales auxquelles ces données se rapportent (et pas uniquement par rapport aux personnes physiques comme c'est le cas dans le RGPD). En effet, la directive "vie privée et communications électroniques" (directive 2002/58) protège la confidentialité des données liées tant aux personnes morales qu'aux personnes physiques.

Relation avec les législations sectorielles/ organiques

Pour qu'une autorité puisse valablement obtenir des données d'identification ou des métadonnées de l'opérateur, il est nécessaire qu'elle réponde aux deux conditions cumulatives suivantes: respecter l'article 127/1, §§ 2 à 4 et une norme législative formelle doit lui donner le pouvoir d'obtenir ces données de l'opérateur. Cette norme législative formelle sera en pratique la législation organique de l'autorité qui demande les données ou une législation sectorielle et doit avoir au moins le niveau d'une loi: loi fédérale, décret, ordonnance, règlement européen, etc. Lorsqu'une des deux conditions n'est pas remplie, la fourniture des données ne sera pas autorisée. La fourniture des données ne pourra être mise en œuvre que conformément aux finalités de fourniture des données reprises dans l'article 127/1, §§ 2 à 4 et aux conditions reprises dans la loi organique/sectorielle de l'autorité qui demande à obtenir les données.

Par conséquent, et pour répondre à une crainte exprimée lors de la consultation publique sur l'avant-projet de loi, il n'est pas correct de considérer que tout agent d'une autorité (par exemple un policier/une policière) qui entre dans l'une des catégories de l'article 127/1, §§ 2 à 4, peut demander des données aux opérateurs.

van gegevens bewaard door de operatoren krachtens de artikelen 122, 123, 126, 126/1 en 127.

Artikel 127/1 regelt enkel de verzoeken die de autoriteiten richten aan de operatoren om gegevens te verkrijgen. Het is niet van toepassing op de situaties waarin de gegevens worden verzonden naar een autoriteit door een van de bij de communicatie betrokken partijen of worden gevraagd door een autoriteit aan een van deze partijen. Tot deze laatste hypothese behoort met name de situatie waarin een partij haar metagegevens doorstuurt naar een autoriteit met het oog op een klacht, een geschillenbeslechting of een ambtshalve onderzoek.

Artikel 127/1 is evenmin van toepassing wanneer een operator anonieme gegevens verzendt naar een derde. De gegevens moeten anoniem gemaakt worden overeenkomstig de eisen van de AVG en moeten anoniem gemaakt worden ten aanzien van natuurlijke personen en rechtspersonen op wie deze gegevens betrekking hebben (en niet alleen ten aanzien van de natuurlijke personen zoals het geval is in de AVG). De richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58) beschermt immers de vertrouwelijkheid van de gegevens die verband houden met zowel rechtspersonen als natuurlijke personen.

Betrekking met de sectorale/organieke wetgevingen

Opdat een autoriteit op geldige wijze identificatiegegevens of metagegevens kan krijgen van de operator, is het nodig dat ze beantwoordt aan de volgende twee cumulatieve voorwaarden: eerbiediging van artikel 127/1, §§ 2 tot 4, en een formele wetgevende norm moet haar machtigen om deze gegevens te krijgen van de operator. Deze formele wettelijke norm zal in de praktijk de organieke wetgeving zijn van de autoriteit die de gegevens vraagt of een sectorale wetgeving en moet minstens het niveau van een wet hebben: federale wet, decreet, ordonnantie, Europese Verordening, enz. Wanneer een van de twee voorwaarden niet is vervuld, zal de verstrekking van de gegevens niet worden toegestaan. De verstrekking van de gegevens zal enkel ten uitvoer kunnen worden gebracht in overeenstemming met de doeleinden van gegevensverstrekking vermeld in artikel 127/1, §§ 2 tot 4 en volgens de voorwaarden opgenomen in de organieke/sectorale wet van de autoriteit die vraagt om de gegevens te verkrijgen.

Bijgevolg en om te antwoorden op een vrees die geuit is tijdens de openbare raadpleging over het voorontwerp van wet, is het niet correct om ervan uit te gaan dat elke ambtenaar van een autoriteit (bijvoorbeeld een politieagent(e)) die onder een van de categorieën van artikel 127/1, §§ 2 tot 4, valt, aan de operatoren gegevens

Seules les personnes autorisées par la législation organique ou sectorielle concernée pourront valablement effectuer cette démarche (à titre d'exemple, selon les circonstances, le procureur du Roi ou le juge d'instruction, conformément au Code d'instruction criminelle).

Il est à noter qu'il suffit que les lois organiques ou sectorielles définissant les conditions dans lesquelles les autorités compétentes peuvent demander à un opérateur des données conservées sur la base des articles 122, 123, 126, 126/1 et 127 ne fassent référence qu'au type de données (données d'identité, données de trafic, données de localisation) qui peuvent être demandées par l'autorité, indépendamment de la base juridique qui permet la conservation des données et de la base de données dans laquelle les données sont conservées.

Lien avec l'article 127/3

Comme prévu à l'article 127/3, les autorités doivent adresser leur demande de données de communications électroniques à la Cellule de coordination de l'opérateur. Cela n'empêche évidemment pas que la réponse de cette cellule soit envoyée de manière automatisée (sans intervention humaine).

Objectifs suivis lors de la rédaction de l'article 127/1, §§ 1 à 4 et 6

Un premier objectif de l'article 127/1 est de mettre en œuvre la jurisprudence de la CJUE. Dans son arrêt La Quadrature du Net du 6/10/2020 (C-511/18, 512/18 et 520/18), la CJUE a indiqué ce qui suit: "166 […] l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visé

mag vragen. Enkel de personen die gemachtigd zijn door de organieke of sectorale wetgeving in kwestie zullen die stap op geldige wijze mogen zetten (bijvoorbeeld, afhankelijk van de omstandigheden, de procureur des Konings of de onderzoeksrechter, overeenkomstig het Wetboek van Strafvordering).

Het weze hierbij opgemerkt dat het voldoende is dat de organieke of sectorale wetten waarin de voorwaarden worden bepaald waaronder de betreffende autoriteit aan een operator kan vragen om gegevens te verkrijgen die worden bewaard op basis van de artikelen 122, 123, 126, 126/1 en 127, enkel verwijzen naar het type data (identiteitsgegevens, verkeersgegevens, locatiegegevens) dat door de autoriteit kan worden opgevraagd, ongeacht de rechtsgrond op basis waarvan de gegevens worden opgeslagen en ongeacht de databank waarin de gegevens worden opgeslagen.

Link met artikel 127/3

Zoals bepaald in artikel 127/3 moeten de autoriteiten hun verzoek om elektronische-communicatiegegevens richten aan de Coördinatiecel van de operator. Dat neemt natuurlijk niet weg dat het antwoord van die cel geautomatiseerd wordt verstuurd (zonder menselijke tussenkomst).

Nagestreefde doelstellingen bij het opstellen van artikel 127/1, §§ 1 tot 4 en 6

Een eerste doelstelling van artikel 127/1 bestaat erin de rechtspraak van het HvJ-EU ten uitvoer te brengen. In zijn arrest-*La Quadrature du Net* van 6/10/2020 (C-511/18, 512/18 en 520/18) heeft het HvJ-EU het volgende aangegeven: "166 […] de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van Richtlijn 2002/58 vastgestelde maatregel, [kan] in beginsel enkel […] worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen

au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale."

Le principe repris dans ce passage de l'arrêt (l'accès d'une autorité à des données conservées par un opérateur pour les autorités ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation lui a été imposée) ne vaut que pour les données conservées par les opérateurs pour les autorités (les articles 126, 126/1 et 127 sont des mesures prises au titre de l'article 15, paragraphe 1, de la directive 2002/58) et non pour les données conservées par les opérateurs pour leurs propres besoins ou dans l'intérêt de leurs abonnés (données conservées sur la base des articles 122 et 123 de la loi télécom). La CJUE cite elle-même des exceptions à ce principe (l'accès pour une finalité de lutte contre la criminalité grave à des données conservées à des fins de poursuite et de sanction d'une infraction pénale ordinaire et l'accès en vue de la sauvegarde de la sécurité nationale à des données conservées dans le cadre de la lutte contre la criminalité grave).

Pour les données conservées en vertu des articles 126, 126/1 et 127, l'article 127/1 respecte le principe précité, puisqu'il fait correspondre les finalités de conservation des données et les finalités de fourniture aux autorités de ces données.

Il prévoit cependant des exceptions à ce principe, qui ressortent du bon sens, pour les finalités de contrôle par l'IBPT ou par une autorité de protection des données de l'opérateur et les finalités de réutilisation de données à des fins de recherche scientifique ou historique ou à des fins statistiques. En effet, il ne s'agit pas de finalités qui justifient la conservation des données (les opérateurs ne conservent pas de données pour ces finalités) mais qui justifient la fourniture de données à une autorité.

Les autres objectifs de l'article 127/1, §§ 1 à 5 sont:

— apporter de la transparence aux utilisateurs finaux quant à l'utilisation de leurs données d'identification et leurs métadonnées;

— apporter de la transparence aux opérateurs quant aux différentes autorités qui peuvent leur demander des données d'identification et des métadonnées;

de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mist [sic] de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen."

Het principe vervat in deze passage van het arrest (de toegang van een autoriteit tot gegevens bewaard door een operator voor de autoriteiten kan in principe enkel gerechtvaardigd zijn door het doel van algemeen belang waarvoor die bewaring hem werd opgelegd) geldt enkel voor de gegevens bewaard door de operatoren voor de autoriteiten (artikelen 126, 126/1 en 127 zijn maatregelen genomen in hoofde van artikel 15, paragraaf 1, van Richtlijn 2002/58) en niet voor de gegevens bewaard door de operatoren voor hun eigen behoeften of in het belang van hun abonnees (gegevens bewaard op basis van de artikelen 122 en 123 van de telecomwet). Het HvJ-EU citeert zelf uitzonderingen op dat principe (de toegang om een doel van bestrijding van de zware criminaliteit tot gegevens die worden bewaard voor doeleinden van vervolging en bestraffing van een gewoon strafbaar feit en de toegang met het zicht op het bewaren van de nationale veiligheid tot gegevens bewaard in het kader van de bestrijding van zware criminaliteit).

Voor de gegevens bewaard krachtens de artikelen 126, 126/1 en 127, eerbiedigt artikel 127/1 het voormelde principe aangezien het de doeleinden van bewaring van de gegevens doet overeenstemmen met de doeleinden van verstrekking aan de autoriteiten van deze gegevens.

Het voorziet evenwel in uitzonderingen op dat principe, die onder de noemer van gezond verstand vallen, voor de doeleinden van controle door het BIPT of door een autoriteit voor de bescherming van de gegevens van de operator en de doeleinden van hergebruik van gegevens ten behoeve van wetenschappelijk of historisch onderzoek of voor statistische doeleinden. Het gaat inderdaad niet om doeleinden die de bewaring van de gegevens rechtvaardigen (de operatoren bewaren geen gegevens voor die doeleinden) maar die de verstrekking van gegevens aan een autoriteit rechtvaardigen.

De overige doelstellingen van artikel 127/1, §§ 1 tot 5 zijn:

— de eindgebruikers transparantie te geven over het gebruik van hun identificatiegegevens en hun metagegevens;

— de operatoren transparantie te bieden over de verschillende autoriteiten die aan hen identificatiegegevens en metagegevens kunnen vragen;

— assurer une certaine cohérence entre les législations sectorielles.

De manière générale, le présent article vise les autorités concernées en fonction d'une liste de finalités poursuivies et ne reprend plus une liste détaillée d'autorités comme c'était le cas de l'ancienne liste de l'article 126, § 2 et ce pour les raisons suivantes.

Cela permet d'assurer que la législation couvre les différents cas de figure et les évolutions futures. À cet égard, il convient de noter qu'il est rapidement apparu que la liste détaillée des autorités visées à l'ancien article 126, § 2 était incomplète. L'adaptation des dispositions légales qui reprennent une liste détaillée d'autorités peut être un exercice difficile (par exemple parce que la loi a été attaquée devant la Cour constitutionnelle et peut difficilement être modifiée ou parce que le gouvernement fédéral doit encore être formé) et très lent (la modification d'une loi prend généralement plusieurs mois), alors que le fait pour une autorité de ne pas figurer sur la liste (ou pas de manière entièrement correcte), alors que c'est nécessaire, provoque immédiatement des difficultés opérationnelles pour cette dernière (en pratique certains opérateurs refusent de lui communiquer les données demandées, qui sont nécessaires pour qu'elle puisse remplir ses missions).

Les données d'identification et de souscription visées par les articles 126 et 127 sont des données basiques dont ont besoin un nombre non négligeable d'autorités. On peut s'attendre à ce que ce nombre augmente à l'avenir, étant donné la croissance du nombre d'infractions commises en ligne. Il est également très difficile de dresser dans la loi une liste exhaustive de toutes les dispositions légales qui permettent aux différentes autorités d'obtenir des opérateurs des données d'identification ou des métadonnées.

Dès lors que les paragraphes 2 à 4 de l'article 127/1 comprennent des finalités de fourniture des données qui sont rédigées en termes généraux (finalités "macro"), les opérateurs et les citoyens ne peuvent, à la lecture de ces seuls paragraphes, immédiatement identifier l'ensemble des autorités qui dans la pratique tombent sous les catégories fixées par ces paragraphes. C'est pourquoi le ministre (défini à l'article 2, 2°, de la loi télécom) fera publier au *Moniteur belge* une circulaire qui reprend une liste des autorités belges qui sont habilitées à obtenir des données d'identification et des métadonnées conservées par les opérateurs sur la base de la loi télécom. L'avantage d'une circulaire par rapport à la réglementation est que la circulaire pourra être facilement et rapidement modifiée en cas de modification de l'article 127/1 ou d'une loi sectorielle ou organique qui

— een zekere coherentie tussen de sectorale wetgevingen waarborgen.

Dit artikel beoogt in het algemeen de betrokken autoriteiten op basis van een lijst van nagestreefde doeleinden en bevat niet langer een uitvoerige lijst van autoriteiten zoals dat het geval was voor de oude lijst van artikel 126, § 2, om de volgende redenen.

Zo kan ervoor gezorgd worden dat de wetgeving de verschillende gevallen en de toekomstige ontwikkelingen beslaat. In dat kader dient te worden opgemerkt dat al snel is gebleken dat de uitvoerige lijst van de autoriteiten bedoeld in het oude artikel 126, § 2, onvolledig was. De aanpassing van de wettelijke bepalingen die een uitvoerige lijst van autoriteiten omvatten, kan een moeilijke oefening zijn (bijvoorbeeld omdat de wet werd aangevochten bij het Grondwettelijk Hof en maar moeilijk kan gewijzigd worden of omdat de federale regering nog moet worden gevormd) en een erg trage oefening zijn (een wet wijzigen neemt verscheidene maanden in beslag), terwijl een autoriteit onmiddellijk operationele problemen ondervindt wanneer ze niet op de lijst staat (of niet volledig correct), terwijl dat wel nodig is (in de praktijk weigeren sommige operatoren om haar de gevraagde gegevens te bezorgen die ze nodig heeft om haar opdrachten te kunnen vervullen).

De identificatie- en abonnementsgegevens bedoeld in de artikelen 126 en 127 zijn basisgegevens die benodigd zijn door een niet-verwaarloosbaar aantal autoriteiten. Dat aantal zal wellicht toenemen in de toekomst gezien de groei van het aantal online gepleegde inbreuken. Het is ook erg moeilijk om in de wet een volledige lijst op te stellen, met alle wettelijke bepalingen die de verschillende autoriteiten in staat stellen om de identificatie- of metagegevens te verkrijgen van de operatoren.

Daar de paragrafen 2 tot 4 van artikel 127/1 doeleinden van gegevensverstrekking omvatten die in algemene bewoordingen zijn geformuleerd ("macrodoeleinden"), kunnen de operatoren en burgers bij de lezing van die paragrafen alleen niet onmiddellijk alle autoriteiten identificeren die in de praktijk onder de in die paragrafen bepaalde categorieën vallen. Daarom zal de minister (gedefinieerd in artikel 2, 2°, van de telecomwet) in het *Belgisch Staatsblad* een omzendbrief laten publiceren met daarin een lijst van de Belgische autoriteiten die gemachtigd zijn om identificatiegegevens en metagegevens te verkrijgen die worden bewaard door de operatoren krachtens de telecomwet. Het voordeel van een omzendbrief ten opzichte van de reglementering is dat de omzendbrief gemakkelijk en snel kan gewijzigd worden in geval van wijziging van artikel 127/1 of van

donne le pouvoir à une autorité d'obtenir des données d'un opérateur.

Paragraphe 1er

Dans sa jurisprudence, la CJUE fait référence à de nombreuses reprises à la criminalité grave, mais sans la définir. Il n'existe pas non plus de définition autonome de la notion de "criminalité grave" dans le droit de l'Union. Il appartient aux États membres de l'Union européenne de le déterminer. Le droit pénal et la procédure pénale relèvent de la compétence des États membres. La qualification pénale peut donc varier entre les États membres en fonction des traditions, des priorités, de la politique pénale, de l'évolution de la criminalité et des développements sociaux.

Toutefois, l'avocat général de la Cour de Justice a donné quelques indications et critères qui peuvent permettre d'arriver à une définition.

Pour l'avocat général, la notion de criminalité grave est une notion dynamique, qui se veut évolutive. Par exemple, il indique que la gravité d'une infraction pénale ne dépend pas seulement du niveau de la sanction. Le fait qu'un État membre prévoit un taux d'emprisonnement peu élevé, voire une peine alternative, n'enlève donc rien à la gravité intrinsèque du type d'infraction concerné. L'échelle des peines généralement applicables dans un État membre donné peut être une indication de la gravité des infractions concernées, mais ce n'est pas le seul aspect.

L'article 127/1 ne définit pas la notion de criminalité grave mais reprend certaines infractions qui sont considérées comme ressortant de cette notion. En effet, il est actuellement difficile de prévoir une définition exhaustive de cette notion dans la loi, étant donné qu'elle est dynamique comme le souligne l'avocat général et qu'il est difficile à l'heure actuelle d'avoir la certitude que tous les cas de figure sont couverts. Cependant, la liste fixée au paragraphe 1er pourra être complétée ultérieurement sur la base des enseignements de la pratique.

L'article 127/1, § 1er, qui donne des indications sur la notion de criminalité grave devra si nécessaire être revu en fonction de futurs arrêts éventuels de la Cour constitutionnelle et de la CJUE par rapport à la fourniture aux autorités publiques de données conservées par les opérateurs.

Le premier point du paragraphe 1er de l'article 127/1 renvoie à la peine minimale d'emprisonnement correctionnel principal visée à l'article 88*bis*, alinéa 1er, du Code d'instruction criminelle. De la sorte, une modification de

een sectorale of organieke wet die een autoriteit machtigt om gegevens te verkrijgen van een operator.

Paragraaf 1

In zijn rechtspraak verwijst het HvJ-EU heel dikwijls naar de zware criminaliteit maar zonder deze te definieren. Ook in het Unierecht bestaat er geen autonome definitie van het begrip "zware criminaliteit". Het is aan de lidstaten zelf van de Europese Unie om dit te bepalen. Het strafrecht en het strafprocesrecht behoren tot de bevoegdheid van de lidstaten. De strafrechtelijke kwalificatie kan zo verschillen tussen lidstaten onderling, in functie van tradities, prioriteiten, strafrechtelijk beleid, de evolutie van de criminaliteit en maatschappelijke ontwikkelingen.

De advocaat-generaal bij het Hof van Justitie heeft wel een aantal aanwijzingen en criteria gegeven die kunnen helpen om tot een definitie te komen.

Voor de advocaat-generaal is het begrip zware criminaliteit een dynamisch en evolutief begrip. Zo geeft hij aan dat de ernst van een strafbaar feit niet alleen afhangt van de hoogte van de straf. Het feit dat een lidstaat voorziet in een lage gevangenisstraf, of zelfs een alternatieve straf, doet dus niets af aan de intrinsieke ernst van het betrokken soort strafbaar feit. De in een bepaalde lidstaat algemeen toepasselijke schaal van sancties kan een aanwijzing zijn voor de ernst van de betrokken strafbare feiten, maar dit is niet het enige aspect.

Artikel 127/1 geeft geen definitie van het begrip van zware criminaliteit maar neemt bepaalde overtredingen over waarvan wordt beschouwd dat ze onder dit begrip vallen. Het is vandaag inderdaad moeilijk om dit begrip exhaustief te definiëren in de wet aangezien het een dynamisch begrip is zoals de advocaat-generaal benadrukt en het momenteel moeilijk is om zeker te zijn dat de lading alle gevallen dekt. De lijst vastgelegd in paragraaf 1 kan later echter worden aangevuld aan de hand van leringen uit de praktijk.

Artikel 127/1, § 1, dat inlichtingen geeft over het begrip van zware criminaliteit, zal indien nodig moeten worden herzien afhankelijk van eventuele toekomstige arresten van het Grondwettelijk Hof en van het HvJ-EU met betrekking tot de verstrekking aan de openbare autoriteiten van door de operatoren bewaarde gegevens.

Het eerste punt van paragraaf 1 van artikel 127/1 verwijst naar de minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88*bis*, eerste lid, van het Wetboek van Strafvordering. Zo zal automatisch rekening gehouden

cet article 88*bis* sera automatiquement prise en compte pour l'application de l'article 127/1, § 1er, de la loi télécom.

Jusqu'à la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, il était possible, dans le cadre d'une procédure pénale belge, de requérir des données relatives au trafic et à la localisation dans le cadre d'une instruction sur toutes les infractions possibles. Lors de la rédaction de la loi du 29 mai 2016, le législateur a estimé nécessaire d'introduire une limite claire dans l'article 88*bis* du Code d'instruction criminelle applicable. La loi a introduit que cette mesure ne peut être utilisée que s'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

La collecte de telles données constitue une limitation des droits et libertés individuels et, en vertu du principe de proportionnalité, ne peut par conséquent être autorisée qu'en cas d'infraction proportionnelle à l'ordre juridique. Le même seuil est utilisé pour la délivrance d'un mandat d'arrêt (article 16 de la loi du 20 juillet 1990 relative à la détention préventive) et des mesures d'instruction analogues telles l'interception du courrier (article 46*ter* Code d'instruction criminelle) ainsi que la collecte de renseignements sur les comptes bancaires (article 46*quater* Code d'instruction criminelle).

En outre, les infractions pénales qui sont punies d'une sanction de niveau 5 ou 6 au sens de l'article XV.70 du Code de droit économique relèvent de la criminalité grave:

"La sanction de niveau 5 est constituée d'une amende pénale de 250 à 100 000 euros et d'un emprisonnement d'un mois à un an ou d'une de ces peines seulement.

La sanction de niveau 6 est constituée d'une amende pénale de 500 à 100 000 euros et d'un emprisonnement d'un an à cinq ans ou d'une de ces peines seulement."

Comme indiqué ci-dessus, l'avocat général indique que "le fait qu'un État membre prévoit un taux d'emprisonnement peu élevé, voire une peine alternative, n'enlève donc rien à la gravité intrinsèque du type d'infraction concerné." On peut donc considérer que peuvent relever de la notion de criminalité grave au sens de la jurisprudence de la CJUE des infractions soumises à des sanctions administratives très élevées (une peine alternative à une peine d'emprisonnement), qui punissent des infractions graves.

worden met een wijziging van dat artikel 88*bis* bij de toepassing van artikel 127/1, § 1, van de telecomwet.

Tot voor de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, was het in de Belgische strafprocedure mogelijk, in het kader van een gerechtelijk onderzoek, verkeers- en lokalisatiegegevens op te vragen bij de opsporing naar alle mogelijke misdrijven. Bij de totstandkoming van de wet van 29 mei 2016 achtte de wetgever het noodzakelijk om een duidelijke grens in te voeren in het toepasselijke artikel 88*bis* van het Wetboek van strafvordering. In de wet werd ingevoerd dat de maatregel enkel nog gebruikt kan worden wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben.

Het inwinnen van dergelijke gegevens vormt een beperking van de individuele rechten en vrijheden en kan derhalve, ingevolge het proportionaliteitsbeginsel, slechts worden toegestaan, ingeval van een evenredige inbreuk op de rechtsorde. Dezelfde drempel wordt gehanteerd voor het verlenen van een aanhoudingsmandaat (artikel 16 van de wet van 20 juli 1990 betreffende de voorlopige hechtenis), en gelijkaardige onderzoeksmaatregelen zoals het onderscheppen van post (artikel 46*ter* Wetboek van strafvordering), en het inwinnen van inlichtingen betreffende bankrekeningen (artikel 46*quater* Wetboek van strafvordering).

Bovendien vallen de strafrechtelijke inbreuken die worden bestraft met een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht, onder zware criminaliteit:

"De sanctie van niveau 5 bestaat uit een strafrechtelijke geldboete van 250 tot 100 000 euro en een gevangenisstraf van één maand tot één jaar of uit één van die straffen alleen.

De sanctie van niveau 6 bestaat uit een strafrechtelijke geldboete van 500 tot 100.000 euro en een gevangenisstraf van één jaar tot vijf jaar of uit één van die straffen alleen."

Zoals hierboven vermeld, geeft de advocaat-generaal aan: "Het feit dat een lidstaat voorziet in een lage gevangenisstraf, of zelfs een alternatieve straf, doet dus niets af aan de intrinsieke ernst van het betrokken soort strafbaar feit." We kunnen dus beschouwen dat het begrip van zware criminaliteit in de zin van de rechtspraak van het HvJ-EU overtredingen kan omvatten die onderhevig zijn aan erg hoge administratieve sancties (een alternatieve straf voor een gevangenisstraf), als bestraffing van zware overtredingen.

Le simple fait que des autorités administratives soient compétentes pour la prévention, la recherche, la détection ou la poursuite de tels faits, et/ou qu'elles puissent punir de tels faits par une sanction administrative, n'ôte en effet rien à la gravité de ces faits. Souvent, cette voie administrative a été mise en place précisément pour décharger le parquet et pour tenir compte de l'expertise technique. La demande d'une autorité administrative dans le cadre de son enquête d'obtenir des données de communications électroniques porte donc tout autant sur un fait suffisamment grave pour justifier la fourniture de ces données et vise à préserver la même unité de l'intérêt légal protégé qu'en cas d'intervention des autorités pénales.

Sont ainsi visées par la notion de criminalité grave les infractions aux articles 14 et 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché), à savoir aux interdictions administratives en matière d'abus de marché (voir le point 3° de cette disposition), qui sont passibles d'amendes administratives maximales très élevées (s'agissant de personnes physiques, 5 millions d'euros et, s'agissant de personnes morales, 15 millions d'euros ou, si le montant obtenu par application de ce pourcentage est plus élevé, 15 % du chiffre d'affaires annuel total) (voir l'article 36, § 2, alinéa 2, 2°, de la loi du 2 août 2002). Ces amendes maximales sont considérablement plus élevées que celles prévues pour les infractions aux autres dispositions dudit règlement et à la plupart des autres législations financières (voir notamment l'article 36, § 2, de la loi du 2 août 2002). La raison en est que l'impact de ces infractions sur l'intégrité des marchés financiers et sur la confiance des investisseurs est important; elles font partie, au sein du secteur financier, des infractions les plus graves. La gravité de ces infractions ressort en outre du fait que les mêmes faits (sous réserve de la présence d'une intention) sont également passibles de sanctions pénales qui peuvent aller jusqu'à quatre ans d'emprisonnement en cas de manipulation de marché ou d'opération d'initié et jusqu'à deux ans d'emprisonnement en cas de divulgation d'informations privilégiées (voir les articles 39 et 40 de la loi du 2 août 2002).

Paragraphe 2

2°: la prévention des menaces graves pour la sécurité publique

Cette finalité est une des finalités mentionnées dans l'arrêt La Quadrature du Net de la CJUE.

Het loutere feit dat administratieve autoriteiten bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van dergelijke feiten, en/of dat zij dergelijke feiten kunnen bestraffen met een administratieve sanctie, doet immers niets af aan de ernst ervan. Vaak is die administratieve weg precies ingesteld om het parket te ontlasten en rekening te houden met technische expertise. De vraag van een administratieve overheid om in het kader van haar onderzoek elektronische communicatiegegevens te verkrijgen, heeft dan evenzeer betrekking op een feit dat voldoende ernstig is om de verstrekking van deze gegevens te verantwoorden en heeft tot doel hetzelfde beschermde rechtsgoed te vrijwaren als bij een optreden van de strafrechtelijke autoriteiten.

Aldus vallen ook inbreuken op de artikelen 14 en 15 van de Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik), zijnde de administratieve verbodsbepalingen inzake marktmisbruik (zie punt 3° van deze bepaling), waarop zeer hoge maximale administratieve geldboetes staan (voor natuurlijke personen 5 miljoen euro en voor rechtspersonen 15 miljoen euro of, indien dit hoger is, 15 procent van de totale jaaromzet (zie artikel 36, § 2, tweede lid, 2°, van de wet van 2 augustus 2002)), onder het begrip zware criminaliteit. Dergelijke maximum boetes zijn aanzienlijk hoger dan voor de inbreuken op andere bepalingen van de Verordening marktmisbruik en op de meeste andere financiële wetgeving (zie met name artikel 36, § 2, van de wet van 2 augustus 2002). Dit omdat de impact van deze inbreuken op de integriteit van de financiële markten en het vertrouwen van de beleggers groot is; binnen de financiële sector gaat het om één van de meest ernstige inbreuken. Bovendien blijkt de ernst van de inbreuk ook uit het feit dat voor dezelfde feiten (mits de aanwezigheid van opzet) ook strafrechtelijke sancties zijn voorzien die kunnen oplopen tot vier jaar gevangenisstraf voor marktmanipulatie en handel met voorwetenschap en tot twee jaar gevangenisstraf voor mededeling van voorwetenschap (zie artikelen 39 en 40 van de wet van 2 augustus 2002).

Paragraaf 2

2°: de preventie van ernstige bedreigingen voor de openbare veiligheid

Dit is een van de doeleinden vermeld in het arrest-*La Quadrature du Net* van het HvJ-EU.

3°: la sauvegarde des intérêts vitaux d'une personne physique

Cette finalité correspond à celle reprise à l'article 6.1, d) du RGPD ("le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique").

En pratique, on peut penser aux hypothèses suivantes: l'utilisation de données de localisation par la cellule personne disparue de la police fédérale (en cas de disparition inquiétante, la police ne peut pas toujours immédiatement déterminer s'il s'agit d'un acte criminel ou non) et par les services d'urgence offrant de l'aide sur place (100, 101 et 112). Pour ces derniers services, l'article 107 de la loi télécom prévoit que l'opérateur doit fournir les données de localisation de l'appelant aux services d'urgence qui offrent de l'aide sur place lors de l'appel. En cas de difficultés techniques pour la fourniture de ces données de localisation en temps réel, ces services doivent pouvoir obtenir les dernières données de localisation de l'appelant conservées.

4°: la sécurité des réseaux, des services et des systèmes d'information

Les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau de communications électroniques, du service de communications électroniques ou des systèmes d'information sont à l'heure actuelle l'IBPT et le Centre pour la Cybersécurité Belgique (CCB). En sa qualité de CSIRT national, le CCB est, en effet, chargé, en vertu de l'article 60 de la loi NIS (loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique) de la détection, de l'observation et de l'analyse des problèmes de sécurité informatique en Belgique.

5°: les infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques

L'article 127, § 2, alinéa 1er, 5°, fait référence à une infraction commise en ligne (ex. hacking, vente de produits illicites, toute infraction sur internet) ou par le biais d'un réseau ou service de communications électroniques (ex. smishing, harcèlement par téléphone, etc.), que l'infraction soit punie par une sanction pénale et/ou par une sanction administrative. Il ne s'agit donc pas d'une infraction dont les faits constitutifs ont été commis dans le monde physique (ex. viol, vol, meurtre, etc.) et pour laquelle un moyen de communications électroniques a été utilisé (par exemple un échange de messages en vue de préparer une infraction). Une infraction commise en ligne ou par téléphone/SMS ne laisse que des traces

3°: de bescherming van de vitale belangen van een natuurlijke persoon

Dit doeleinde stemt overeen met dat van artikel 6.1, d) van de AVG ("de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen").

In de praktijk kan men denken aan de volgende gevallen: het gebruik van locatiegegevens door de cel Vermiste Personen van de federale politie (in geval van een onrustwekkende verdwijning kan de politie niet altijd onmiddellijk bepalen of het om een misdrijf gaat of niet) en door de nooddiensten die ter plaatse hulp bieden (100, 101 en 112). Voor die laatste diensten schrijft artikel 107 van de telecomwet voor dat de operator tijdens de oproep de locatiegegevens van de oproeper moet verstrekken aan de nooddiensten die ter plaatse hulp bieden. Bij technische moeilijkheden voor de realtimeverstrekking van deze locatiegegevens moeten deze diensten de laatste, bewaarde locatiegegevens van de oproeper kunnen krijgen.

4°: de veiligheid van de netwerken, de diensten en de informatiesystemen

De autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of -dienst of de informatiesystemen zijn momenteel met name het BIPT en het Centrum voor Cybersecurity België (CCB). In zijn hoedanigheid van nationaal CSIRT is het CCB immers, krachtens artikel 60 van de NIS-wet (wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid), belast met het opsporen, observeren en analyseren van computerbeveiligingsproblemen in België.

5°: de inbreuken gepleegd online of via een elektronische-communicatienetwerk of -dienst

Artikel 127, § 2, eerste lid, 5°, verwijst naar een online gepleegde inbreuk (bijv. hacking, verkoop van verboden producten, elke inbreuk op het internet) of via een elektronische-communicatiedienst (bijv. smishing, telefonische pesterijen, enz.), ongeacht of de inbreuk bestraft wordt met een strafrechtelijke straf en/of met een administratieve straf. Het gaat dus niet om een inbreuk waarvan de feiten gepleegd zijn in de fysieke wereld (bijv. verkrachting, diefstal, moord, enz.) en waarvoor een elektronische-communicatiemiddel is gebruikt (bijv. een uitwisseling van berichten om een inbreuk voor te bereiden). Een inbreuk die online is gepleegd of via de telefoon/een sms laat enkel digitale sporen na. Daarom

numériques. Dès lors, il n'est pas acceptable que les autorités qui recherchent et/ou poursuivent ce type d'infraction ne soient pas autorisées à obtenir ces traces numériques, que l'infraction soit grave ou pas. En effet, n'autoriser la fourniture de ces données que lorsque l'infraction relève de la criminalité grave impliquerait qu'il ne serait en pratique pas possible de poursuivre ce type d'infraction dans les autres cas de figure, ce qui serait contraire à l'État de droit. Concernant la fourniture de données conservées par les opérateurs aux autorités, il y a donc lieu de tenir compte non seulement de la gravité de l'infraction mais aussi de la nature de l'infraction (infraction online/offline).

Les autorités administratives couvertes par le cinquième point (5°) sont entre autres les autorités suivantes:

le Centre pour la Cybersécurité Belgique (CCB) car ses différentes tâches légales, telles que fixées par l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique et la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS), visent notamment à prévenir et détecter les infractions pénales en matière de cybercriminalité (diffusion de messages d'alerte ou d'informations sur les risques et incidents auprès des parties intéressées; information et sensibilisation des utilisateurs des systèmes d'information et de communication);

le service de médiation pour les télécommunications, qui est une autorité chargée d'apporter de l'aide aux personnes (et non un service de police). Il fournit à la victime d'une utilisation malveillante du réseau (en particulier le harcèlement téléphonique) le nom, le prénom et l'adresse de l'auteur de cette utilisation conformément à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

les agents visés à l'article XV.2, § 1er du Code de droit économique, de la Direction générale Qualité et Sécurité ou de la Direction générale de l'Inspection économique du Service Public Fédéral Économie, PME, Classes Moyennes et Énergie, en vue de l'exercice de la compétence visée à l'article XV.3, 5°/1 du même Code, dans le cadre de leurs compétences légalement attribuées. Ces agents peuvent demander aux opérateurs les données permettant l'identification des auteurs d'infractions aux législations qui relèvent de leurs compétences, agissant sous l'anonymat, sous une fausse dénomination, sous un pseudonyme ou toute autre forme qui empêche de connaître l'identité réelle de l'acteur économique;

is het dan ook niet aanvaardbaar dat de autoriteiten die dit soort van inbreuk onderzoeken en/of vervolgen, niet gemachtigd zijn om deze digitale sporen te krijgen, ongeacht of de inbreuk nu ernstig is of niet. De verstrekking van deze gegevens enkel toestaan wanneer de inbreuk onder zware criminaliteit valt, zou immers impliceren dat het in de praktijk niet mogelijk zou zijn om dergelijke inbreuken te vervolgen in andere gevallen, wat in strijd zou zijn met de rechtsstaat. Wat betreft de verstrekking aan de autoriteiten van door de operatoren bewaarde gegevens dient er dus niet enkel rekening te worden gehouden met de ernst van de inbreuk maar ook met de aard van de inbreuk (online/offline inbreuk).

De administratieve autoriteiten die onder het vijfde punt (5°) vallen, zijn onder andere de volgende:

het Centrum voor Cybersecurity België (CCB) want zijn verschillende wettelijke taken, zoals bepaald bij het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België en de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS-wet), zijn er meer bepaald op gericht om de strafbare feiten inzake cybercriminaliteit te voorkomen en op te sporen (verspreiden van waarschuwingen of informatie over de risico's en incidenten onder de geïnteresseerden; informeren en sensibiliseren van de gebruikers van informatie- en communicatiesystemen);

de Ombudsdienst voor telecommunicatie, die een autoriteit is die belast is met het bieden van hulp aan personen (en geen politiedienst). Hij verstrekt aan slachtoffers van kwaadwillig gebruik van het netwerk (in het bijzonder van telefonische pesterijen) de naam, voornaam en het adres van de dader van dat gedrag conform artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

de ambtenaren bedoeld in artikel XV.2, § 1 van het Wetboek van economisch recht, van de Algemene Directie Kwaliteit en Veiligheid of van de Algemene Directie Economische Inspectie van de federale overheidsdienst Economie, kmo, Middenstand en Energie, met het oog op de uitoefening van de bevoegdheid als bedoeld in artikel XV.3, 5°/1 van hetzelfde Wetboek, in het kader van hun wettelijk toegekende bevoegdheden. Deze ambtenaren mogen aan de operatoren de gegevens vragen die de identificatie mogelijk maken van plegers van de inbreuken op de wetgevingen die onder hun bevoegdheid vallen, die anoniem handelen, onder een valse benaming, onder een pseudoniem of onder een andere vorm die verhindert de werkelijke identiteit van de economische speler te kennen;

les membres du personnel statutaire ou contractuel du SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement, visé à l'article 11 de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits, dans le cadre des compétences qui leur sont accordées par la loi. Ces personnes peuvent demander aux opérateurs les données permettant l'identification des auteurs d'infractions aux législations qui relèvent de leurs compétences, agissant sous l'anonymat, sous une fausse dénomination, sous un pseudonyme ou toute autre forme qui empêche de connaître l'identité réelle de l'acteur économique.

Un certain nombre d'autorités administratives (cf. SPF Santé publique et SPF Économie précités) sont chargées du contrôle du respect de certaines législations dans le cadre des activités qui se font en ligne. Ce contrôle implique de rechercher les infractions et de les constater. En cas de constatation d'une infraction, le parquet ou l'autorité administrative pourra la poursuivre.

En pratique, les autorités qui sont compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques ne pourront pas toutes obtenir de l'opérateur des données qui permettent de tirer des conclusions précises sur les personnes concernées. Cela dépendra de la loi organique/sectorielle de chaque autorité. À titre d'exemple, le service de médiation pour les télécommunications ne fait qu'identifier l'auteur des appels malveillants alors que les autorités judiciaires pourraient être amenées à localiser l'équipement terminal qui a été utilisé pour commettre une infraction en ligne ou par le biais d'un service de téléphonie mobile (par exemple une machine qui est utilisée pour envoyer du "smishing").

6°: la criminalité grave

Tombent sous le point 6° entre autres les agents visés à l'article XV.2 du Code de droit économique pour exercer la compétence visée à l'article XV.3, 5°/1, à condition que cela se fasse en vue de la prévention, la recherche, la détection ou la poursuite de la criminalité grave.

L'auditeur de la FSMA agit également dans le cadre de la lutte contre les formes graves de criminalité, notamment lorsqu'il enquête sur les abus de marché (voir le commentaire concernant la définition de criminalité grave au § 1er).

de statutaire of contractuele personeelsleden van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu zoals bedoeld in art. 11 van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere produkten, in het kader van hun wettelijk toegekende bevoegdheden. Deze personen mogen aan de operatoren de gegevens vragen die de identificatie mogelijk maken van plegers van de inbreuken op de wetgevingen die onder hun bevoegdheid vallen, die anoniem handelen, onder een valse benaming, onder een pseudoniem of onder een andere vorm die verhindert de werkelijke identiteit van de economische speler te kennen.

Een zeker aantal administratieve autoriteiten (cf. de voormelde FOD Volksgezondheid en FOD Economie) zijn belast met de controle op de eerbiediging van bepaalde wetgevingen in het kader van de activiteiten die online plaatsvinden. Deze controle houdt het onderzoek en de vaststelling van inbreuken in. Wanneer een inbreuk wordt vastgesteld, zal het parket of de administratieve autoriteit die vervolgen.

In de praktijk zullen de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een inbreuk die online werd gepleegd of via een elektronische-communicatienetwerk of -dienst niet allemaal gegevens kunnen verkrijgen van de operator aan de hand waarvan precieze conclusies kunnen worden getrokken in verband met de betrokken personen. Dat zal afhangen van de organieke/sectorale wet van elke autoriteit. Zo identificeert de Ombudsdienst voor telecommunicatie enkel de dader van kwaadwillige oproepen terwijl de gerechtelijke autoriteiten zouden kunnen gevraagd worden om de eindapparatuur die werd gebruikt om online of via een mobiele-telefoniedienst een inbreuk te plegen, te lokaliseren (bijvoorbeeld een toestel dat werd gebruikt voor "smishing").

6°: zware criminaliteit

Vallen onder punt 6° onder andere de ambtenaren bedoeld in artikel XV.2 van het Wetboek van economisch recht, om de bevoegdheid uit te oefenen bedoeld in artikel XV.3, 5°/1 van hetzelfde Wetboek, op voorwaarde dat dit gebeurt met het oog op de preventie, het onderzoek, de opsporing of de vervolging van zware criminaliteit.

Ook de auditeur van de FSMA treedt op voor doeleinden van de strijd tegen zware criminaliteit, met name wanneer hij een onderzoek voert naar marktmisbruik (zie de toelichting bij de definitie van zware criminaliteit in § 1).

7°: l'intérêt économique ou financier important

Le point 7 est inspiré de l'article 23.1, e), du RGPD et reprend certaines autorités administratives qui sont compétentes pour poursuivre des infractions qui ne constituent pas (toujours) également des infractions au sens du Code pénal.

Il s'agit d'abord de l'auditeur (ou, en son absence, de l'auditeur adjoint) de la FSMA. Celui-ci est en effet habilité à demander des données aux fins prévues par les articles 81, 82, 2° et 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ou par les dispositions qui déclarent ces articles d'application, notamment dans le cadre d'une enquête administrative portant sur certaines infractions à la législation financière dont la FSMA – qui poursuit ainsi des objectifs importants d'intérêt public général au sens de l'article 23, paragraphe 1, point e), du RGPD (voir déjà l'exposé des motifs portant sur l'article 46*bis* de la loi du 2 août 2002: Doc 54, 3172/001, p. 61) – contrôle le respect. Ces infractions font l'objet d'une sanction administrative à caractère pénal. Font également partie de ces infractions celles qui ne relèvent pas de la criminalité grave (voir le point 6°), et ne constituent pas non plus des infractions au sens du Code pénal (voir le point 8°), et qui tombent par conséquent sous le point 7°.

Lorsque la FSMA (par la voie de son auditeur) requiert ces données pour répondre aux demandes de coopération émanant d'autorités compétentes d'autres États membres de l'EEE ou d'États tiers qui exercent des compétences comparables à celles de la FSMA (voir les articles 81, 82, 2°, et 84 juncto 35, § 1er, alinéa 1er, de la loi du 2 août 2002), elle poursuit également de tels objectifs importants d'intérêt public général de l'Union européenne ou de la Belgique. Il est en effet aussi dans l'intérêt économique et financier de la Belgique que l'on coopère sur le plan international pour lutter contre de telles infractions financières, étant donné que cette coopération se fait sur la base de réciprocité.

Les finalités poursuivies par l'auditeur sont considérées comme étant d'une importance supérieure (ou à tout le moins d'importance équivalente) aux finalités pour lesquelles les données ont été conservées en vertu des articles 122 et 123, de sorte que la fourniture de ces données est justifiée. Il se fait par ailleurs que la réglementation européenne, et en particulier l'article 23, paragraphe 2, h), du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché ("règlement relatif aux abus de marché"), l'article 69, paragraphe 2, r), de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments

7°: belangrijk economisch of financieel belang

Punt 7 is gebaseerd op artikel 23.1, e) van de AVG en vermeldt een aantal administratieve autoriteiten die bevoegd zijn om inbreuken te vervolgen die niet (altijd) ook een inbreuk vormen in de zin van het Strafwetboek.

Ten eerste gaat het om de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) van de FSMA. Hij heeft immers de bevoegdheid om deze gegevens op te vragen voor de doeleinden bepaald in de artikelen 81, 82, 2° en 84, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten of in de bepalingen die deze artikelen van toepassing verklaren, met name in het kader van een administratiefrechtelijk onderzoek naar bepaalde inbreuken op de financiële wetgeving waarvoor de FSMA – die daarbij belangrijke doelstellingen van algemeen belang in de zin van artikel 23, lid 1, punt e), van de AVG nastreeft (zie reeds de memorie van toelichting bij artikel 46*bis* van de wet van 2 augustus 2002: Doc 54, 3172/001, p. 61) – bevoegd is. Deze inbreuken worden gesanctioneerd met een administratieve sanctie met strafkarakter. Hieronder vallen ook inbreuken die geen zware criminaliteit betreffen (zie punt 6°), en ook geen misdrijf in de zin van het Strafwetboek (zie punt 8°), en die bijgevolg onder punt 7° ressorteren.

Ook wanneer de FSMA (via haar auditeur) de gegevens opvraagt om tegemoet te komen aan verzoeken om samenwerking vanwege bevoegde autoriteiten van andere lidstaten van de EER of van derde staten die vergelijkbare bevoegdheden uitoefenen als de FSMA (zie artikelen 81, 82, 2° en 84 juncto 35, § 1, eerste lid, van de wet van 2 augustus 2002) streeft zij dergelijke belangrijke doelstellingen van algemeen belang van de Europese Unie of van België na. Het is immers ook in het Belgisch economisch en financieel belang dat voor de bestrijding van dergelijke financieelrechtelijke inbreuken internationaal wordt samengewerkt aangezien dit gebeurt op basis van wederkerigheid.

De doeleinden die de auditeur nastreeft, worden beschouwd als zijnde zwaarwichtiger dan (of minstens van een gelijkwaardig belang) de doeleinden waarvoor de gegevens werden bewaard op grond van de artikelen 122 en 123, zodat de verstrekking van deze gegevens gerechtvaardigd is. Het is overigens ook zo dat Europese regelgeving, en met name artikel 23, lid 2, h), van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik ("Verordening marktmisbruik"), artikel 69, lid 2, r), van Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten ("MiFID II") en

financiers (“MiFID II”) et l’article 98, paragraphe 2, d), i), de la directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM) (“UCITS”), impose que, dans la mesure où le droit national autorise que les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications soient réclamés (ce qui est le cas en Belgique), les autorités administratives compétentes telles que la FSMA doivent également pouvoir requérir ces données.

Il s’agit ensuite de l’Autorité belge de la concurrence, afin de refléter les pouvoirs dont elle dispose en vertu de l’article IV.40 du Code de droit économique pour déceler des infractions au droit de la concurrence. Cette autorité est compétente pour appliquer les règles de droit de la concurrence (notamment les articles IV.1 et IV.2, IV.2/1 du Code du droit économique et les articles 101 et 102 TFEU) qui sont d’ordre public (CJUE, arrêt du 1er juin 1999, Eco Swiss,, C-126/97, §§ 36-40 et CJUE, arrêt du 13 juillet 2006, C-295/04 à C-298/04, Manfredi, § 31). La politique de la concurrence est une politique d’intérêt général, tout comme le droit de la concurrence est un droit qui relève de l’ordre public économique (voyez en ce sens, TUE, 8 juillet 2008, affaire T-54/03, Lafarge c/ Commission et Conseil, § 718 et TPIUE, 12 juillet 2011, affaire T-113/07, Toshiba Corp c/ Commission, § 281). Par ailleurs, la Cour de Justice de l’Union européenne a reconnu le caractère secret des cartels et la difficulté, par conséquent, de démontrer leur existence (voyez notamment CJUE, arrêt du 7 janvier 2004, C-204/00 P et alii, Aalborg Portland §§ 55-57). La tâche de protection de la concurrence dont l’Autorité belge de concurrence est investie constitue donc une mission d’intérêt économique général. Cette finalité est considérée comme étant d’une importance supérieure, ou à tout le moins d’importance équivalente, aux finalités pour lesquelles les données ont été conservées en vertu des articles 122 et 123, de sorte que la fourniture de ces données est justifiée.

8°: le fait qui constitue une infraction pénale, sans relever de la criminalité grave

Le point 8 du paragraphe 2 vise un fait qui constitue une infraction pénale au sens de l’article 1er du Code pénal mais qui ne relève pas de la criminalité grave. La catégorie fixée au point 8 est applicable, que la recherche du fait qui constitue l’infraction pénale et les poursuites soient faites par une autorité administrative (qui impose par exemple une amende administrative) ou par une autorité judiciaire. Il n’y a en effet pas de raison de ne pas prévoir les mêmes possibilités de recherche pour la voie administrative par rapport à la voie pénale, la voie

artikel 98, lid 2, d), i), van Richtlijn 2009/65/EG van het Europees Parlement en de Raad van 13 juli 2009 tot coördinatie van de wettelijke en bestuursrechtelijke bepalingen betreffende bepaalde instellingen voor collectieve belegging in effecten (icbe’s) (“UCITS”), vereist dat indien de nationale wetgeving toestaat dat bestaande verkeersgegevensoverzichten waarover een telecommunicatie-exploitant beschikt, worden opgevraagd (wat in België het geval is), ook de bevoegde administratieve autoriteiten zoals de FSMA deze gegevens moeten kunnen opvragen.

Ten tweede gaat het om de Belgische Mededingingsautoriteit, om de bevoegdheden te weerspiegelen waarover zij beschikt krachtens artikel IV.40 van het Wetboek van economisch recht om inbreuken op het mededingingsrecht op te sporen. Deze autoriteit is bevoegd om de concurrentieregels toe te passen (met name de artikelen IV.1, IV.2 en IV.2/1 van het Wetboek van economisch recht en de artikelen 101 en 102 VWEU) die van openbare orde zijn (zie HvJ-EU, arrest van 1er juin 1999, Eco-Swiss, C-126/97, §§ 36-40 en HvJ-EU, arrest van 13 juli 2006, C-295/04 tot C-298/04, Manfredi, § 31). Het mededingingsbeleid is een beleid van algemeen belang, net zoals het mededingingsrecht een recht is dat onder de economische openbare orde valt (zie in die zin, GEA, 8 juli 2008, zaak T-54/03, Lafarge tg/ Commissie en Raad, § 718 en GEA, 12 juli 2011, zaak T-113/07, Toshiba Corp tg/ Commissie, § 281). Daarenboven heeft het Hof van Justitie van de Europese Unie het clandestiene karakter erkend van kartels en dus de moeilijkheid om het bestaan ervan te bewijzen (zie HvJ-EU, arrest van 7 januari 2004, C-204/00 P et alii, Aalborg Portland §§ 55-57). De taak om de mededinging te beschermen waarmee de Belgische Mededingingsautoriteit is belast, vormt dus een doelstelling van algemeen economisch belang. Dit doeleinde wordt beschouwd als zijnde zwaarwichtiger of minstens van een gelijkwaardig belang als de doeleinden waarvoor de gegevens werden bewaard op grond van de artikelen 122 en 123, zodat de verstrekking van deze gegevens gerechtvaardigd is.

8°: het feit dat een strafrechtelijke inbreuk vormt, zonder onder zware criminaliteit te vallen

Punt 8 van paragraaf 2 doelt op een feit dat een strafrechtelijke inbreuk vormt in de zin van artikel 1 van het Strafwetboek maar dat niet onder de zware criminaliteit valt. De categorie vastgelegd in punt 8 is toepasselijk, ongeacht of het onderzoek van het feit dat de strafbare inbreuk vormt en de vervolging worden gedaan door een administratieve autoriteit (die bijvoorbeeld een administratieve boete oplegt) dan wel door een gerechtelijke autoriteit. Er is immers geen reden om voor de administratieve weg niet in dezelfde onderzoeksmogelijkheden

administrative ayant été mise en place pour décharger le parquet.

Il reviendra à la législation organique/sectorielle qui permet à l'autorité de demander à l'opérateur des données d'identification ou des métadonnées d'assurer la proportionnalité de la demande, conformément à la jurisprudence applicable.

À cet égard, la CJUE, dans son l'arrêt "Prokuratuur" du 2 mars 2021 (affaire C-746/18), a décidé ce qui suit:

"L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période." (voir dispositif).

Les faits à l'origine de cet arrêt concernaient la fourniture à une autorité de données conservées par un opérateur pour les autorités et ne concernaient donc pas la fourniture à une autorité de données conservées par un opérateur pour ses propres besoins ou dans l'intérêt de ses clients (art. 122 et 123 de la loi télécom). Cependant, le principe de proportionnalité dégagé dans cet arrêt de la CJUE doit constituer un fil conducteur dans tous les cas de figure. Il se retrouve dans le Code d'instruction criminelle. En effet, en vertu de l'article 46*bis* du Code d'instruction criminelle, le procureur du Roi peut demander à un opérateur des données d'identification pour la recherche des crimes

te voorzien als voor de strafrechtelijke weg, aangezien de administratieve weg is ingesteld om het parket te ontlasten.

Het is aan de organieke/sectorale wetgeving die de autoriteit machtigt om aan de operator identificatie- of metagegevens te vragen, om te zorgen voor de evenredigheid van het verzoek, conform de toepasselijke rechtspraak.

Wat dat betreft, heeft het HvJ-EU in zijn arrest-Prokuratuur van 2 maart 2021 (zaak C-746/18) het volgende beslist:

"Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer - welke toegang niet beperkt is tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid - , en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn." (zie dispositief).

De feiten aan de basis van dat arrest hadden betrekking op de verstrekking aan een autoriteit van gegevens bewaard door een operator voor de autoriteiten en hadden dus geen betrekking op de verstrekking aan een autoriteit van gegevens bewaard door een operator voor zijn eigen behoeften of in het belang van zijn klanten (art. 122 en 123 van de telecomwet). Het evenredigheidsbeginsel dat voortvloeit uit dat arrest van het HvJ-EU moet evenwel de rode draad vormen in alle gevallen. Het is vastgelegd in het Wetboek van Strafvordering. Krachtens artikel 46*bis* van het Wetboek van Strafvordering kan de procureur des Konings immers aan een operator identificatiegegevens vragen voor het

et délits. Sur la base de l'article 88*bis* du Code d'instruction criminelle, le juge d'instruction pourra demander à un opérateur de procéder au repérage des données de trafic de moyens de communications électroniques à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées et à la localisation de l'origine ou de la destination de communications électroniques, uniquement s'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, ce qui est un seuil plus élevé que les "crimes et délits" mentionnés dans l'article 46*bis* du Code d'instruction criminelle. Ce seuil plus élevé se justifie par le fait que les données que l'autorité judiciaire demande à l'opérateur constituent une ingérence plus grande dans la vie privée des intéressés dans le cadre de l'article 88*bis* que dans le cadre de l'article 46*bis*.

Les autorités visées au point 8° du paragraphe 2 comprennent notamment les autorités judiciaires et les agents visés à l'article XV.2 du Code de droit économique, pour exercer la compétence visée à l'article XV.3, 5°/1 du même Code.

9°: le contrôle des opérateurs

La pratique montre que pour un contrôle efficace du respect par les opérateurs de la législation télécom, il est parfois nécessaire que les officiers de police judiciaire de l'IBPT consultent une base de données d'un opérateur et puissent y effectuer des contrôles.

10°: la réutilisation de données à des fins de recherche scientifique ou historique ou à des fins statistiques

Cette finalité est inspirée de l'article 56 du RGPD. Conformément à l'article 5, al. 1er, b) du RGPD, le traitement de données, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales. Aux termes de l'article 89, al. 1er, du règlement précité, le traitement à des fins statistiques est soumis à des garanties appropriées pour les droits et libertés de la personne concernée.

S'agissant des mesures techniques et organisationnelles, le considérant 163 du RGPD renvoie au règlement (CE) n° 223/2009 du Parlement européen et du Conseil.

onderzoek van misdaden en wanbedrijven. Op basis van artikel 88*bis* van het Wetboek van Strafvordering zal de onderzoeksrechter uitsluitend aan een operator kunnen vragen om verkeersgegevens van elektronische-communicatiemiddelen te vergaren vanaf welke elektronische communicatie wordt of werd verstuurd of aan welke elektronische communicatie wordt of werd gericht, en om de herkomst of de bestemming van elektronische communicatie te lokaliseren, wanneer er ernstige aanwijzingen bestaan dat de inbreuken van die aard zijn dat ze kunnen leiden tot een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf, wat een hogere drempel is dan "een misdaad of een wanbedrijf" zoals vermeld in artikel 46*bis* van het Wetboek van Strafvordering. Deze hogere drempel is gerechtvaardigd door het feit dat de gegevens die de gerechtelijke autoriteit vraagt aan de operator, een grotere inmenging vormen in de persoonlijke levenssfeer van de betrokkenen in het kader van artikel 88*bis* dan in het kader van artikel 46*bis*.

De autoriteiten bedoeld in punt 8° van paragraaf 2 betreffen onder meer de gerechtelijke autoriteiten en de ambtenaren bedoeld in artikel XV.2 van het Wetboek van economisch recht, voor het uitoefenen van de bevoegdheden bedoeld in artikel XV.3, 5°/1 van hetzelfde Wetboek.

9°: controle van de operatoren

De praktijk toont dat voor een doeltreffende controle van de eerbiediging van de telecomwetgeving door de operatoren, de officieren van gerechtelijke politie van het BIPT soms een databank van een operator moeten raadplegen en daarin controles moeten kunnen uitvoeren.

10°: het hergebruik van gegevens voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden

Dit doeleinde is gebaseerd op artikel 56 van de AVG. In overeenstemming met artikel 5, eerste lid, van de AVG moeten gegevensverwerking en persoonsgegevens worden verzameld voor specifieke, expliciete en legitieme doeleinden en vervolgens niet op een met deze doeleinden onverenigbare manier verwerkt worden; verdere verwerking voor statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd. Overeenkomstig artikel 89, lid 1, van voornoemde verordening is de verwerking voor statistische doeleinden onderworpen aan passende waarborgen voor de rechten en vrijheden van de betrokkene.

Voor de technische en organisatorische maatregelen wordt in overweging 163 van de AVG verwezen naar Verordening (EG) nr. 223/2009 van het Europees

Ce règlement encadre la production et le développement des statistiques européennes et garantit l'indépendance professionnelle des instituts nationaux de statistiques. Ce règlement instaure également le principe du secret statistique selon lequel les données confidentielles relatives à des unités statistiques individuelles qui sont obtenues directement à des fins statistiques ou indirectement à partir de sources administratives ou autres doivent être protégées.

Dans le cadre de ses missions conférées par la loi du 4 juillet 1962 relative à la statistique publique et du règlement (CE) 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes, la Direction générale Statistique – Statistics Belgium (Statbel) du SPF Économie, PME, Classes Moyennes et Énergie, qui tombe sous la catégorie visée à l'article 127, § 2, alinéa 1er, 9°, doit traiter des données pertinentes et à jour. Par ailleurs, la Direction générale Statistique – Statistics Belgium du SPF Économie, PME, Classes Moyennes et Énergie doit respecter le principe "only once"; à cet égard, les données anonymes ou pseudonymisées ne suffisent pas toujours. Le traitement de données nécessaire à l'établissement des statistiques rend nécessaire un "couplage" c'est à dire le croisement, la mise en relation de données pertinentes provenant de différentes sources.

En vue de répondre aux exigences de qualité définies par Eurostat, Statbel doit être en mesure de disposer de données avec identifiant direct. Ces données sont nécessaires en vue de l'établissement de statistiques relatives à l'utilisation des télécommunications par les ménages et les entreprises. À cet égard, Statbel procède à des opérations de couplage mettant en relation ses propres données avec les données reçues dans le cadre de cette loi conformément à l'article 3, alinéa 2, de l'arrêté royal du 13 juin 2014 déterminant d'une part, les mesures réglementaires, administratives, techniques et organisationnelles spécifiques afin d'assurer le respect des prescriptions relatives à la protection des données à caractère personnel ou relatives à des entités individuelles et de secret statistique et d'autre part, fixant les conditions auxquelles l'Institut national de Statistique peut agir en qualité d'organisation intermédiaire en vue d'un traitement ultérieur à des fins statistiques.

Concrètement, Statbel doit pouvoir disposer de l'adresse où une connexion internet est établie ainsi que l'identité de la personne au nom de laquelle le raccordement est effectué (numéro de registre national et nom). Ces informations sont nécessaires afin de faire le lien entre les résidents d'une habitation ou l'entreprise qui ont participé à l'enquête sur l'utilisation des TIC auprès

Parlement en de Raad van toepassing. Deze verordening biedt een kader voor de productie en ontwikkeling van Europese statistieken en waarborgt de professionele onafhankelijkheid van de nationale statistische instellingen. Deze verordening introduceert ook het beginsel van het statistisch geheim, waarbij vertrouwelijke gegevens met betrekking tot individuele statistische eenheden die rechtstreeks voor statistische doeleinden werden ingezameld of indirect uit administratieve of andere bronnen worden verkregen, moeten worden beschermd.

In het kader van de opdrachten die haar zijn toevertrouwd door de wet van 4 juli 1962 betreffende de officiële statistieken en door Verordening (EG) nr. 223/2009 van het Europees Parlement en de Raad van 11 maart 2009 betreffende de Europese statistiek, moet de Algemene Directie Statistiek – Statistiek België (Statbel) van de FOD Economie, K.M.O., Middenstand en Energie, die onder de categorie valt bedoeld in artikel 127, § 2, eerste lid, 9°, relevante en actuele gegevens verwerken. Bovendien moet de Algemene Directie Statistiek – Statistiek België (Statbel) van de FOD Economie, K.M.O., Middenstand en Energie het "only once"-beginsel respecteren; in dit opzicht volstaan anonieme of gepseudonimiseerde gegevens niet altijd. De gegevensverwerking die nodig is voor de opstelling van statistieken vereist een "koppeling", d.w.z. de kruising en koppeling van relevante gegevens uit verschillende bronnen.

Om aan de door Statbel gedefinieerde kwaliteitseisen te kunnen voldoen, moet Statbel over gegevens met directe identificatoren kunnen beschikken. Deze gegevens zijn nodig voor de opstelling van statistieken over het gebruik van telecommunicatie door huishoudens en bedrijven. In dit verband voert Statbel koppelingen uit waarbij de eigen gegevens worden gekoppeld aan de gegevens die op grond van deze wet zijn ontvangen, overeenkomstig artikel 3, lid 2, van het koninklijk besluit van 13 juni 2014 tot vaststelling van, enerzijds, de specifieke reglementaire, administratieve, technische en organisatorische maatregelen om de naleving te waarborgen van de vereisten inzake de bescherming van de persoonsgegevens of van de gegevens betreffende individuele entiteiten en van de statistische vertrouwelijkheid, en anderzijds, tot vaststelling van de voorwaarden waaronder Nationaal Instituut voor Statistiek kan optreden als intermediaire organisatie met het oog op de verdere verwerking voor statistische doeleinden.

Concreet moet Statbel beschikken over het adres waar een internetaansluiting aanwezig is en de identiteit van de persoon in wiens naam de aansluiting tot stand komt (rijksregisternummer en naam). Deze informatie is nodig om het verband te kunnen leggen tussen de bewoners van een woning of het bedrijf dat heeft deelgenomen aan de ICT-enquête onder huishoudens en bedrijven. Deze

des ménages et auprès des entreprises. Ces enquêtes trouvent leur fondement légal respectivement dans le règlement (UE) 2019/1700 du Parlement européen et du Conseil du 10 octobre 2019 établissant un cadre commun pour des statistiques européennes relatives aux personnes et aux ménages fondées sur des données au niveau individuel collectées à partir d'échantillons, modifiant les règlements (CE) no 808/2004, (CE) no 452/2008 et (CE) no 1338/2008 du Parlement européen et du Conseil, et abrogeant le règlement (CE) no 1177/2003 du Parlement européen et du Conseil et le règlement (CE) no 577/98 du Conseil et dans le règlement (UE) 2019/2152 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux statistiques européennes d'entreprises, abrogeant dix actes juridiques dans le domaine des statistiques d'entreprises. Afin d'évaluer et d'améliorer la représentativité de l'échantillon réalisé, il faut des données de l'ensemble de la population et pas seulement des ménages ou des entreprises ayant participé à l'enquête.

En outre, toujours conformément aux règlements européens précités, Statbel doit disposer de données relatives à la capacité en termes de vitesse de la connexion ainsi que le type d'abonnement en termes de vitesse de connexion. S'agissant du coût pour les personnes concernées, Statbel doit également recevoir des données relatives au montant payé pour les services de télécommunications, ventilé par services. Enfin, l'identité de la personne à qui la facture est adressée (numéro de registre national, nom et adresse) sont également nécessaires en vue de faire le lien avec les dépenses de la famille. Ces données sont nécessaires à la réalisation du volet "consommation" des statistiques relatives aux personnes et aux ménages conformément au règlement (UE) 2019/1700 précité.

L'obtention de ces données avec identifiant direct n'a pas d'incidence sur l'obtention de données d'autres données sous un format agrégé nécessaires à la réalisation d'autres statistiques.

S'agissant de la protection des données, les agents de Statbel sont soumis au secret statistique. Cela signifie, aux termes de l'article 1er ter de la loi du 4 juillet 1962 précitée que les données relatives à des unités statistiques individuelles qui sont obtenues directement à des fins statistiques ou indirectement à partir de sources administratives ou autres sont protégées contre toute violation du droit à la confidentialité. Cela implique que toute utilisation non statistique des données obtenues et toute divulgation illicite sont interdites. Par ailleurs, l'arrêté royal du 13 juin 2014 précité, impose à Statbel le respect de mesures techniques et organisationnelles destinées à protéger les données. Enfin, le règlement (UE) 2016/679 du Parlement européen et du Conseil

enquêtes hebben hun rechtsgrondslag respectievelijk in Verordening (EU) 2019/1700 van het Europees Parlement en de Raad van 10 oktober 2019 tot vaststelling van een gemeenschappelijk kader voor Europese statistieken over personen en huishoudens op basis van bij steekproeven verzamelde gegevens op individueel niveau en tot wijziging van Verordening (EG) nr. 808/2004, (EG) nr. 452/2008 en (EG) nr. 1338/2008 van het Europees Parlement en de Raad en tot intrekking van Verordening (EG) nr. 1177/2003 van het Europees Parlement en de Raad en Verordening (EG) nr. 577/98 van de Raad, en in Verordening (EU) 2019/2152 van het Europees Parlement en de Raad van 27 november 2019 betreffende Europese bedrijfsstatistieken, tot intrekking van tien rechtshandelingen op het gebied van bedrijfsstatistieken. Om de representativiteit van de uitgevoerde steekproef te beoordelen en te verbeteren, zijn gegevens nodig van de gehele bevolking en niet alleen van de huishoudens of ondernemingen die aan de enquête hebben deelgenomen.

Bovendien moet Statbel, steeds conform de Europese reglementering, beschikken over gegevens over de capaciteit in termen van verbindingssnelheid, alsmede over het soort abonnement in termen van verbindingssnelheid.Wat de uitgaven door de betrokken personen betreft, dient Statbel ook de gegevens met betrekking tot het betaald bedrag voor telecomdiensten, uitgesplitst per dienst, te ontvangen. De identiteit van de persoon aan wie de factuur geadresseerd is (rijksregisternummer, naam en adres) zijn nodig om de link met de uitgaven van het huishouden te kunnen maken. Deze gegevens zijn noodzakelijk voor de realisatie van het onderdeel "consumptie" van de statistieken met betrekking tot personen en huishoudens conform het genoemde reglement (EU) 2019/1700.

De verwerving van de gegevens met directie identificatie heeft geen impact op de verwerving van andere gegevens in geaggregeerde vorm die noodzakelijk zijn voor de realisatie van andere statistieken.

Met betrekking tot de bescherming van gegevens zijn de personeelsleden van Statbel onderworpen aan statistische geheimhouding. Dit betekent, in termen van artikel 1 ter van de eerder vernoemde wet van 4 juli 1962, dat de gegevens die verband houden met afzonderlijke statistische eenheden en rechtstreeks voor statistische doeleinden zijn verzameld of onrechtstreeks aan administratieve of andere bronnen zijn ontleend, worden beschermd tegen iedere schending van het recht op geheimhouding. Dat impliceert dat elk niet-statistisch gebruik van de verworven gegevens en elke onwettige openbaarmaking is verboden. Bovendien verplicht het voornoemde Koninklijk Besluit van 13 juni 2014 Statbel technische en organisatorische maatregelen te nemen

du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation (règlement général sur la protection des données) garantit la réutilisation des données à des fins statistiques en son article 5, § 1er, b).

Outre la production de statistiques, la Direction générale Statistique – Statistics Belgium (Statbel) a également pour mission de mettre à disposition d'administrations publiques fédérales, fédérées et locales, ainsi qu'aux personnes physiques et morales poursuivant un but de recherche scientifique, des données d'études pseudonymisées en vertu de l'article 15 de la loi du 4 juillet 1962 relative à la statistique publique. Ces transmissions de données sont encadrées par un contrat de confidentialité, qui prévoit une série d'obligations à charge du destinataire de données en vue de garantir la protection et la confidentialité des données. Par ailleurs, la transmission de données confidentielles est également prévue entre autorités statistiques, en vertu de l'article 15*ter* de la loi du 4 juillet 1962, précitée.

Infractions relevant de plusieurs catégories

Il est possible qu'une même infraction relève de plusieurs catégories. Ainsi, une infraction commise en ligne peut également relever de la criminalité grave. Dans ce cas, il va de soi que la fourniture aux autorités judiciaires de données conservées en relation avec l'infraction sera d'autant plus facile à justifier.

Paragraphe 3

Dans son arrêt La Quadrature du Net, la CJUE considère qu'est permise une législation nationale "prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire." (c'est nous qui soulignons).

Il faut d'abord souligner que la conservation par un opérateur d'une liste d'adresses IP à la source de la connexion n'a pas d'utilité en pratique pour les autorités. Pour que la conservation de ce type de données soit utile, il est nécessaire que l'opérateur conserve ces adresses IP à la source de la connexion en lien avec d'autres données: les adresses IP doivent pouvoir être reliées aux équipements auxquels ces adresses IP ont

ter bescherming van de gegevens. Tot slot waarborgt Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming) in artikel 5, lid 1, onder b), ervan het hergebruik van gegevens voor statistische doeleinden.

Naast de productie van statistieken heeft de Algemene Directie Statistiek – Statistics Belgium (Statbel), krachtens artikel 15 van de wet van 4 juli 1962 betreffende de openbare statistiek, de opdracht gepseudonimiseerde studiegegevens beschikbaar te stellen aan openbare besturen van federaal, deelstaat- en lokaal niveau, alsmede aan natuurlijke en rechtspersonen die een wetenschappelijk onderzoeksdoel nastreven. Het verzenden (of doorgeven) van de gegevens is onderworpen aan een vertrouwelijkheidsovereenkomst, die een serie van verplichten voorziet ten aanzien van de ontvanger van de gegevens ten einde de bescherming en de vertrouwelijkheid van de gegevens te beschermen. Daarnaast is het uitwisselen van vertrouwelijk gegevens tussen statistische instanties voorzien krachtens het artikel 15*ter* van de eerder vernoemde wet van 4 juli 1962.

Inbreuken die onder verschillende categorieën vallen

Het is mogelijk dat eenzelfde inbreuk onder verschillende categorieën valt. Zo kan een online gepleegde inbreuk ook onder zware criminaliteit vallen. In dat geval spreekt het voor zich dat de verstrekking aan de gerechtelijke autoriteiten van bewaarde gegevens in verband met de inbreuk, gemakkelijker te rechtvaardigen zal zijn.

Paragraaf 3

In zijn arrest-*La Quadrature du Net*, oordeelt het HvJ-EU dat het toegestaan is dat een nationale wet, "ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorziet in een algemene en ongedifferentieerde bewaring van de IP-adressen die toegewezen zijn aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk." (Wij onderlijnen).

In de eerste plaats dient te worden benadrukt dat de bewaring door een operator van een lijst met IP-bronadressen van de verbinding, geen praktisch nut heeft voor de autoriteiten. Opdat de bewaring van dit soort van gegevens nuttig zou zijn, is het nodig dat de operator deze IP-bronadressen van de verbinding bewaart, gelinkt aan andere gegevens: de IP-adressen moeten kunnen worden gelinkt aan de apparatuur waaraan deze

été attribuées et ces équipements doivent pouvoir être reliés à l'identité civile des propriétaires de ces équipements. C'est ce qui explique que dans le point 152 de son arrêt La Quadrature du Net, la CJUE a indiqué que "les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée."

Ensuite, la pratique montre que la conservation de l'adresse IP à la source de la connexion est indispensable dans le cadre de la poursuite de la criminalité ordinaire ou d'infraction commise en ligne. Ceci peut être illustré à l'aide des exemples suivants:

lorsqu'une autorité communique à un opérateur une adresse IP à la source de la connexion (obtenue par exemple d'une plateforme de marché en ligne où une infraction a été constatée) en vue d'obtenir l'identité de l'appareil auquel cette adresse IP a été attribuée et ainsi identifier l'auteur de l'infraction, l'opérateur ne pourra pas fournir l'identité de cet appareil s'il n'a pas conservé les adresses IP à la source de la connexion en lien avec ces appareils en vue de permettre cette identification (finalité de conservation);

un autre exemple est l'identification d'une partie à la communication à la demande du service de médiation pour les télécommunications ou des autorités judiciaires (par exemple qui est le rédacteur d'un message déterminé). Dans ce cas, il est parfois nécessaire de retrouver d'abord l'identifiant qui a servi à la communication (par exemple le numéro de téléphone ou l'adresse IP du rédacteur du message), afin d'identifier ensuite la machine et finalement la personne derrière cet identifiant. Cette opération d'identification n'est pas possible si l'opérateur ne conserve pas l'adresse IP à la source de la connexion dans ce but d'identification (finalité de conservation).

Dans les deux exemples précités et pour ce qui concerne la fourniture à une autorité de données, ce sont les règles relatives à l'identité civile qui doivent être appliquées (fourniture de données possible dans le cadre de la criminalité ordinaire), puisque ce que cherche à connaître l'autorité est l'identité civile d'une personne déterminée (la personne "derrière" l'adresse IP).

Dans le point 154 de son arrêt La Quadrature du Net, la CJUE reconnait elle-même que "dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer

IP-adressen werden toegewezen en deze apparatuur moet kunnen worden gelinkt aan de burgerlijke identiteit van de eigenaars van deze apparatuur. Dat verklaart waarom in punt 152 van zijn arrest-*La Quadrature du Net* het HvJ-EU aangeeft: "Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronische-communicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd."

De praktijk wijst verder uit dat de bewaring van het IP-bronadres van de verbinding onontbeerlijk is in het kader van de vervolging van gewone criminaliteit of online gepleegde inbreuken. Dat kan worden geïllustreerd met de volgende voorbeelden:

wanneer een autoriteit aan een operator een IP-bronadres van de verbinding meedeelt (bijvoorbeeld verkregen via een online verkoopplatform waarop een inbreuk werd vastgesteld) om de identiteit te krijgen van het toestel waaraan dat IP-adres is toegewezen en dus de dader van de inbreuk te identificeren, dan mag de operator de identiteit van dat toestel niet verstrekken als hij de IP-bronadressen van de verbinding gelinkt aan deze apparatuur niet heeft bewaard met het oog op deze identificatie (doeleinde van bewaring);

een ander voorbeeld is de identificatie van een deel van de communicatie op verzoek van de Ombudsdienst voor telecommunicatie of van de gerechtelijke autoriteiten (bijvoorbeeld wie heeft een bepaald bericht opgesteld). In dat geval is het soms noodzakelijk om eerst de identifier te vinden die voor de communicatie gediend heeft (bijvoorbeeld het telefoonnummer of IP-adres van de opsteller van het bericht) om daarna het toestel en uiteindelijk de persoon achter die identifier te identificeren. Deze identificatie is niet mogelijk indien de operator het IP-bronadres van de verbinding niet bewaart met het oog op identificatie (doeleinde van de bewaring).

In de twee voormelde voorbeelden en wat betreft de verstrekking aan een autoriteit van gegevens, zijn het de regels in verband met de burgerlijke identiteit die moeten worden gehanteerd (gegevensverstrekking mogelijk in het kader van de gewone criminaliteit) aangezien datgene dat de autoriteit wenst te achterhalen, de burgerlijke identiteit is van een bepaalde persoon (de persoon "achter" het IP-adres).

In punt 154 van zijn arrest-*La Quadrature du Net*, erkent het HvJ-EU zelf "dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel

le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction."

Par conséquent, priver les autorités chargées de la poursuite d'une infraction en ligne de toute exploitation de l'adresse IP à la source de la connexion, lorsque l'infraction ne relève pas de la criminalité grave, reviendrait *de facto* à rendre impossible la poursuite des infractions en ligne qui ne relèvent pas de la criminalité grave. Le législateur n'envisage donc pas qu'une telle solution doive être retenue à la lecture de l'arrêt La Quadrature du Net de la CJUE.

Par ailleurs, en cas d'incident de sécurité sur un réseau, il peut être nécessaire que le CCB ou l'IBPT prenne connaissance de l'adresse IP à l'origine de l'incident ou des adresses IP touchées par l'incident, de manière à pouvoir y remédier, dans les limites de leurs compétences respectives. De même, le législateur ne considère pas que l'arrêt La Quadrature du Net doive être considéré comme portant atteinte à la faculté de ces autorités de remplir leurs missions en obtenant, si besoin, des adresses IP à la source de la communication. En effet, les finalités poursuivies par ces autorités ne font pas partie de celles qui ont été examinées par la CJUE à ce jour.

Le législateur estime qu'il respecte l'objectif poursuivi par l'arrêt La Quadrature du Net de la CJUE. En effet, la CJUE a jugé dans cet arrêt (point 153) ce qui suit: "les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier". Dans ce passage de l'arrêt, la CJUE vise les adresses IP de manière générale. Il convient cependant de rappeler qu'en vertu de l'article 126 de la loi télécom et conformément à la jurisprudence de la CJUE, les opérateurs ne doivent conserver de manière généralisée et indifférenciée que les seules adresses IP à la source de la connexion et que cet article 126 prévoit qu'il ne porte pas sur l'adresse IP du destinataire de la communication. Or, l'exploitation de seules adresses IP à la source de la connexion ne permet pas le traçage exhaustif du parcours de navigation d'un internaute.

Il ressort du même arrêt que ce traçage n'est permis que dans le cadre de la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale (point 156).

kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd."

De autoriteiten belast met de vervolging van een online gepleegde inbreuk elk gebruik van het IP-bronadres van de verbinding ontzeggen, wanneer de inbreuk niet onder de zware criminaliteit valt, zou *de facto* inhouden dat het onmogelijk is om online gepleegde inbreuken te vervolgen die niet onder de zware criminaliteit vallen. De wetgever vindt dus niet dat een dergelijke oplossing in aanmerking mag komen bij het lezen van het arrest-*La Quadrature du Net* van het HvJ-EU.

In geval van een veiligheidsincident op een netwerk kan het bovendien noodzakelijk zijn dat het CCB of het BIPT kennis neemt van het IP-adres dat aan de oorsprong ligt van het incident of van de IP-adressen die getroffen zijn door het incident, om het probleem te kunnen verhelpen, binnen de limieten van hun respectieve bevoegdheid. Evenzo vindt de wetgever niet dat het arrest-*La Quadrature du Net* moet worden beschouwd als een aantasting van de mogelijkheid van deze autoriteiten om hun opdrachten te vervullen, desnoods door aan de bron van de communicatie toegewezen IP-adressen te verkrijgen. De doeleinden die deze autoriteiten nastreven maken immers geen deel uit van die welke tot op heden door het HvJ-EU zijn onderzocht.

De wetgever meent dat hij het door het arrest-*La Quadrature du Net* van het HvJ-EU nagestreefde doel eerbiedigt. Het HvJ-EU heeft in dat arrest (punt 153) evenwel het volgende geoordeeld:"Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld." In dit uittreksel uit het arrest beoogt het HvJ-EU de IP-adressen in het algemeen. Er dient echter aan te worden herinnerd dat krachtens artikel 126 van de telecomwet en conform de rechtspraak van het HvJ-EU, de operatoren enkel de IP-bronadressen van de verbinding op algemene en ongedifferentieerde wijze dienen te bewaren en dat dat artikel 126 bepaalt dat dit geen betrekking heeft op het IP-adres van de geadresseerde van de communicatie. Wanneer enkel de IP-bronadressen van de communicatie worden gebruikt, is het overigens niet mogelijk om de volledige zoekgeschiedenis van een internetgebruiker te traceren.

Uit hetzelfde arrest blijkt dit traceren slechts toegestaan is in het kader van de bestrijding van zware criminaliteit, het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid (punt 156).

Pour respecter cet arrêt de la CJUE, l'article 127/1 prévoit que si l'autorité est en mesure d'effectuer un tel traçage, à l'aide des informations en sa possession et des adresses IP à la source de la connexion obtenues de l'opérateur (il n'est pas certain que cette hypothèse puisse se produire en pratique), la demande adressée à l'opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la protection des intérêts vitaux de personnes physiques. Il reviendra à l'autorité qui demande les données et ensuite à la juridiction ou à l'autorité administrative indépendante qui effectue le contrôle de la demande de données envers l'opérateur de vérifier si la demande permettra d'effectuer un traçage du parcours de navigation d'une personne sur Internet. Lorsqu'une autorité parvient à identifier l'auteur d'une communication (par exemple qui est la personne "derrière" une adresse IP à la source de la connexion), les informations dont a connaissance l'autorité ne se rapportent qu'à une seule communication. Dans ce cas, il ne faut pas considérer que l'autorité est à même d'effectuer un traçage du parcours de navigation de l'internaute.

L'auditeur de la FSMA agit également dans le cadre de la lutte contre la criminalité grave, notamment lorsqu'il enquête sur les abus de marché (voir le commentaire concernant la définition de criminalité grave au § 1er et voir § 2, 6°), et dans ce contexte, il obtient l'adresse IP source, également pour d'autres finalités que l'identification. Pour les autres finalités visées aux articles 81, 82, 2°, et 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ou aux dispositions déclarant ces articles applicables qui ne concernent pas la prévention, la recherche, la détection ou la poursuite de la criminalité grave (voir § 2, 7°), cette adresse IP ne peut être traitée qu'à des fins d'identification.

Paragraphe 4

L'auditeur de la FSMA agit, dans le cadre de ses enquêtes sur les abus de marché, aux fins de la lutte contre la criminalité grave et peut, dans ce contexte, également obtenir des données qui sont conservées par les opérateurs en vertu de l'article 126/1. L'on se reportera à cet égard au commentaire du paragraphe 3 concernant ce point.

Paragraphe 5

Afin d'éviter toute interprétation de la législation organique ou sectorielle sur laquelle une autorité se base pour obtenir les données de l'opérateur, il est essentiel

Om dat arrest van het HvJ-EU in acht te nemen, bepaalt artikel 127/1 dat indien de autoriteit in staat is om een dergelijke tracering uit te voeren aan de hand van de informatie in haar bezit en IP-bronadressen van de verbinding verkregen van de operator (het is niet zeker dat deze hypothese mogelijk is in de praktijk), het verzoek gericht aan de operator om de IP-bronadressen van een verbinding slechts is toegestaan voor de doeleinden van bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventie van ernstige dreigingen voor de openbare veiligheid en de bescherming van de vitale belangen van een fysieke persoon. Het zal aan de autoriteit zijn die de gegevens vraagt en vervolgens aan de rechterlijke instantie of de onafhankelijke administratieve overheid die het verzoek om gegevens gericht aan de operator controleert, om na te gaan of het verzoek het mogelijk zal maken om de zoekgeschiedenis van een persoon op internet te traceren. Wanneer een autoriteit erin slaagt om te achterhalen wie een communicatie heeft uitgevoerd (bijvoorbeeld wie de persoon "achter" een IP-bronadres van de verbinding is), heeft de informatie waar de autoriteit kennis van heeft, enkel betrekking op één communicatie. In dat geval moet niet beschouwd worden dat de autoriteit de zoekgeschiedenis van een internetgebruiker kan traceren.

Ook de auditeur van de FSMA treedt op voor doeleinden van de strijd tegen zware criminaliteit, met name wanneer hij een onderzoek voert naar marktmisbruik (zie de toelichting bij de definitie van zware criminaliteit in § 1 en zie § 2, 6°), en krijgt in dat kader het IP-bronadres, ook voor andere doeleinden dan de identificatie. Voor de andere doeleinden bedoeld in de artikelen 81, 82, 2°, en 84, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten of in de bepalingen die deze artikelen van toepassing verklaren die niet de preventie, het onderzoek, de opsporing of de vervolging van zware criminaliteit betreffen (zie § 2, 7°), mag dat IP-adres enkel voor doeleinden van identificatie worden behandeld.

Paragraaf 4

De auditeur van de FSMA treedt in het kader van zijn onderzoeken naar marktmisbruik op voor doeleinden van de strijd tegen zware criminaliteit en kan in dat kader dan ook gegevens verkrijgen die door de operatoren zijn bewaard krachtens artikel 126/1. Hiervoor kan verwezen worden naar de toelichting bij paragraaf 3 in dit verband.

Paragraaf 5

Om elke interpretatie van de organieke of sectorale wetgeving waarop een autoriteit zich baseert om gegevens te verkrijgen van de operator, te vermijden, is

que cette législation prévoie le pouvoir de l'autorité d'obtenir les données de l'opérateur (ou une expression équivalente, cette notion pouvant être plus large que la notion d'opérateur au sens de la loi télécom) et ne se contente pas de prévoir un pouvoir d'obtenir des données de toute personne. Il est aussi essentiel que cette législation prévoie que l'autorité peut obtenir des données d'identification ou des métadonnées (ou toute expression qui vise à préciser les données à obtenir de l'opérateur) et ne se contente pas de prévoir que l'autorité peut demander toute information utile.

Afin de respecter la jurisprudence de la CJUE, la législation sectorielle ou organique devra aussi prévoir un contrôle interne (validation par un supérieur hiérarchique et/ou avis du préposé à la protection des données à caractère personnel) ou externe (par une juridiction ou une autorité administrative indépendante) de la demande de l'autorité d'obtenir certaines données d'un opérateur.

Pour accroître la transparence envers le citoyen et envers les opérateurs, le ministre (tel que défini à l'article 2, 2°, de la loi télécom) fera publier au *Moniteur belge* une circulaire sur la fourniture aux autorités de données d'identification et de métadonnées conservées par les opérateurs sur la base de la loi télécom. Ne peuvent pas être reprises sur cette circulaire des autorités qui seraient simplement légalement habilitées à demander à des acteurs économiques toute donnée utile.

Il reviendra aux autorités concernées de fournir au ministre les informations à reprendre dans la circulaire. Si nécessaire, le ministre ou l'IBPT pourra demander aux autorités concernées les informations manquantes.

Paragraphe 6

En pratique, pour assurer la confidentialité des demandes des autorités qui sont fournies aux opérateurs, il est possible que le NTSU-CTIF, en tant que service central, soit l'autorité qui adresse à un opérateur la demande formulée par une autre autorité, sans révéler quelle autorité est l'auteur de la demande.

Avant de donner suite à une demande de données qui fait l'objet d'un contrôle interne, il revient à l'opérateur de vérifier l'existence de la base légale nécessaire pour requérir les données. En revanche, que le contrôle soit interne ou externe, il ne revient pas à l'opérateur

het van essentieel belang dat die wetgeving voorziet in de machtiging van de autoriteit om de gegevens te verkrijgen van de operator (of een gelijkwaardige uitdrukking, aangezien dit begrip breder kan zijn dan het begrip van operator in de zin van de telecomwet) en zich niet beperkt tot een machtiging om gegevens te verkrijgen van gelijk welke persoon. Het is ook van essentieel belang dat deze wetgeving voorschrijft dat de autoriteit identificatiegegevens of metagegevens kan verkrijgen (of elke uitdrukking die beoogt de van de operator te verkrijgen gegevens te preciseren) en zich niet beperkt tot het bepalen dat de autoriteit gelijk welke nuttige informatie mag vragen.

Teneinde in overeenstemming te zijn met de rechtspraak van het HvJ-EU, zal de sectorale of organieke wetgeving ook moeten voorzien in een interne controle (validering door een hiërarchische meerdere en/of advies van de aangestelde voor de bescherming van de persoonsgegevens) of een externe controle (door een rechterlijke instantie of een onafhankelijke administratieve overheid) van het verzoek van de autoriteit om bepaalde gegevens te verkrijgen van een operator.

Om meer transparantie te bieden aan de burger en aan de operatoren, zal de minister (zoals bepaald in artikel 2, 2°, van de telecomwet) in het *Belgisch Staatsblad* een omzendbrief laten publiceren over de verstrekking aan de autoriteiten van identificatiegegevens en metagegevens bewaard door de operatoren op grond van de telecomwet. Deze omzendbrief mag geen autoriteiten opnemen die eenvoudigweg wettelijk gemachtigd zouden zijn om van economische spelers gelijk welke nuttige informatie te vragen.

Het zal aan de betrokken autoriteiten zijn om aan de minister de informatie te bezorgen die moet worden opgenomen in de omzendbrief. Indien nodig, zal de minister of het BIPT aan de betrokken autoriteiten de ontbrekende informatie kunnen vragen.

Paragraaf 6

Om praktisch gezien de vertrouwelijkheid van de verzoeken van de autoriteiten aan de operatoren te garanderen, is het mogelijk dat de NTSU-CTIF, als centrale dienst, de autoriteit is die aan een operator het verzoek richt dat geformuleerd is door een andere autoriteit, zonder bekend te maken welke autoriteit het verzoek heeft gedaan.

Alvorens gevolg te geven aan een verzoek om gegevens dat het voorwerp uitmaakt van een interne controle, is het de taak van de operator om na te gaan of de wettelijke basis aanwezig is die nodig is om de gegevens op te vragen. Ongeacht of het gaat om een

de juger de la proportionnalité des demandes de données de cette autorité ni de vérifier si la demande est suffisamment motivée.

Paragraphe 7

Ce paragraphe reprend le contenu de l'ancien article 126, § 5, de la loi télécom (version avant annulation de la loi "conservation de données" par la Cour constitutionnelle).

La communication des statistiques est généralisée à la fourniture aux autorités de l'ensemble des données conservées en vertu des articles 122, 123, 126, 126/1 et 127.

Lors de la consultation publique, plusieurs opérateurs ont proposé de supprimer l'obligation des opérateurs de fournir des statistiques à l'IBPT, ces statistiques pouvant être extraites de l'outil TANK du NTSU-CTIF (outil permettant l'automatisation des demandes vers les opérateurs et des réponses de ces derniers vers les autorités). La suppression de cette obligation n'est pas envisageable à l'heure actuelle: il ne peut être exclu que dans un premier temps certaines statistiques ne puissent pas être extraites de TANK et de nombreuses autorités n'utilisent pas TANK pour demander des données d'identification ou de trafic aux opérateurs. Cependant, le texte de l'article a été adapté pour permettre plus de flexibilité en pratique. Dorénavant, les opérateurs ne devront plus automatiquement envoyer les statistiques à l'IBPT mais uniquement à sa demande. L'IBPT pourra obtenir via la plateforme "TANK" du NTSU-CTIF certaines statistiques et demander les informations manquantes aux opérateurs.

Le Roi ne doit plus définir les statistiques qui doivent être fournies à l'IBPT, étant donné qu'en pratique les statistiques définies dans l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques correspondent aux statistiques déjà décrites dans l'article 127/1, § 7.

Art. 12 (insertion de l'article 127/2)

Introduction

L'article 127/2 porte sur la qualité et la sécurité des données conservées par les opérateurs. Cet article reprend des principes qui se trouvaient auparavant dans l'ancien article 126, § 4, de la loi télécom (article

interne of een externe controle, is het daarentegen niet aan de operator om te oordelen over de evenredigheid van de verzoeken om gegevens van die autoriteit, noch om na te gaan of het verzoek voldoende gemotiveerd is.

Paragraaf 7

Deze paragraaf neemt de inhoud over van het oude artikel 126, § 5, van de telecomwet (versie voorafgaand aan de nietigverklaring van de wet "gegevensbewaring" door het Grondwettelijk Hof).

De mededeling van de statistieken wordt veralgemeend met de verstrekking aan de autoriteiten van het geheel van gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127.

Tijdens de openbare raadpleging hebben verschillende operatoren voorgesteld om de verplichting van de operatoren om aan het BIPT statistieken te verstrekken, te schrappen; deze statistieken kunnen immers worden gehaald uit de tool TANK van de NTSU-CTIF (tool die de automatisering mogelijk maakt van de verzoeken aan de operatoren en van de antwoorden vanwege deze laatste aan de autoriteiten). De opheffing van die verplichting valt momenteel niet te overwegen: er kan niet worden uitgesloten dat in eerste instantie bepaalde statistieken niet uit TANK kunnen worden gehaald en talrijke autoriteiten maken geen gebruik van TANK om identificatie- of verkeersgegevens aan de operatoren te vragen. De tekst van het artikel is evenwel aangepast om in de praktijk meer flexibiliteit mogelijk te maken. Voortaan zullen de operatoren niet meer automatisch de statistieken naar het BIPT moeten opsturen, maar enkel wanneer het dat vraagt. Het BIPT zal via het "TANK"-platform van de NTSU-CTIF bepaalde statistieken kunnen krijgen en de ontbrekende informatie aan de operatoren vragen.

De Koning moet de statistieken die aan het BIPT verstrekt moeten worden, niet meer definiëren, aangezien in de praktijk de statistieken die bepaald zijn in het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie overeenstemmen met de statistieken die reeds beschreven zijn in artikel 127/1, § 7.

Art. 12 (invoeging van artikel 127/2)

Inleiding

Artikel 127/2 heeft betrekking op de kwaliteit en de veiligheid van de gegevens die door de operatoren worden bewaard. Dit artikel neemt principes over die voordien in het oude artikel 126, § 4, van de telecomwet stonden

existant avant l'annulation de la loi "conservation des données" par la Cour constitutionnelle).

Paragraphe 1er

Il est ajouté une obligation complémentaire à charge des opérateurs: celle de garantir la qualité des données conservées en vertu des articles 122, 123, 126, 126/1 et 127. Dès lors que ces données peuvent, sous certaines conditions, être utilisées notamment à des fins de sauvegarde de la sécurité nationale et de lutte contre la criminalité, il est crucial que leur qualité soit incontestable. Dans cet objectif, les opérateurs prennent toutes les mesures adéquates pour garantir en tout temps leur exactitude, leur intégrité et leur fiabilité.

Dans son avis, l'Autorité de protection des données indique qu'il y a un manque de clarté sur la distinction entre données conservées pour les autorités et données conservées pour les propres besoins des opérateurs. En effet, les nouveaux articles 122 et 123 de la loi télécom imposent des obligations de conservation à des fins de lutte contre la fraude (dont peuvent être victimes les opérateurs) et afin d'assurer la sécurité des réseaux (ce qui constitue une obligation à charge des opérateurs). L'avant-projet prévoit, par ailleurs, que les autorités pourront, sous certaines conditions, obtenir un accès à ces données, y compris pour d'autres finalités que pour celles pour lesquelles elles ont initialement été conservées. "Ces données sont-elles dès lors conservées pour les autorités ou pour les besoins propres des opérateurs?" Les données conservées sur la base des articles 122 et 123 le sont pour les propres besoins des opérateurs, et dans certains cas, également pour préserver les intérêts de leurs clients. À titre d'exemple, lorsque l'opérateur conserve des données de trafic pour se prémunir de fraudes dont il est victime, cette conservation de données est faite pour ses propres besoins. Par contre, lorsque l'opérateur conserve des données de trafic pour protéger ses abonnés de fraudes commises par un tiers, cette conservation est faite dans l'intérêt des abonnés mais également dans l'intérêt de l'opérateur. En effet, dans ce cas de figure, l'opérateur a un intérêt à éviter à ce qu'un nombre important de ses abonnés soient victimes d'une fraude, afin d'éviter une perte d'attrait du service de communications électroniques qu'il offre.

Il revient aux opérateurs de décider comment ils s'organisent pour la conservation des données au bénéfice des autorités (en particulier les données conservées conformément aux articles 126, 126/1, 127). Dès lors, si une même donnée est visée dans plusieurs articles, ils peuvent conserver la donnée une seule fois. Par contre,

(artikel dat bestond voor de nietigverklaring van de wet "gegevensbewaring" door het Grondwettelijk Hof).

Paragraaf 1

Er wordt een bijkomende verplichting toegevoegd voor de operatoren: deze om de kwaliteit van de gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127, te garanderen. Aangezien deze gegevens, onder bepaalde voorwaarden, kunnen worden gebruikt met name voor doeleinden van vrijwaring van de nationale veiligheid en strijd tegen de criminaliteit, is het onontbeerlijk dat ze van onomstotelijke kwaliteit zijn. Daartoe treffen de operatoren alle gepaste maatregelen om te allen tijde de juistheid, integriteit en betrouwbaarheid ervan te garanderen.

In haar advies zegt de Gegevensbeschermingsautoriteit: "[het] ontbreekt […] aan duidelijkheid over het onderscheid tussen gegevens die de operatoren bewaren ten behoeve van de autoriteiten en de gegevens die ze bewaren voor hun eigen behoeften. De nieuwe artikelen 122 en 123 van de telecomwet leggen immers verplichtingen op tot bewaring met het oog op het bestrijden van fraude (waarvan de operatoren het slachtoffer kunnen zijn) en met het oog op de veiligheid van de netwerken (wat een verplichting is in hoofde van de operatoren). Bovendien voorziet het voorontwerp dat de autoriteiten onder bepaalde voorwaarden toegang kunnen krijgen tot die gegevens, ook voor andere doeleinden dan deze waarvoor ze oorspronkelijk werden bewaard". Worden die gegevens dan bewaard ten behoeve van de autoriteiten of voor de eigen behoeften van de operatoren?" De gegevens die worden bewaard op basis van de artikelen 122 en 123 worden bewaard voor de eigen behoeften van de operatoren en in sommige gevallen ook om de belangen van hun klanten te vrijwaren. Wanneer de operator bijvoorbeeld verkeersgegevens bewaart om zich te wapenen tegen fraude waarvan hij het slachtoffer is, dan dient die gegevensbewaring voor de eigen behoeften. Bewaart de operator daarentegen verkeersgegevens om zijn abonnees te beschermen tegen fraude gepleegd door een derde, dan is die bewaring in het belang van de abonnees maar ook in het belang van de operator. In dat geval heeft de operator er immers belang bij dat vermeden wordt dat een groot aantal van zijn abonnees slachtoffer worden van fraude, om te vermijden dat de elektronische-communicatiedienst die hij aanbiedt, zijn aantrekkingskracht verliest.

Het is aan de operatoren om te beslissen hoe ze zich organiseren voor de bewaring van de gegevens ten behoeve van de autoriteiten (in het bijzonder de gegevens bewaard conform de artikelen 126, 126/1, 127). Wanneer eenzelfde gegeven wordt bedoeld in verscheidene artikelen, mogen ze dat gegeven dus één keer bewaren.

les opérateurs doivent tout mettre en œuvre pour établir les liens entre les données conservées pour les autorités qui sont nécessaire pour répondre aux demandes des autorités (soit la pratique montre qu'un tel lien est nécessaire pour répondre à un type de demandes des autorités, ou un tel lien est nécessaire pour répondre à une demande spécifique d'une autorité). Cela ne signifie pas que les opérateurs doivent prendre à leur charge certaines tâches normalement dévolues à la police ou aux autorités judiciaires. Ceci est nécessaire vu que pour répondre à une demande d'une autorité, un opérateur pourrait être amené à consulter des données conservées sur la base de différents articles.

Dans son avis, l'Autorité de protection des données souligne "que si le législateur entend permettre aux autorités de réaliser des recherches sur des personnes concernées à partir des différentes données conservées par les opérateurs, il lui reviendrait de déterminer, dans le respect du principe de proportionnalité, les critères de recherche qui pourraient être utilisés par les autorités compétentes pour faire leurs recherches et établir les liens." Le législateur ne perçoit pas comment ce point de l'avis pourrait être mis en œuvre, dès lors que cela supposerait vraisemblablement d'établir une liste exhaustive de tous les types de requêtes susceptibles d'être faites par toute autorité habilitée à effectuer une demande d'accès. Ceci est impossible à mettre en œuvre au vu du caractère évolutif des besoins des autorités et des données conservées par les opérateurs. En revanche, cette demande devra toujours être justifiée et proportionnée. Par ailleurs, la disposition critiquée par l'Autorité de protection des données ne permet pas à une autorité d'avoir accès à plus de données que les données auxquelles elle peut accéder.

Dans le passé, les opérateurs devaient conserver les données de trafic sur la base de l'article 126 de la loi télécom. À la suite de la jurisprudence de la CJUE, la loi télécom a été revue et les opérateurs doivent dorénavant conserver des données pour les autorités en vertu de différentes bases légales (articles 126 et 126/1 de la loi télécom et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité pour ce qui concerne la conservation généralisée et indifférenciée de métadonnées de communications électroniques en cas de menace grave pour la sécurité nationale). Le fait que les opérateurs conservent dorénavant des données en vertu de différentes bases légales ne peut pas avoir comme conséquence un cloisonnement des données, sans que les opérateurs ne puissent faire de lien entre elles.

De operatoren moeten daarentegen alles in het werk stellen om de verbanden te leggen tussen de gegevens die bewaard worden voor de autoriteiten, die nodig zijn om te antwoorden op de vragen van de autoriteiten (ofwel toont de praktijk aan dat een dergelijk verband noodzakelijk is om te antwoorden op een type van vragen van de autoriteiten, ofwel is een dergelijk verband noodzakelijk om te antwoorden op een specifieke vraag van een autoriteit). Dat betekent niet dat de operatoren bepaalde taken die normaal gezien toebedeeld zijn aan de politie of aan de gerechtelijke autoriteiten, op zich moeten nemen. Dit is nodig aangezien een operator, om te antwoorden op een verzoek van een autoriteit, genoopt zou kunnen zijn om gegevens te raadplegen die zijn bewaard op basis van verschillende artikelen.

In haar advies benadrukt de Gegevensbeschermingsautoriteit: "als de wetgever de autoriteiten wil toelaten om op basis van de verschillende gegevens die worden bewaard door de operatoren onderzoek te doen naar de betrokken personen, [moet] hij – overeenkomstig het evenredigheidsbeginsel – de zoekcriteria […] bepalen aan de hand waarvan de bevoegde autoriteiten hun onderzoek kunnen verrichten en de verbanden kunnen leggen." De wetgever ziet niet in hoe dit punt van het advies uitgevoerd zou kunnen worden, omdat dit nu eenmaal waarschijnlijk zou veronderstellen dat een volledige lijst wordt opgesteld van alle soorten van verzoeken die kunnen worden gedaan door alle autoriteiten die bevoegd zijn verklaard om een verzoek om toegang te doen. Dat is onmogelijk toe te passen gelet op de evolutieve aard van de behoeften van de autoriteiten en van de gegevens die worden bewaard door de operatoren. Dit verzoek zal daarentegen steeds gerechtvaardigd en evenredig moeten zijn. Bovendien maakt de door de Gegevensbeschermingsautoriteit bekritiseerde bepaling het voor een autoriteit niet mogelijk om meer gegevens in te zien dan de gegevens waartoe zij toegang mag hebben.

Vroeger moesten de operatoren de verkeersgegevens bewaren op basis van artikel 126 van de telecomwet. Na de rechtspraak van het HvJ-EU is de telecomwet herzien en moeten de operatoren voortaan gegevens voor de autoriteiten bewaren krachtens verschillende wettelijke grondslagen (de artikelen 126 en 126/1 van de telecomwet en de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten wat betreft de algemene en ongedifferentieerde bewaring van elektronische-communicatiemetagegevens in geval van ernstige bedreiging voor de nationale veiligheid). Het feit dat de operatoren voortaan gegevens bewaren krachtens verschillende wettelijke grondslagen mag niet tot gevolg hebben dat de gegevens worden versnipperd, zonder dat de operatoren daartussen een verband kunnen leggen.

Paragraphe 2

Le paragraphe 2, alinéa 1er, reprend des mesures de protection des données conservées par les opérateurs pour les autorités.

Un opérateur ne peut pas utiliser pour ses propres besoins les données qu'ils conservent pour les autorités. Bien entendu, un opérateur peut conserver une même donnée pour plusieurs finalités (pour ses propres besoins et pour les autorités).

Paragraphe 3

Le paragraphe 3 reprend des mesures de protection des données conservées par les opérateurs et auxquelles les autorités pourraient demander accès.

L'exigence que les données conservées sur la base de la loi belge (la loi télécom, le Code d'instruction criminelle, par exemple le *quick freeze* ou la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, par exemple les métadonnées de communications électroniques conservées en cas de menace grave pour la sécurité nationale) qui sont demandées par une autorité belge lui soient communiquées en Belgique ne signifie pas que les données doivent être conservées sur le territoire de la Belgique. En effet, ces données doivent être conservées sur le territoire de l'Union européenne. Cela signifie par contre que les opérateurs doivent communiquer à l'autorité belge en Belgique les données demandées, sans que cette autorité ne doive aller les chercher à l'étranger, ni passer par une commission rogatoire. Les autorités belges légalement autorisées doivent donc être en mesure d'obtenir ces données en tout temps, quel que soit le lieu où ces données sont conservées ou quel que soit le lieu où se trouve le siège social de l'opérateur. Un opérateur qui offre en Belgique des services de communications électroniques est en effet soumis à la présente loi.

Lorsque le délai de conservation d'une donnée est atteint, l'opérateur supprime la donnée ou la rend anonyme. Ce principe est mis en œuvre dans les articles 122 et 123 de la loi. Bien entendu, l'opérateur ne pourra pas supprimer la donnée ou la rendre anonyme s'il a reçu une injonction d'une autorité de prolonger la durée de conservation de la donnée (conservation rapide des données ou "*quick freeze*").

La demande à la Cellule de coordination ainsi que la réponse de cette dernière peuvent avoir lieu de manière automatisée.

Paragraaf 2

Paragraaf 2, eerste lid, vermeldt maatregelen ter bescherming van de door de operatoren voor de autoriteiten bewaarde gegevens.

Een operator mag de gegevens die hij bewaart voor de autoriteiten, niet voor zijn eigen behoeften gebruiken. Een operator kan eenzelfde gegeven uiteraard voor verscheidene doeleinden bewaren (voor zijn eigen behoeften en voor de autoriteiten).

Paragraaf 3

Paragraaf 3 vermeldt maatregelen ter bescherming van de door de operatoren bewaarde gegevens waartoe de autoriteiten toegang zouden kunnen vragen.

De eis dat de gegevens bewaard op basis van de Belgische wet (de telecomwet, het Wetboek van Strafvordering, bijvoorbeeld de *quick freeze* of de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, bijvoorbeeld de elektronische-communicatiemetagegevens die bewaard worden in geval van ernstige bedreiging voor de nationale veiligheid) die gevraagd worden door een Belgische autoriteit, eraan worden meegedeeld in België, betekent niet dat de gegevens bewaard moeten worden op Belgisch grondgebied. Deze gegevens moeten namelijk bewaard worden op het grondgebied van de Europese Unie. Dat betekent daarentegen dat de operatoren aan de Belgische autoriteit in België de gevraagde gegevens moeten meedelen, zonder dat deze autoriteit die moet gaan halen in het buitenland, noch via een rogatoire commissie moet passeren. De wettelijk gemachtigde Belgische autoriteiten moeten dus in staat zijn om die gegevens te allen tijde te krijgen, ongeacht de plaats waar die gegevens worden bewaard of ongeacht de plaats waar de hoofdzetel van de operator gelegen is. Een operator die in België elektronische-communicatiediensten aanbiedt is immers aan de onderhavige wet onderworpen.

Wanneer de bewaringstermijn van een gegeven bereikt is, verwijdert de operator het gegeven of maakt hij het anoniem. Dat principe wordt ten uitvoer gebracht in de artikelen 122 en 123 van de wet. De operator zal het gegeven natuurlijk niet mogen schrappen of anoniem maken wanneer hij een bevel heeft gekregen van een overheid om de bewaringstermijn van het gegeven te verlengen (snelle bewaring van de gegevens of "*quick freeze*").

Het verzoek aan de Coördinatiecel alsook het antwoord van deze laatste, kan automatisch verlopen.

Paragraphe 4

Ce journal porte sur les demandes des différentes autorités en matière de données d'identification et de métadonnées de communications électroniques.

L'obligation d'enregistrement ("log") automatisé dans le journal de chaque accès aux données conservées par l'opérateur pour les autorités a pour objectif d'éviter qu'il ne soit possible d'accéder à ces données sans trace de cet accès dans le journal. De la sorte, un accès non autorisé (abus) aux données pourra être retrouvé grâce au journal.

Une distinction est faite entre l'accès aux données conservées par l'opérateur aux fins des autorités et l'accès aux données qu'il conserve pour ses propres fins ou dans l'intérêt de ses abonnés, car pour ce qui concerne la deuxième catégorie d'accès, différentes équipes de l'opérateur (par exemple son équipe facturation ou anti-fraude), et pas uniquement sa Cellule de coordination, doivent pouvoir accéder à ces données. Pour assurer des règles proportionnées, l'obligation d'enregistrement de l'accès aux données conservées par l'opérateur pour ses propres fins ou dans l'intérêt de ses abonnés ne vaut que pour sa Cellule de coordination.

L'objectif du journal est de permettre de vérifier si l'accès à une donnée conservée était bien justifié par une demande d'une autorité et, si ce n'est pas le cas, de retrouver la personne qui a accédé aux données.

Il ressort des contributions à la consultation publique sur l'avant-projet de loi que l'automatisation de l'enregistrement ("log") de l'accès d'un membre de la Cellule de coordination aux données conservées (identité de cette personne et moment de l'accès) pour répondre à une demande d'une autorité n'est pas une mesure complexe à mettre en place, ce type de "log" étant d'ores-et-déjà largement généralisé. En revanche, l'enregistrement automatisé des autres données prévues par l'article 127/2, § 4, n'est actuellement pas prévu et supposerait un investissement qui pourrait s'avérer démesuré au regard des demandes effectivement reçues par certains opérateurs. En conséquence, il est prévu que ces données peuvent être introduites de manière manuelle dans le journal. Cela ne portera pas préjudice à la valeur du journal, vu que les données qui permettent de retracer une consultation de données conservées seront quant à elles bien enregistrées de manière automatique dans le journal. Le cas échéant, les opérateurs pourront aussi reprendre dans le journal les informations nécessaires pour retrouver la demande dans le système "Tank" du

Paragraaf 4

Dit logboek heeft betrekking op de aanvragen van de verschillende autoriteiten inzake de identificatiegegevens en de elektronische-communicatiemetagegevens.

De verplichting tot automatische registratie ("log") in het logboek van elke toegang tot de gegevens die de operator bewaart voor de autoriteiten, heeft tot doel te vermijden dat toegang tot die gegevens mogelijk is zonder sporen ervan in het logboek. Zo kan een niet-toegestane toegang (misbruik) tot de gegevens teruggevonden worden dankzij het logboek.

Er wordt een onderscheid gemaakt tussen de toegang tot de gegevens die de operator bewaart voor doeleinden van de autoriteiten en de toegang tot de gegevens die hij bewaart voor zijn eigen doeleinden of in het belang van zijn abonnees, want wat die tweede categorie van toegang betreft, moeten verschillende teams van de operator (bijvoorbeeld zijn factureringsteam of zijn antifraudeteam) en niet enkel zijn Coördinatiecel, toegang kunnen hebben tot die gegevens. Om te zorgen voor evenredige regels, geldt de verplichting tot registratie van de toegang tot de gegevens die de operator bewaart voor zijn eigen doeleinden of in het belang van zijn abonnees enkel voor zijn Coördinatiecel.

Het doel van het logboek bestaat erin om na te gaan of de toegang tot een bewaard gegeven wel degelijk gerechtvaardigd is door een verzoek van een overheid en, indien dat niet het geval is, om de persoon die toegang heeft gehad tot de gegevens, terug te vinden.

Uit de bijdragen tot de openbare raadpleging over het voorontwerp van wet blijkt dat de automatisering van de registratie ("log") van de toegang van een lid van de Coördinatiecel tot de bewaarde gegevens (identiteit van deze persoon en moment van de toegang) om te antwoorden op een vraag van een autoriteit, geen ingewikkelde maatregel is om in te voeren, aangezien zo'n type van "log" reeds ruim veralgemeend is. De geautomatiseerde registratie van de overige gegevens waarin artikel 127/2, § 4, voorziet is daarentegen momenteel niet voorgeschreven en zou een investering veronderstellen die enorm zou kunnen blijken ten aanzien van de aanvragen die sommige operatoren daadwerkelijk ontvangen. Bijgevolg wordt bepaald dat deze gegevens manueel in het logboek mogen worden ingevuld. Dat zal niets afdoen aan de waarde van het logboek, aangezien de gegevens aan de hand waarvan een raadpleging van bewaarde gegevens kan worden achterhaald, daarentegen wel automatisch geregistreerd zullen worden in het logboek. Eventueel zullen de operatoren in het logboek ook informatie kunnen opnemen die nodig is

NTSU-CTIF (gestion des requêtes des autorités et de leur réponse).

Le journal doit permettre de prendre facilement connaissance de la demande de l'autorité (ou d'une copie de cette demande). Seul ce qui est demandé à l'opérateur doit être repris dans le journal.

L'opérateur ne doit pas conserver dans le journal la réponse envoyée à l'autorité mais bien les "métadonnées" liées à cette réponse. En cas de doute sur la légalité d'un accès aux données conservées, cela permettra de rechercher la réponse envoyée à l'autorité et, le cas échéant, de contacter l'autorité indiquée dans le journal.

Lorsqu'une autorité formule sa demande dans un document et reprend en annexe de ce document les finalités et le contexte de l'enquête ou des informations qui justifient la demande, l'opérateur devra conserver dans le journal (une copie de) ce document (la demande) mais ne pourra pas y conserver les annexes.

Par contre, si ces finalités, ce contexte ou ces informations sont incorporés dans la demande de l'autorité (et n'en sont pas dissociables), l'opérateur devra enregistrer dans le journal la copie de la demande sans la modifier.

Dans son avis, l'Autorité de protection des données indique ce qui suit: "L'avant-projet indique que "le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte". L'Autorité souligne, au contraire, qu'il est nécessaire que la finalité concrète pour laquelle l'accès aux données a été demandé soit ajoutée dans les informations que doit comprendre le journal parce que cette information est nécessaire, pour permettre un contrôle effectif a posteriori de l'utilisation des données. Toutefois, au vu de la sensibilité de cette information, il faut prévoir que cette information soit journalisée de manière "floutée"." Ce point de l'avis de l'Autorité de protection des données n'a pas été suivi, dès lors que l'objectif du journal est de contrôler l'accès du personnel de l'opérateur aux données conservées (et d'éviter ainsi tout accès abusif à ces données) et non pas de contrôler la demande de l'autorité (justification et proportionnalité). Il convient également de rappeler que le journal comprend déjà un certain nombre d'informations (en particulier une copie de la demande de l'autorité ou un lien vers la demande) qui permet de vérifier si l'accès aux données conservées était bien justifié. Les données et documents dans le

om de aanvraag terug te vinden in het systeem "Tank" van de NTSU-CTIF (beheer van de verzoeken van de autoriteiten en het antwoord erop).

Via het logboek moet gemakkelijk kennis kunnen worden genomen van het verzoek van de autoriteit (of van een kopie van dat verzoek). Enkel wat wordt gevraagd aan de operator moet worden opgenomen in het logboek.

De operator hoeft het aan de autoriteit gestuurde antwoord niet te bewaren in het logboek maar wel de "metagegevens" in verband met dat antwoord. In geval van twijfel over de wettelijkheid van een toegang tot de bewaarde gegevens, kan op die manier het antwoord dat werd verstuurd aan de autoriteit worden opgezocht en desgevallend contact worden opgenomen met de autoriteit vermeld in het logboek.

Wanneer een autoriteit haar verzoek in een document formuleert en als bijlage bij dat document de doeleinden en de context van het onderzoek of informatie ter rechtvaardiging van het verzoek opneemt, dan moet de operator in het logboek (een kopie van) dat document (het verzoek) bewaren maar zonder de bijlagen erbij.

Indien die doeleinden, die context of die informatie daarentegen zijn opgenomen in het verzoek van de autoriteit (en daar niet van kunnen worden losgekoppeld), dan zal de operator in het logboek de kopie van het verzoek moeten opnemen zonder het te wijzigen.

In haar advies geeft de Gegevensbeschermingsautoriteit het volgende aan: "Het voorontwerp stelt als volgt: "Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan.". De Autoriteit benadrukt echter dat het concrete doel waarvoor de toegang tot de gegevens werd gevraagd in de informatie in het logboek moet worden vermeld aangezien die informatie nodig is om het gebruik van de gegevens a posteriori daadwerkelijk te kunnen controleren. Gezien de gevoeligheid van die informatie moet ze echter "omfloerst" worden opgetekend."." Dit punt van het advies van de Gegevensbeschermingsautoriteit is niet gevolgd, omdat het doel van het logboek nu eenmaal erin bestaat de toegang van het personeel van de operator tot de bewaarde gegevens te controleren (en zo elke onrechtmatige toegang tot deze gegevens te vermijden) en niet om de vraag van de autoriteit te controleren (rechtvaardiging en evenredigheid). Tevens moet eraan worden herinnerd dat het logboek ook al een aantal inlichtingen bevat (in het bijzonder een afschrift van het verzoek van de autoriteit of een link naar het verzoek) waarmee kan worden nagegaan of de toegang tot de bewaarde gegevens wel degelijk gerechtvaardigd

journal permettront à l'Autorité de protection de données de s'adresser à l'autorité qui a fait la demande pour obtenir plus d'informations sur cette dernière.

La tenue du journal, l'accès à celui-ci et les modifications qui y sont apportées doivent faire l'objet d'une procédure claire et conforme aux standards du RGPD, de manière à garantir l'authenticité et l'intégrité des données. Dans son avis, l'Autorité de protection des données estime que toute manipulation dans le journal doit être elle-même journalisée ou qu'il faut introduire une impossibilité d'effacement des données reprises dans le journal. Ces deux points sont suivis. D'abord, l'opérateur ne peut pas modifier des données qui ont déjà été introduites dans le journal. Ensuite, l'opérateur devra garder un inventaire des différentes consultations du journal (cela permet entre autres de déterminer dans quelle mesure l'opérateur contrôle l'accès aux données conservées à l'aide du journal).

Dans le cadre du contrôle de l'opérateur, l'IBPT et l'Autorité de protection des données peuvent consulter le journal ou exiger une copie de ce dernier. Cela n'empêche pas une consultation du journal dans un autre cadre (par exemple par le juge d'instruction si une personne a accédé aux données de manière illégale).

Paragraphe 5

La possibilité de demander un audit externe (organisme externe à l'opérateur) a été ajoutée de manière à faciliter le contrôle par l'IBPT du respect des obligations à charge des opérateurs. L'opérateur devra proposer à l'IBPT un organisme et il reviendra à l'IBPT de marquer son accord avant que cet organisme ne puisse effectuer le contrôle. Dans le cadre de son accord, l'IBPT examinera si l'organisme est bien qualifié et indépendant. Si l'opérateur ne propose pas à l'IBPT d'organisme adéquat, ce dernier sera choisi par l'IBPT.

Dans le cadre de la consultation publique, certains opérateurs ont indiqué que le coût de l'audit devrait être supporté par l'IBPT. Il convient à cet égard de noter que le principe d'un audit de sécurité à charge de l'opérateur est déjà inscrit à l'article 114/2, § 2 (sécurité des réseaux). Par ailleurs, l'IBPT ne pourra mettre les coûts de l'audit à charge de l'opérateur que s'il dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2, 3 ou 4.

was. Aan de hand van de gegevens en documenten in het logboek zal de Gegevensbeschermingsautoriteit zich kunnen richten tot de autoriteit die het verzoek heeft gedaan, om meer informatie over die laatste te krijgen.

Het houden van het logboek, de toegang ertoe en de wijzigingen die erin worden aangebracht, moeten het voorwerp uitmaken van een duidelijke procedure die in overeenstemming is met de standaarden van de AVG, zodat de authenticiteit en de integriteit van de gegevens gewaarborgd zijn. In haar advies is de Gegevensbeschermingsautoriteit van oordeel dat elke manipulatie in het logboek zelf in het logboek opgenomen moet worden of dat een onmogelijkheid moet worden ingevoerd om gegevens die in het logboek staan, te wissen. Beide punten zijn gevolgd. Ten eerste mag de operator gegevens die reeds in het logboek zijn ingevuld niet wijzigen. Ten tweede zal de operator een inventaris moeten bijhouden van de verschillende raadplegingen van het logboek (zo kan onder andere worden bepaald in welke mate de operator de toegang tot de gegevens die met behulp van het logboek bewaard worden, controleert).

In het kader van de controle van de operator kunnen het BIPT en de Gegevensbeschermingsautoriteit het logboek raadplegen of een kopie ervan eisen. Dat neemt niet weg dat het logboek in een ander kader kan worden geraadpleegd (bijvoorbeeld door de onderzoeksrechter indien een persoon toegang heeft gehad tot de gegevens op een onwettige manier).

Paragraaf 5

De mogelijkheid om een externe audit te vragen (instantie van buiten de operator) werd toegevoegd teneinde de controle door het BIPT op de inachtneming van de verplichtingen ten laste van de operatoren te vergemakkelijken. De operator zal aan het BIPT een instantie moeten voorstellen en het zal aan het BIPT zijn om zijn akkoord te geven alvorens die instantie de controle mag uitvoeren. In het kader van zijn akkoord, zal het BIPT nagaan of de instantie wel degelijk gekwalificeerd en onafhankelijk is. Als de operator het BIPT geen geschikte instantie voorstelt, zal deze door het BIPT worden gekozen.

In het kader van de openbare raadpleging hebben sommige operatoren laten weten dat de kosten van de audit gedragen zouden moeten worden door het BIPT. Daarbij moet worden opgemerkt dat het principe van een veiligheidsaudit ten laste van de operator reeds is ingeschreven in artikel 114/2, § 2 (veiligheid van de netwerken). Bovendien zal het BIPT de kosten van de audit maar ten laste kunnen leggen van de operator indien het over aanwijzingen beschikt die zouden kunnen wijzen op een inbreuk van een operator op paragraaf 2, 3 of 4.

Cependant, cet auditeur ne pourra pas prendre connaissance du journal de l'opérateur ou de demandes d'accès des autorités, et ce afin de protéger la confidentialité de ces demandes. L'audit portera donc sur la sécurité et la protection des données conservées.

Art. 13 (insertion de l'article 127/3)

Paragraphe 1er

L'article 127/3 reprend le contenu de l'ancien article 126/1, annulé dans le cadre de l'annulation de la loi "conservation des données" par la Cour constitutionnelle. Quelques modifications ont été apportées à cet article.

Tout d'abord, au paragraphe 1er, vu que la notion de service de communications électroniques est définie dans le Code de manière plus large qu'actuellement, il n'est plus nécessaire de viser dans l'article 127/3 les opérateurs et les fournisseurs de service mais il suffit de viser les opérateurs.

L'alinéa 1er renvoyait à une liste de dispositions ("des articles 46*bis*, 88*bis* et 90*ter* du Code d'instruction criminelle, des articles 18/7, 18/8, 18/16 et 18/17 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et des articles 81, 82, 2°, et 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers"), qui, avec le temps, est devenue longue et incomplète. Cette liste est remplacée par une référence aux pouvoirs des autorités de demander aux opérateurs fournissant des réseaux ou services de communications électroniques en Belgique des données relatives aux communications électroniques.

Ce sont les membres de la Cellule de coordination qui sont les seuls à pouvoir répondre aux demandes des autorités d'obtenir des données relatives aux communications électroniques. Cela n'empêche pas de mettre en œuvre un système automatisé de demandes envers la Cellule et de réponses automatiques de cette dernière vers le demandeur.

Afin de protéger les données et dans un but d'efficacité, il est essentiel que les différentes autorités qui entendent obtenir de l'opérateur des données de communications électroniques s'adressent à sa Cellule de coordination.

Paragraphe 2

Pour répondre aux requêtes des autorités, les opérateurs seront amenés de plus en plus souvent à consulter

Toch zal deze auditor geen kennis kunnen nemen van het logboek van de operator of de verzoeken om toegang vanwege de autoriteiten, teneinde de vertrouwelijkheid van deze verzoeken te vrijwaren. De audit zal dus betrekking hebben op de beveiliging en de bescherming van de bewaarde gegevens.

Art. 13 (invoeging van artikel 127/3)

Paragraaf 1

Artikel 127/3 neemt de inhoud over van het oude artikel 126/1, dat nietig is verklaard in het kader van de nietigverklaring van de wet "gegevensbewaring" door het Grondwettelijk Hof. In dat artikel zijn enkele wijzigingen aangebracht.

Allereerst, in paragraaf 1, aangezien de notie van elektronische-communicatiedienst in het Wetboek ruimer gedefinieerd is dan nu het geval is, is het niet meer noodzakelijk om in artikel 127/3 de operatoren en de aanbieders van diensten te beogen, maar volstaat het om de operatoren te beogen.

Het eerste lid verwees naar een lijst van bepalingen ("de artikelen 46*bis*, 88*bis* en 90*ter* van het Wetboek van strafvordering, de artikelen 18/7, 18/8, 18/16 en 18/17 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en de artikelen 81, 82, 2°, en 84, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten") die in de loop van de tijd lang en onvolledig is geworden. Deze lijst wordt vervangen door een verwijzing naar de bevoegdheden van de autoriteiten om aan de operatoren die in België elektronische-communicatienetwerken of -diensten verstrekken, gegevens met betrekking tot de elektronische communicatie te mogen vragen.

De leden van de Coördinatiecel zijn de enigen die mogen antwoorden op de verzoeken van de autoriteiten om gegevens over de elektronische communicatie te krijgen. Dat belet niet dat een geautomatiseerd systeem van verzoeken aan de Cel en automatische antwoorden van deze laatste aan de aanvrager wordt aangewend.

Teneinde de data te beschermen en met het oog op efficiëntie, is het essentieel dat de verschillende autoriteiten die van de operator elektronische-communicatiegegevens horen te krijgen, zich richten tot diens Coördinatiecel.

Paragraaf 2

Om op de verzoeken van de autoriteiten te antwoorden, zullen de operatoren steeds vaker

des métadonnées de communications électroniques qu'ils conservent pour leurs propres besoins (ex. facturation ou marketing) ou dans l'intérêt de leurs clients (ex. lutte contre la fraude). Cependant, en pratique, les membres de la Cellule de coordination n'ont généralement pas d'accès aux bases de données comprenant ces données ni n'ont l'expertise pour consulter ces bases de données de manière rapide et précise et y retrouver les données recherchées. Cela signifie que ce sont les experts de l'opérateur qui sont familiers avec ces bases de données qui devront rassembler les informations recherchées et les communiquer à la Cellule de coordination. Cependant, contrairement aux membres de la Cellule de coordination, ces experts n'ont pas fait l'objet d'un screening de sécurité. Dès lors, pour protéger les informations relatives aux enquêtes, l'article 127/3 prévoit dorénavant que les membres de la Cellule de coordination ne fournissent aux experts que les seules informations nécessaires pour obtenir leur aide. Cela signifie qu'ils ne pourront pas leur communiquer le réquisitoire en tant que tel, ni toute information sur le contexte de l'enquête.

Lors de la consultation publique sur la transposition du Code et lors de la consultation publique relative au présent avant-projet de loi, de nombreux opérateurs ont insisté pour supprimer l'obligation d'établissement sur le territoire belge de la Cellule de coordination de la Justice. Cette cellule est prévue à l'article 2, § 2, de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques (ci-après "l'arrêté royal collaboration légale") et est l'équivalent de la Cellule de coordination visée à l'article 127/3. Ils ont proposé que cette cellule puisse être établie sur le territoire de l'Union européenne.

En effet, les opérateurs internationaux n'ont pas toujours l'expertise nécessaire en Belgique pour répondre aux demandes des autorités. Ils estiment que les autorités belges seraient mieux servies si l'opérateur pouvait répondre à la demande à partir de son centre d'expertise, souvent situé à l'étranger.

En pratique, pour respecter l'arrêté royal collaboration légale, certains opérateurs désignaient comme membre de leur Cellule de coordination Justice un intermédiaire en Belgique (par exemple un bureau d'avocats) mais les techniciens qui traitaient effectivement la demande de l'autorité se trouvaient à l'étranger. Il convient d'éviter d'inciter les opérateurs à procéder de la sorte, car cela n'est pas conforme au principe de la législation selon lequel le recours du membre de la Cellule de coordination à un préposé doit rester l'exception. Une telle situation n'est pas bénéfique pour les autorités belges:

elektronische-communicatiemetagegevens moeten raadplegen die ze voor hun eigen behoeften (bijv. facturering of marketing) of in het belang van hun klanten (bijv. fraudebestrijding) bewaren. In de praktijk hebben de leden van de Coördinatiecel doorgaans echter geen toegang tot de databanken die deze gegevens bevatten en hebben ze evenmin de knowhow om deze databanken snel en nauwkeurig te raadplegen en daarin de gezochte gegevens terug te vinden. Dat betekent dat het de experts van de operator zijn die met deze databanken vertrouwd zijn, die de gezochte informatie zullen moeten verzamelen en meedelen aan de Coördinatiecel. In tegenstelling tot de leden van de Coördinatiecel hebben die experts evenwel niet het voorwerp uitgemaakt van een veiligheidsscreening. Om de informatie met betrekking tot de verzoeken te beschermen bepaalt artikel 127/3 daarom voortaan dat de leden van de Coördinatiecel aan de experts enkel de informatie verstrekken die nodig is om hun hulp te krijgen. Dat betekent dat ze aan hen niet de vordering op zich, noch enige informatie over de context van het verzoek zullen mogen meedelen.

Tijdens de openbare raadpleging over de omzetting van het Europees wetboek en tijdens de openbare raadpleging over het onderhavige voorontwerp van wet hebben talrijke operatoren erop gestaan dat de verplichting zou worden afgeschaft dat de Coördinatiecel Justitie gevestigd moet zijn op Belgisch grondgebied. Deze cel wordt voorgeschreven in artikel 2, § 2, van het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie (hierna "het koninklijk besluit wettelijke medewerking") en is het equivalent van de Coördinatiecel bedoeld in artikel 127/3. Zij hebben voorgesteld dat die cel zou mogen worden opgericht op het grondgebied van de Europese Unie.

De internationale operatoren hebben immers niet altijd de nodige knowhow in België om op de verzoeken van de autoriteiten te antwoorden. Zij zijn van oordeel dat de Belgische autoriteiten beter gediend zouden worden als de operator zou mogen antwoorden op het verzoek vanuit zijn expertisecentrum, dat vaak in het buitenland ligt.

Om in de praktijk het koninklijk besluit wettelijke medewerking na te leven, wezen sommige operatoren een tussenpersoon in België aan als lid van hun Coördinatiecel Justitie (bijvoorbeeld een advocatenkantoor), maar de technici die de vraag van de autoriteit daadwerkelijk behandelden bevonden zich in het buitenland. Er moet worden vermeden dat de operatoren aangespoord worden om zo te werk te gaan, want dat strookt niet met het principe van de wetgeving volgens dewelke het beroep van het lid van de Coördinatiecel op een aangestelde de uitzondering moet blijven. Een dergelijke situatie is niet gunstig voor de Belgische autoriteiten:

le membre de la Cellule de coordination en Belgique ne dispose pas de l'expertise technique nécessaire pour une collaboration efficace avec les autorités;

le membre de la Cellule de coordination en Belgique fera l'objet d'un avis de sécurité, mais aucun screening ne sera effectué par rapport aux personnes à l'étranger qui vont effectivement traiter la demande.

Il faut également rappeler que la notion d'opérateur, avec la transposition du Code, s'élargit, puisqu'elle inclut dorénavant les fournisseurs au public de services de communications interpersonnelles qui ne sont pas fondés sur la numérotation. Ces fournisseurs ne disposent pas de réseau en Belgique. Certains fournisseurs qui offrent des services dans plusieurs États membres (et par exemple des services en Belgique à partir de l'étranger) estiment que l'exigence de la Cellule de coordination en Belgique constitue une restriction disproportionnée par rapport aux libertés prévues par le droit de l'Union européenne (liberté d'établissement et libre circulation des services).

Cependant, dans son avis sur l'avant-projet de loi, le Comité R plaide pour le maintien de l'avis de sécurité dans la loi (durée de validité limitée à 5 ans et cet avis peut être modifié à tout moment en raison d'antécédents problématiques).

Pour trouver un équilibre entre les différents intérêts en jeu, un système transitoire est mis en place. À savoir que l'exigence d'un avis de sécurité est provisoirement maintenue mais sera levée pour les étrangers avec l'adoption d'un arrêté royal qui fixera des mesures de sécurité alternatives et permettra, pour les opérateurs qui ne disposent pas d'un réseau de communications électroniques en Belgique, l'établissement de la Cellule de coordination sur le territoire de l'Union européenne.

Lorsque ces mesures alternatives de sécurité seront mises en place par arrêté royal, des personnes pour lesquelles l'Autorité Nationale de Sécurité (ANS) ne peut rendre un avis de sécurité, à défaut de suffisamment d'informations disponibles lors de l'enquête de sécurité (typiquement les personnes résidant à l'étranger), pourront faire partie de la Cellule de coordination de l'opérateur si elles respectent ces mesures alternatives. Cela permettra à l'opérateur d'établir sa Cellule de coordination sur le territoire de l'Union européenne.

Lorsque ces mesures alternatives seront mises en place, les personnes pour lesquelles l'ANS peut rendre un avis de sécurité (les personnes résidant depuis un

het lid van de Coördinatiecel in België beschikt niet over de technische knowhow die noodzakelijk is voor een efficiënte medewerking met de autoriteiten;

het lid van de Coördinatiecel in België zal het voorwerp uitmaken van een veiligheidsadvies, maar ten opzichte van de personen in het buitenland die het verzoek daadwerkelijk zullen behandelen, zal er geen screening zijn.

Bovendien moet eraan worden herinnerd dat het begrip operator met de omzetting van het Europees wetboek uitgebreid wordt, aangezien daarin vanaf nu ook de aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten aan het publiek begrepen zijn. Deze aanbieders beschikken niet over een netwerk in België. Sommige aanbieders die diensten aanbieden in verschillende lidstaten (en bijvoorbeeld diensten in België vanuit het buitenland) zijn van oordeel dat de eis van de Coördinatiecel in België een onevenredige beperking vormt ten opzichte van de vrijheden waarin het recht van de Europese Unie voorziet (vrijheid van vestiging en vrij verkeer van diensten).

In zijn advies over het voorontwerp van wet pleit Comité I evenwel voor het behoud van het veiligheidsadvies in de wet (geldigheidsduur beperkt tot 5 jaar en dat advies kan steeds worden gewijzigd wegens problematische antecedenten).

Om een evenwicht te vinden tussen de verschillende belangen waarom het gaat, wordt een overgangssysteem ingesteld. En dat is dat de eis van een veiligheidsadvies voorlopig behouden wordt maar afgeschaft zal worden voor buitenlanders met de aanneming van een koninklijk besluit dat alternatieve veiligheidsmaatregelen zal vaststellen en het mogelijk zal maken, voor de operatoren die niet over een elektronische-communicatienetwerk beschikken in België, dat de Coördinatiecel wordt gevestigd op het grondgebied van de Europese Unie.

Wanneer die alternatieve veiligheidsmaatregelen bij koninklijk besluit vastgesteld zullen zijn, zullen personen voor wie de Nationale Veiligheidsoverheid (NVO) geen veiligheidsadvies kan verstrekken, bij gebrek aan voldoende beschikbare informatie tijdens het veiligheidsonderzoek (typisch de personen die in het buitenland verblijven), deel mogen uitmaken van de Coördinatiecel van de operator, als zij aan die alternatieve maatregelen voldoen. Daardoor zal de operator zijn Coördinatiecel kunnen vestigen op het grondgebied van de Europese Unie.

Nadat deze alternatieve maatregelen ingesteld zullen zijn, zullen de personen voor wie de NVO een veiligheidsadvies kan verstrekken (de personen die al enige

certain temps en Belgique) resteront soumises à l'exigence d'un avis de sécurité.

Pour répondre à un point du Comité R, il convient également de rappeler qu'en vertu de l'article 22*quinquies*/1, § 5, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, l'ANS peut de sa propre initiative émettre ultérieurement un nouvel avis de sécurité sur la base de nouvelles informations (par exemple il apparaît qu'une personne qui était considérée comme fiable ne l'est pas).

Il revient à l'ANS de fixer la durée de validité de l'avis de sécurité lorsqu'elle le rend, cette durée ne pouvant pas être supérieure à 5 ans.

L'autorité administrative compétente pour le traitement des avis est le ministre de la Justice. Cependant, en pratique, rien n'empêche ce ministre de déléguer sa tâche à une administration.

Depuis sa modification par la loi du 2 mai 2019, l'article 22*quinquies*, § 6, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité prévoit une obligation à charge d'une entreprise de désigner un officier de sécurité lorsque certains membres du personnel de cette entreprise sont soumis à un avis de sécurité positif.

Cette obligation n'a cependant pas été conçue dans le contexte de la Cellule de coordination des opérateurs et s'avère être disproportionnée pour les opérateurs qui ne doivent pas déjà désigner un tel officier en raison d'autres activités que la Cellule de coordination et qui ne reçoivent pas ou peu de demandes des autorités judiciaires relatives aux données de communications électroniques.

Dès lors une dérogation à l'obligation de désigner un officier de sécurité est introduite dans la présente loi pour le cas spécifique de la Cellule de coordination. Il convient de rappeler que la présente loi déroge déjà à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. En effet, l'article 22*quinquies* de cette loi prévoit une procédure au terme de laquelle l'ANS prend une décision d'imposer un avis de sécurité pour des catégories de personnes au sein de certaines organisations. Le présent article déroge à cette procédure, vu qu'il impose lui-même l'avis de sécurité.

Certaines exigences qui se trouvaient auparavant dans l'article 126/1, paragraphe 1er, (communication des

tijd in België verblijven) onderworpen blijven aan de eis inzake een veiligheidsadvies.

Om te antwoorden op een punt van Comité I, moet ook eraan herinnerd worden dat krachtens artikel 22*quinquies*/1, § 5, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, de NVO op eigen initiatief later een nieuw veiligheidsadvies mag uitbrengen op basis van nieuwe informatie (wanneer bijvoorbeeld blijkt dat een persoon die als betrouwbaar was beschouwd, dat niet is).

Het komt aan de NVO toe om de geldigheidsduur van het veiligheidsadvies te bepalen, wanneer zij dat verstrekt, maar die duur mag niet langer zijn dan 5 jaar.

De administratieve instantie die bevoegd is voor de behandeling van de adviezen is de minister van Justitie. In de praktijk staat echter niets in de weg dat deze minister zijn taak delegeert aan een administratie.

Sedert de wijziging ervan bij de wet van 2 mei 2019 voorziet artikel 22*quinquies*, § 6, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen in een verplichting in hoofde van een onderneming om een veiligheidsofficier aan te wijzen wanneer sommige personeelsleden van die onderneming onderworpen zijn aan een positief veiligheidsadvies.

Deze verplichting is echter niet bedacht in de context van de Coördinatiecel van de operatoren en blijkt onevenredig te zijn voor de operatoren die nog niet een dergelijke officier moeten aanwijzen wegens andere activiteiten buiten de Coördinatiecel en die van de gerechtelijke autoriteiten geen of weinig verzoeken ontvangen in verband met de elektronische-communicatiegegevens.

Daarom wordt in de onderhavige wet een afwijking van de verplichting om een veiligheidsofficier aan te wijzen ingevoerd voor het specifieke geval van de Coördinatiecel. Er moet herinnerd worden aan het feit dat de onderhavige wet reeds afwijkt van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Artikel 22*quinquies* van deze wet voorziet immers in een procedure na afloop waarvan de NVO een beslissing neemt om een veiligheidsadvies op te leggen voor categorieën van personen bij sommige organisaties. Het onderhavige artikel wijkt af van deze procedure, aangezien het zelf het veiligheidsadvies oplegt.

Sommige eisen die voordien opgenomen waren in artikel 126/1, paragraaf 1, (mededeling van de

coordonnées des membres de la Cellule de coordination à l'Autorité de protection des données et à l'IBPT) ont été supprimées, étant donné qu'elles seront dorénavant réglées par arrêté royal. Il s'agit en effet d'aspects pratiques qui mettent en œuvre les principes d'accessibilité du personnel des opérateurs traitant les demandes des autorités.

La communication des coordonnées de la Cellule de coordination aux autorités sera dorénavant réglée par arrêté royal.

La délégation au Roi permettra d'organiser la manière dont les coordonnées de la Cellule de coordination et de ses membres sont portées à la connaissance des autorités belges qui ont besoin de ces informations. En pratique et à l'heure actuelle, la communication de ces coordonnées se fait par le biais d'un outil informatique mis en place par l'IBPT.

Paragraphe 3

La référence à l'article 114 de la loi télécom a été supprimée, étant donné que l'article 127/2, § 3, alinéa 2, 2°, fait dorénavant référence à l'article équivalent de la même loi après la transposition du Code des communications électroniques européen.

Les anciens articles 126/1 et 127 indiquaient que l'opérateur est le responsable du traitement. De manière à simplifier la législation, c'est dorénavant l'article 127/3 qui reprend les différents articles pour lesquels l'opérateur est considéré comme le responsable du traitement.

Cette disposition est sans préjudice à d'autres hypothèses pour lesquelles l'opérateur doit également être qualifié de responsable du traitement.

Ensuite, au paragraphe 3, la fonction de préposé à la protection des données à caractère personnel a été supprimée pour la raison suivante. Cette fonction a dû être introduite dans l'article 126/1 par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, vu que les opérateurs ne devaient pas encore désigner un délégué à la protection des données en vertu du RGPD. Vu que ce dernier est entretemps entré en vigueur et que tout opérateur doit, conformément à l'article 37.1.(b) du RGDP, disposer d'un délégué à la protection des données, les missions du délégué au sens de l'ancien article 126/1 de la loi télécom tombent dorénavant dans les missions du délégué à la protection des données au sens du RGPD.

contactgegevens van de leden van de Coördinatiecel aan de Gegevensbeschermingsautoriteit en aan het BIPT) zijn opgeheven, aangezien ze voortaan bij koninklijk besluit worden geregeld. Het gaat immers om praktische aspecten die de principes toepassen inzake toegankelijkheid van het personeel van de operatoren die de vorderingen van de autoriteiten behandelen.

De mededeling van de contactgegevens van de Coördinatiecel aan de autoriteiten, zal voortaan vastgelegd zijn bij koninklijk besluit.

De delegatie aan de Koning zal het mogelijk maken om de manier te organiseren waarop de contactgegevens van de Coördinatiecel en van de leden ervan, ter kennis worden gebracht van de Belgische autoriteiten, die deze informatie nodig hebben. In de praktijk en op dit ogenblik geschiedt de mededeling van die contactgegevens via een computerprogramma dat door het BIPT is ingesteld.

Paragraaf 3

De verwijzing naar artikel 114 van de telecomwet werd verwijderd, aangezien artikel 127/2, § 3, tweede lid, 2°, voortaan verwijst naar het gelijkwaardige artikel van dezelfde wet na de omzetting van het Europees wetboek voor elektronische communicatie.

De voormalige artikelen 126/1 en 127 duidden de operator aan als verantwoordelijke voor de verwerking. Om de wetgeving te vereenvoudigen, is het voortaan artikel 127/3 dat de verschillende artikelen overneemt waarvoor de operator als verantwoordelijke van de verwerking wordt beschouwd.

Deze bepaling doet geen afbreuk aan andere hypothesen waarvoor de operator ook als verantwoordelijke voor de verwerking moet aangemerkt zijn.

Vervolgens, in paragraaf 3 is de functie van aangestelde voor de bescherming van de persoonsgegevens geschrapt om de volgende reden. Die functie moest worden ingevoerd in artikel 126/1 bij de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, aangezien de operatoren nog geen functionaris voor gegevensbescherming moesten aanwijzen krachtens de AVG. Vermits die verordening inmiddels in werking is getreden en elke operator, conform artikel 37.1 (b) van de AVG over een functionaris voor gegevensbescherming moet beschikken, vallen de opdrachten in de zin van het oude artikel 126/1 van de telecomwet van die aangestelde voortaan binnen de opdrachten van de functionaris voor gegevensbescherming in de zin van de AVG.

Paragraphe 4

Les délégations au Roi prévues dans l'ancien article 127, § 1er, et l'ancien article 126/1, § 4, qui permettaient à ce dernier de régler la collaboration entre les opérateurs et les autorités pour la fourniture de données à ces dernières ont été réécrites dans l'article 127/3, paragraphe 4.

Au paragraphe 4, les délégations au Roi visent dorénavant l'avis des autorités de protection de données à caractère personnel et non plus l'avis de la Commission pour la protection de la vie privée. Il ne peut en effet pas être exclu que l'arrêté royal d'exécution de l'article 127/1 comprenne certaines dispositions qui règlent le fonctionnement des services de police ou des services de renseignement et de sécurité, pour autant que cela ait un impact sur la collaboration des opérateurs avec ces autorités. Dans ce cas, l'Organe de Contrôle de l'information policière et le Comité R devront également rendre leur avis sur ces dispositions.

Pour une meilleure lisibilité de la LCE, le paragraphe 4 reprend les éléments de l'ancien article 127 qui concernent la collaboration entre les opérateurs et les autorités belges, pour ce qui concerne l'obtention des données relatives aux communications électroniques, en particulier la fixation des tarifs dans le cadre de cette collaboration. Ce paragraphe a également été retravaillé pour expliquer les principaux éléments que le Roi doit encore régler.

Dans l'arrêté royal d'exécution de l'article 127/3, le Roi pourra, si c'est justifié, prévoir des règles différentes selon différentes catégories d'opérateurs, de manière à prendre en compte les situations différentes dans lesquelles ils se trouvent.

Art. 14 (modifications à l'article 145)

La liste des articles dont le non-respect est puni pénalement est adaptée aux nouveaux articles qui ont pour objectif la fourniture de données de communications électroniques aux autorités.

Le montant de l'article 145, paragraphe 1er, a été revu à la hausse, étant donné que le montant actuel n'est plus de nature dissuasive au vu la capacité financière de certains opérateurs.

Par ailleurs, le paragraphe 3*ter* de l'article 145, annulé par la Cour constitutionnelle dans son arrêt n° 57/2021, a été réintroduit. Il est en effet essentiel que des sanctions

Paragraaf 4

De delegaties aan de Koning vastgelegd in het voormalige artikel 127, § 1, en het voormalige artikel 126/1, § 4, die deze laatste in staat stelden om de samenwerking tussen de operatoren en de autoriteiten voor de verstrekking van gegevens aan deze laatsten te regelen, werden herschreven in artikel 127/3, paragraaf 4.

In paragraaf 4 doelen de delegaties aan de Koning voortaan op het advies van de gegevensbeschermingsautoriteiten en niet langer op het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Het kan immers niet worden uitgesloten dat het koninklijk besluit ter uitvoering van artikel 127/1 enkele bepalingen bevat die de werking van de politiediensten of van de inlichtingen- en veiligheidsdiensten regelen, voor zover dat een impact heeft op de medewerking van de operatoren met die autoriteiten. In dat geval zullen het Controleorgaan op de politionele informatie en het Comité I ook hun advies over die bepalingen moeten verstrekken.

Voor een betere leesbaarheid van de WEC neemt paragraaf 4 de elementen over van het oude artikel 127 die betrekking hebben op de samenwerking tussen de operatoren en de Belgische overheid, wat betreft het verkrijgen van de elektronische-communicatiegegevens, in het bijzonder de vaststelling van de tarieven in het kader van die samenwerking. Deze paragraaf is eveneens herwerkt om de voornaamste elementen uit te leggen die de Koning nog moet regelen.

In het koninklijk besluit ter uitvoering van artikel 127/3 zal de Koning, indien dat gerechtvaardigd is, verschillende regels kunnen vaststellen volgens verschillende categorieën van operatoren, om rekening te houden met de uiteenlopende situaties waarin zij zich bevinden.

Art. 14 (wijzigingen aan artikel 145)

De lijst van de artikelen waarvan de niet-inachtneming strafrechtelijk wordt bestraft, is aangepast aan de nieuwe artikelen met als doel de verstrekking van elektronische-communicatiegegevens aan de autoriteiten.

Het bedrag van artikel 145, paragraaf 1, is opwaarts herzien, aangezien het huidige bedrag niet meer ontradend werkt, gelet op het financiële vermogen van sommige operatoren.

Paragraaf 3*ter* van artikel 145, die werd vernietigd door het Grondwettelijk Hof in zijn arrest nr. 57/2021, werd overigens opnieuw ingevoegd. Het is immers van

pénales soient prévues en cas d'abus lors de l'accès aux données de trafic conservées par les opérateurs pour les autorités.

essentieel belang dat er wordt voorzien in strafsancties in geval van misbruik bij inzage in de verkeersgegevens die de operatoren bewaren voor de autoriteiten.

CHAPITRE 3

HOOFDSTUK 3

Modification a la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques

Wijziging aan de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

Art. 15 (modification à l'article 8)

Art. 15 (wijziging aan artikel 8)

Sur la base de l'article 126/1, § 3, 3°, j de la loi télécom en projet, les métadonnées des communications qui se sont déroulées dans les communes dans lesquelles se trouvent un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques doivent faire l'objet d'une conservation préventive de la part des opérateurs.

Op basis van artikel 126/1, § 3, 3°, j van het ontwerp van telecomwet moeten de metadata van communicaties die hebben plaatsgevonden in gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden, door de operatoren preventief worden bewaard.

Afin d'identifier ces communes, elles doivent être reprises sur une liste adoptée par le ministre de la Défense, le ministre de la Justice, et le ministre de l'Intérieur, qui reprend toutes les zones stratégiques soumises à une conservation préventive des données.

Om deze gemeenten te kunnen identificeren, moeten zij worden opgenomen in een lijst die wordt vastgesteld door de minister van Defensie, de minister van Justitie en de minister van Binnenlandse Zaken en waarin alle strategische zones zijn opgenomen die onder de preventieve gegevensbewaring vallen.

C'est sur proposition du service désigné par le Roi (NTSU), qui reçoit de chaque autorité compétente les informations concrètes nécessaires à la détermination de ces zones stratégiques que cette liste est adoptée.

De lijst wordt vastgesteld op basis van een voorstel van de door de Koning aangewezen dienst (NTSU), die van elke bevoegde autoriteit de specifieke informatie ontvangt die nodig is om deze strategische zones te bepalen.

Comme le Centre de crise National, sur la base de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, coordonne la liste des autorités sectorielles et gère l'ensemble de liste, il est logique que le Centre de crise National soit l'autorité compétente pour transmettre la liste de ces communes au service désigné par le Roi.

Aangezien het Nationaal Crisiscentrum, op basis van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, de lijst van sectorale overheden coördineert en de hele lijst beheert, is het logisch dat het Nationaal Crisiscentrum de bevoegde autoriteit is om de lijst van deze gemeenten door te sturen naar de door de Koning aangewezen dienst.

Cependant, l'article 8 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques ne prévoit actuellement la possibilité de transmettre l'emplacement d'une infrastructure critique y compris la commune qu'à l'OCAM, dans le cadre de ses finalités et au bourgmestre concerné.

Artikel 8 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur voorziet momenteel echter alleen in de mogelijkheid om de locatie van een kritieke infrastructuur, met inbegrip van de gemeente, door te geven aan het OCAD, in het kader van zijn doelstellingen, en aan de betrokken burgemeester.

Pour permettre une communication de ces communes dans lesquelles un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques se

Om het mogelijk te maken dat deze gemeenten waar zich een of meer kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden doorgegeven

trouvent au service désigné par le Roi, l'article 8 de la loi du 1er juillet 2011 est dès lors adapté dans ce sens.

CHAPITRE 4

Modifications à la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 16 (modifications à l'article 2)

Une définition de "données relatives à l'utilisateur final ou à l'abonné" a été insérée à l'article 2, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges ("loi statut IBPT").

Cette définition vise à circonscrire les données qui peuvent être considérées, notamment sur la base de la jurisprudence de la Cour de Justice de l'Union européenne (CJUE, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16), comme présentant un degré de sensibilité moindre que les autres métadonnées liées aux communications électroniques, dès lors qu'elles ne permettent pas de tirer des conclusions précises relatives à la vie privée de l'utilisateur final ou de l'abonné.

Ces données se distinguent des autres métadonnées de communications électroniques, telles que définies à l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, pour lesquelles un contrôle préalable externe se justifie au regard de la jurisprudence de la Cour de justice de l'Union européenne (en particulier, CJUE, arrêt du 2 mars 2021, Prokuratuur, C-746/18).

Art. 17 (modifications à l'article 14)

Paragraphe 1er

Il est important de veiller à ce que le respect des nouveaux articles 14, § 2, 2°/1, 25, §§ 8 à 10 et 28/1 de la loi statut IBPT puisse être contrôlée par l'Institut. C'est la raison pour laquelle le contrôle de ces articles a été ajouté à l'article 14, § 1er, 3°, d).

Les articles 14, § 2, 2°/1, 25, §§ 8 à 9 et 28/1, §§ 1 à 2 de la loi statut IBPT prévoient les conditions dans lesquelles l'Institut peut demander des données

worden aan de door de Koning aangewezen dienst, wordt artikel 8 van de wet van 1 juli 2011 dienovereenkomstig aangepast.

HOOFDSTUK 4

Wijzigingen aan de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 16 (wijzigingen aan artikel 2)

In artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector ("BIPT-statuutwet") is een definitie van "gegevens betreffende de eindgebruiker of de abonnee" ingevoegd.

Deze definitie heeft, met name op grond van de rechtspraak van het Hof van Justitie van de Europese Unie (HvJ-EU, arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16), tot doel de gegevens af te bakenen die beschouwd mogen worden als gegevens die een mindere mate van gevoeligheid vertonen dan de overige metagegevens die gelinkt zijn aan de elektronische communicatie, aangezien daaruit geen precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de eindgebruiker of abonnee.

Die gegevens onderscheiden zich van de overige elektronische-communicatiemetagegevens, zoals die gedefinieerd zijn in artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, waarvoor een voorafgaande externe controle gerechtvaardigd is ten aanzien van de rechtspraak van het Hof van Justitie van de Europese Unie (inzonderheid, HvJ-EU, arrest van 2 maart 2021, Prokuratuur, C-746/18).

Art. 17 (wijzigingen aan artikel 14)

Paragraaf 1

Het is belangrijk om erop toe te zien dat de naleving van de nieuwe artikelen 14, § 2, 2°/1, 25, §§ 8 tot 10 en 28/1 van de BIPT-statuutwet kan worden gecontroleerd door het Instituut. Dat is de reden waarom de controle van deze artikelen toegevoegd is in artikel 14, § 1, 3°, d).

De artikelen 14, § 2, 2°/1, 25, §§ 8 tot 9 en 28/1, §§ 1 tot 2 van de BIPT-statuutwet stellen voorwaarden vast waaronder het Instituut gegevens kan vragen die

conservées par les opérateurs en vertu des articles 122, 123, 126, 126/1 et 127 de la loi du 13 juin 2005 relative aux communications électroniques (“loi télécom”).

Les articles 14, § 2, 2°/1, 25, § 10 et 28/1, § 3, de la loi statut IBPT prévoient les conditions dans lesquelles l’Institut peut exiger d’un opérateur de lui permettre de consulter une base de données contenant les données conservées en vertu des articles 122, 123, 126, 126/1 et 127 de la loi télécom, pour le contrôle du respect par un opérateur de ces articles ou de leurs arrêtés d’exécution.

Lorsque l’opérateur refuse de faire droit à ces demandes, le Conseil de l’Institut dispose de la possibilité d’imposer cet accès par la voie d’une décision administrative. Le non-respect d’une décision administrative de l’Institut est puni par les sanctions visées à l’article 21 de la présente loi.

Paragraphe 2

La disposition insérée aux articles 14, § 2, 2/1° et 2/2° vise à régir un cas particulier de demande d’informations.

L’article 14, § 2, 2/1° prévoit la possibilité pour l’IBPT, agissant par le biais de son Conseil, de l’un de ses officiers de police judiciaire, ou de l’un des membres de son personnel, de demander à l’opérateur les données relatives à l’utilisateur final, à l’abonné, ou d’autres métadonnées de communications électroniques qui sont nécessaires à l’accomplissement de l’une de ses missions d’application et de contrôle des dispositions prévues à l’article 14, paragraphe 1er, 3°, a) et g) à i), aux conditions prévues aux articles 25, §§ 8 et 9 et 28/1, paragraphes 1 et 2.

Il s’agit des missions de contrôle du respect de la loi télécom (art. 14, § 1er, 3°, a)) et des autres législations sectorielles en matière de sécurité des réseaux et des systèmes d’information (à savoir: art. 14, § 1er, 3°, g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques; h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques; et i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques).

de operatoren bewaren krachtens de artikelen 122, 123, 126, 126/1 en 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie (“telecomwet”).

De artikelen 14, § 2, 2°/1, 25, § 10 en 28/1, § 3, van de BIPT-statuutwet bepalen de voorwaarden waaronder het Instituut van een operator kan verlangen dat deze het Instituut een databank laat raadplegen die de gegevens bevat die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127 van de telecomwet, om te controleren of een operator deze artikelen of de uitvoeringsbesluiten ervan naleeft.

Wanneer de operator weigert op die verzoeken in te gaan, beschikt de Raad van het Instituut over de mogelijkheid om die toegang op te leggen via een administratief besluit. De niet-naleving van een administratief besluit van het Instituut wordt bestraft met de sancties bedoeld in artikel 21 van de onderhavige wet.

Paragraaf 2

De bepaling die ingevoegd wordt in de artikelen 14, § 2, 2/1° en 2/2°, beoogt een specifiek geval van verzoek om inlichtingen te regelen.

Artikel 14, § 2, 2/1°, voorziet in de mogelijkheid voor het BIPT, dat optreedt via zijn Raad, een van zijn officieren van gerechtelijke politie of een van zijn personeelsleden, om aan de operator de gegevens betreffende de eindgebruiker, de abonnee of andere elektronischecommunicatiemetagegevens te vragen die noodzakelijk zijn voor de vervulling van een van zijn opdrachten inzake toepassing en controle van de in artikel 14, paragraaf 1, 3°, a) en g) tot i), vastgestelde bepalingen, onder de voorwaarden bepaald in de artikelen 25, §§ 8 en 9 en 28/1, de paragrafen 1 en 2.

Het gaat om de opdrachten inzake controle van de naleving van de telecomwet (art. 14, § 1, 3°, a)) en van de overige sectorale wetgevingen betreffende de veiligheid van de netwerken en informatiesystemen (namelijk: art. 14, § 1, 3°, g) van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat betreft de sectoren van de elektronische communicatie en de kritieke infrastructuren; h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wat de sector van de digitale infrastructuren betreft; en i) Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie).

Les finalités poursuivies par ces articles correspondent aux finalités suivantes prévues à l'article 127/1, § 2 de la loi télécom:

— la prévention de menaces graves contre la sécurité publique (art. 127, § 2, 2° de la loi télécom);

— l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques (art. 127, § 2, 4° de la télécom);

— la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques (art. 127, § 2, 5° de la loi télécom);

— le contrôle par l'Institut du respect de la loi télécom et les missions de contrôle des autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle (art. 127, § 2, 9° de la loi télécom).

L'accès aux métadonnées des opérateurs est nécessaire notamment en cas de contrôle du respect par les opérateurs de leurs obligations en matière de protection des utilisateurs (p.ex. facturation détaillée), de secret des communications (p.ex. vérification de la suppression ou de l'anonymisation des données conservées en vertu des articles 122 à 127 de la loi télécom), en matière de lutte contre les fraudes (article 121/8) ou en matière de sécurité des réseaux (article 114 et suivants).

Par ailleurs, l'article 14, § 2, 2/2° prévoit la possibilité pour l'IBPT, agissant par le biais de son Conseil, de l'un de ses officiers de police judiciaire, ou de l'un des membres de son personnel, de demander à l'opérateur, pour l'une de ces missions de contrôle du respect des articles 122, 123, 126, 126/1 et 127, la consultation d'une base de données contenant les données dont la conservation est prévue par ou en vertu de ces articles, aux conditions prévues aux articles 25, § 10 et 28/1, § 3. La finalité poursuivie par cet article correspond à la finalité suivante prévue à l'article 127/1, § 2 de la loi télécom: le contrôle de la loi télécom par l'Institut et les missions de contrôle des autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle (art. 127, § 2, 9° de la loi télécom).

Lorsque la demande est adressée à l'opérateur par un officier de police judiciaire dans le cadre de ses missions prévues à l'article 24 de la présente loi, les dispositions de l'article 25, §§ 8 à 10, sont applicables.

Hetgeen deze artikelen nastreven komt overeen met de volgende doeleinden waarin artikel 127/1, § 2, van de telecomwet voorziet:

— de preventie van ernstige bedreigingen van de openbare veiligheid (art. 127, § 2, 2°, van de telecomwet);

— het onderzoek van veiligheidslekken inzake elektronische-communicatienetwerken of -diensten (art. 127, § 2, 4°, van de telecomwet);

— de preventie, het onderzoek en de opsporing van strafrechtelijke inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd (art. 127, § 2, 5°, van de telecomwet);

— het toezicht van het Instituut op de naleving van de telecomwet en de controleopdrachten van de autoriteiten die bevoegd zijn voor de gegevensbescherming in het kader van hun controleopdrachten (art. 127, § 2, 9°, van de telecomwet).

De toegang tot de metagegevens van de operatoren is noodzakelijk met name in geval van de controle of de operatoren hun verplichtingen naleven inzake bescherming van de gebruikers (bijv. gespecificeerde facturering), de geheimhouding van de communicatie (bijv. verificatie van het wissen of anonimiseren van de gegevens bewaard krachtens de artikelen 122 tot 127 van de telecomwet), fraudebestrijding (artikel 121/8) of netwerkbeveiliging (artikel 114 en volgende).

Bovendien voorziet artikel 14, § 2, 2/2°, in de mogelijkheid voor het BIPT, dat optreedt via zijn Raad, een van zijn officieren van gerechtelijke politie of een van zijn personeelsleden, om voor een van deze controleopdrachten inzake naleving van de artikelen 122, 123, 126, 126/1 en 127, aan de operator de raadpleging te vragen van een databank die de gegevens bevat die moeten worden bewaard door of krachtens deze artikelen, onder de voorwaarden die zijn vastgesteld in de artikelen 25, § 10 en 28/1, § 3. Hetgeen dit artikel nastreeft, komt overeen met het volgende doel waarin artikel 127/1, § 2, van de telecomwet voorziet: de controle van de telecomwet door het Instituut en de controleopdrachten van de autoriteiten die bevoegd zijn voor de gegevensbescherming in het kader van hun controleopdrachten (art. 127, § 2, 9°, van de telecomwet).

Wanneer het verzoek aan de operator wordt gericht door een officier van gerechtelijke politie in het kader van zijn opdrachten vastgesteld in artikel 24 van de onderhavige wet, zijn de bepalingen van artikel 25, §§ 8 tot 10, van toepassing.

Lorsque la demande est adressée à l'opérateur par un membre du personnel de l'IBPT qui n'a pas la qualité d'officier de police judiciaire, les dispositions de l'article 28/1 sont applicables.

Lorsqu'il fait usage de l'article 14, § 2, 2°/1, l'IBPT fixe également le délai de communication des informations demandées, comme c'est le cas pour l'article 14, § 2, 2°.

Art. 18 (modifications à l'article 25)

L'article 24 charge les officiers de police judiciaire de l'IBPT de constater les infractions à la loi du 13 juin 2005 relative aux communications électroniques, au Code pénal et aux lois spéciales lorsque celles-ci sont commises au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications.

Ces infractions peuvent être des fraudes comme par exemple le "smishing" (ou hameçonnage par SMS) ou le "spoofing" (la personne appelée voit apparaître un numéro de téléphone qui ne correspond pas au numéro réel de l'appelant).

Pour l'application de l'article 25, paragraphes 8 et 9, il convient de rappeler que le Code pénal est assimilé à une loi.

Dans un souci d'efficacité et lorsqu'un opérateur informe l'IBPT d'une infraction potentielle à une loi visée à l'article 24, il est essentiel que l'opérateur lui communique dès le départ les données d'identification, de trafic ou de connexion qui sont nécessaires pour que les officiers de police judiciaire de l'IBPT puissent rechercher, constater ou poursuivre cette infraction.

Cependant, lorsqu'un officier de police judiciaire (OPJ) de l'IBPT est informé d'une infraction potentielle à une loi visée à l'article 24, il est parfois nécessaire qu'il obtienne d'un opérateur certaines métadonnées pour compléter son dossier.

Lorsque sa demande concerne des données relatives à l'utilisateur final ou l'abonné, l'OPJ peut en demander la fourniture à l'opérateur concerné moyennant l'approbation de son supérieur hiérarchique à la suite d'une demande motivée, conformément à l'article 25, § 8.

Lorsque, pour les besoins de l'accomplissement de sa mission, un OPJ demande accès à d'autres métadonnées, il soumet sa demande motivée au préalable à

Wanneer het verzoek aan de operator wordt gericht door een personeelslid van het BIPT die niet de hoedanigheid van officier van gerechtelijke politie heeft, zijn de bepalingen van artikel 28/1 van toepassing.

Wanneer gebruik wordt gemaakt van artikel 14, § 2, 2°/1, wanneer het BIPT ook de termijn voor het meedelen van de gevraagde informatie vaststelt, zoals dat het geval is voor artikel 14, § 2, 2°.

Art. 18 (wijzigingen aan artikel 25)

Artikel 24 belast de officieren van gerechtelijke politie van het BIPT met de vaststelling van de inbreuken op de wet van 13 juni 2005 betreffende de elektronische communicatie, het Strafwetboek en de bijzondere wetten wanneer deze gepleegd worden door middel van apparatuur, netwerken of diensten voor elektronische communicatie of voor radiocommunicatie.

Bij deze inbreuken kan het gaan om fraude zoals "smishing" (of phishing via sms) of "spoofing" (de opgebelde persoon krijgt een telefoonnummer te zien dat niet overeenstemt met het werkelijke nummer van de beller).

Voor de toepassing van artikel 25, de paragrafen 8 en 9, moet eraan worden herinnerd dat het Strafwetboek wordt gelijkgesteld met een wet.

Ter wille van de efficiëntie en wanneer een operator het BIPT op de hoogte brengt van een potentiële inbreuk op een wet bedoeld in artikel 24, is het van fundamenteel belang dat de operator meteen de identificatie-, verkeers- of verbindingsgegevens eraan meedeelt die nodig zijn opdat de officiers van gerechtelijke politie van het BIPT die inbreuk kunnen opsporen, vaststellen of vervolgen.

Wanneer een officier van gerechtelijke politie (OGP) van het BIPT echter op de hoogte wordt gebracht van een potentiële inbreuk op een in artikel 24 bedoelde wet, is het soms nodig dat hij van een operator bepaalde metagegevens krijgt om zijn dossier te vervolledigen.

Wanneer zijn verzoek betrekking heeft op gegevens betreffende de eindgebruiker of abonnee, kan de OGP aan de operator in kwestie vragen om die gegevens te verstrekken mits zijn hiërarchische meerdere, naar aanleiding van een gemotiveerd verzoek, toestemming heeft gegeven overeenkomstig artikel 25, § 8.

Wanneer een OGP, ten behoeve van de vervulling van zijn opdracht, toegang vraagt tot andere metagegevens , legt hij zijn gemotiveerd verzoek op voorhand voor

l'autorisation du juge d'instruction, sauf cas d'urgence dûment justifié.

Dans les cas d'urgence dûment justifiés où le contrôle préalable du juge d'instruction n'aura pas été possible, un contrôle ultérieur est effectué par le juge d'instruction.

Pour pouvoir faire un contrôle efficace de l'obligation d'un opérateur de conserver les données prévues aux articles 126, 126/1 et 127, et les copies de documents d'identité (entre autres les données et documents d'identification des utilisateurs de cartes prépayées), ainsi que de son obligation d'effacer les données ou de les rendre anonymes à l'issue de la période de conservation, il est indispensable que les officiers de police judiciaire de l'IBPT puissent consulter les bases de données de l'opérateur contrôlé, qui comprend lesdites données et copies de documents.

La disposition insérée confirme le pouvoir de ces officiers d'exiger cet accès. En pratique, ils contrôlent des échantillons représentatifs d'une base de données.

Étant donné que cet accès permet de consulter un grand nombre de données à caractère personnel des abonnés de l'opérateur, la consultation de la base de données par ces officiers de police judiciaire doit dorénavant être précédée d'une autorisation du Conseil de l'IBPT.

Lorsque l'opérateur refuse de permettre la consultation de sa base de données aux officiers de police judiciaires malgré l'autorisation du Conseil, le Conseil de l'IBPT disposera de la possibilité d'imposer cet accès par une décision administrative. Le non-respect d'une décision du Conseil de l'IBPT est puni par les sanctions visées à l'article 21 de la présente loi.

Le Conseil de l'IBPT apprécie en toute indépendance l'opportunité des contrôles à effectuer, ainsi que les priorités à établir entre ceux-ci en fonction de critères objectifs, tels que le temps écoulé depuis le dernier contrôle, l'existence d'indices d'infractions ou l'existence d'antécédents d'infractions.

Cependant, il n'est pas nécessaire que des soupçons d'infraction soient établis pour qu'un accès à la base de données soit autorisé par le Conseil de l'IBPT, puisque ce contrôle vise précisément à rechercher et détecter l'existence d'infractions éventuelles.

Même si à l'occasion de leur contrôle, les officiers de police judiciaire de l'IBPT sont amenés à prendre

machtiging voor aan de onderzoeksrechter, behalve in een naar behoren gerechtvaardigd noodgeval.

In de naar behoren gerechtvaardigde noodgevallen waarin de voorafgaande controle door de onderzoeksrechter niet mogelijk was, voert de onderzoeksrechter daarna een controle uit.

Om de verplichting van een operator om de in de artikelen 126, 126/1 en 127 bepaalde gegevens en de kopieën van identiteitsdocumenten te bewaren (onder andere gegevens en identiteitsdocumenten van gebruikers van prepaidkaarten) efficiënt te kunnen controleren, alsook zijn verplichting om de gegevens te wissen of ze anoniem te maken na afloop van de bewaringstermijn, is het absoluut noodzakelijk dat de officiers van gerechtelijke politie van het BIPT de databanken van de gecontroleerde operator waarin deze gegevens en documentafschriften opgenomen zijn, kunnen raadplegen.

De ingevoegde bepaling bevestigt de bevoegdheid van deze officiers om die toegang te eisen. In de praktijk controleren zij representatieve steekproeven van een databank.

Aangezien deze toegang het mogelijk maakt om een groot aantal persoonsgegevens van de abonnees van de operator te raadplegen, moet de raadpleging van de databank door deze officiers van gerechtelijke politie voortaan worden voorafgegaan door een toestemming vanwege de Raad van het BIPT.

Wanneer de operator weigert de raadpleging van zijn databank toe te staan aan de officieren van gerechtelijke politie ondanks de toestemming van de Raad, zal de Raad van het BIPT over de mogelijkheid beschikken om deze toegang op te leggen krachtens een administratief besluit. De niet-naleving van een besluit van de Raad van het BIPT wordt bestraft met de sancties bedoeld in artikel 21 van de onderhavige wet.

De Raad van het BIPT beoordeelt volledig onafhankelijk de opportuniteit van de uit te voeren controles, alsook de prioriteiten daaronder op basis van objectieve criteria, zoals de tijd die verlopen is sedert de vorige controle, het bestaan van aanwijzingen van inbreuken of het bestaan van antecedenten van inbreuken.

Het is evenwel niet noodzakelijk dat er verdenkingen van een inbreuk zijn opdat de Raad van het BIPT een toegang tot de databank toestaat, aangezien die controle net tot doel heeft het bestaan van eventuele inbreuken te onderzoeken en op te sporen.

Hoewel de officiers van gerechtelijke politie van het BIPT ter gelegenheid van hun controle ertoe gebracht

connaissance de données des abonnés de l'opérateur contrôlé, il convient de rappeler que l'objectif de ce contrôle est de vérifier le respect par l'opérateur de la législation et non d'enquêter sur les particuliers dont les données sont conservées.

Lorsque l'IBPT agit en tant qu'autorité de contrôle des dispositions nationales prises en application de la directive 2002/58 ("ePrivacy"), soumettre la demande d'accès envers l'opérateur qui est nécessaire pour ce contrôle à un contrôle préalable par une juridiction ou une autorité administrative indépendante reviendrait à contrôler le "contrôleur" et à s'immiscer dans la marge d'appréciation du régulateur dans l'exercice de ses missions de contrôle.

Or, l'article 15*bis*, § 3 de la directive prévoit que "Les États membres veillent à ce que l'autorité nationale compétente et, le cas échéant, d'autres organismes nationaux disposent des pouvoirs d'enquête et des ressources nécessaires, et notamment du pouvoir d'obtenir toute information pertinente dont ils pourraient avoir besoin, afin de surveiller et de contrôler le respect des dispositions nationales adoptées en application de la présente directive."

Il est essentiel que les officiers de police judiciaire puissent prendre une copie des données et documents consultés qui démontrent une infraction afin qu'une réponse puisse être apportée en cas de contestation de l'infraction. Afin de limiter le traitement de données à caractère personnel, ils ne peuvent pas garder de copie dans d'autres cas.

Afin de permettre un contrôle interne et un contrôle par le procureur général des demandes que les officiers de police judiciaire de l'IBPT adressent aux opérateurs, ces derniers tiennent un inventaire de ces demandes auprès de l'IBPT. À cet égard, il est utile de rappeler que selon le paragraphe 5 de l'article 25, les officiers de police judiciaire de l'Institut sont soumis à la surveillance du procureur général.

Art. 19 (insertion de l'article 28/1)

Afin de rendre possible le contrôle du respect des obligations prévues par les normes visées à l'article 14, paragraphe 1er, 3°, a) et g) à i), et dans le cadre des missions de l'IBPT en matière de sécurité des réseaux, les membres du personnel de l'Institut doivent parfois

worden om kennis te nemen van gegevens van de abonnees van de gecontroleerde operator, moet eraan worden herinnerd dat het doel van die controle erin bestaat om na te gaan of de operator de wetgeving naleeft en niet om een onderzoek in te stellen naar de privépersonen van wie de gegevens worden bewaard.

Wanneer het BIPT optreedt als toezichthoudende autoriteit met betrekking tot de nationale bepalingen die genomen zijn overeenkomstig Richtlijn 2002/58 ("ePrivacy"), dan zou het feit van het verzoek aan de operator om toegang die noodzakelijk is om deze controle te verrichten, voor te leggen voor een voorafgaande controle door een rechtscollege of een onafhankelijke administratieve overheid, erop neerkomen dat de "toezichthouder" wordt gecontroleerd en dat er inmenging is in de beoordelingsmarge van de regulator bij de uitoefening van zijn controleopdrachten.

Welnu, artikel 15*bis*, § 3, van de richtlijn schrijft voor: "De lidstaten zorgen ervoor dat de bevoegde nationale instantie en, in voorkomend geval, andere nationale organen over de nodige onderzoeksbevoegdheden en -middelen beschikken, met inbegrip van de bevoegdheid alle relevante informatie op te vragen die zij nodig kunnen hebben om de overeenkomstig deze richtlijn vastgestelde nationale bepalingen te monitoren en na te doen leven."

Het is van fundamenteel belang dat de officiers van gerechtelijke politie een kopie mogen nemen van de geraadpleegde gegevens en documenten die een inbreuk aantonen, opdat een antwoord kan worden gegeven in geval van betwisting van de inbreuk. Om de verwerking van persoonsgegevens te beperken, mogen ze in andere gevallen geen kopie bewaren.

Om een interne controle en een controle door de procureur-generaal mogelijk te maken van de verzoeken die de officiers van gerechtelijke politie van het BIPT aan de operatoren richten, houden deze laatste een inventaris van die verzoeken bij het BIPT bij. In dat opzicht is het nuttig eraan te herinneren dat volgens paragraaf 5 van artikel 25 de officiers van gerechtelijke politie van het Instituut onder het toezicht van de procureur-generaal staan.

Art. 19 (invoeging van artikel 28/1)

Om te kunnen controleren of de verplichtingen vastgesteld door de normen bedoeld in artikel 14, § 1, 3°, a) en g) tot i), in acht worden genomen, en in het kader van de opdrachten van het BIPT inzake netwerkbeveiliging, moeten de personeelsleden van het Instituut soms

pouvoir obtenir certaines métadonnées liées aux communications électroniques.

Lorsque ces membres du personnel n'agissent pas dans un cadre pénal, ils ne sont pas soumis à la surveillance du procureur général.

Les missions qu'ils opèrent ne relevant pas de la "filière pénale", mais bien de la filière administrative, il est donc prévu que la vérification de la nécessité la demande motivée soit réalisée par le supérieur hiérarchique, lorsque la demande concerne exclusivement des données relatives à l'utilisateur final ou à l'abonné.

Lorsque l'opérateur ne répond pas à la demande du membre du personnel, une demande similaire pourra être formulée par le Conseil de l'IBPT. Le non-respect d'une décision de l'IBPT est puni conformément à l'article 21 de la présente loi.

Lorsqu'une demande d'accès à d'autres métadonnées que les données relatives à l'utilisateur final ou l'abonné est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), une validation de la demande motivée par l'Autorité de protection des données est requise.

Comme indiqué précédemment concernant l'article 25, § 10, lorsque l'IBPT agit en tant qu'autorité de contrôle des dispositions nationales prises en application de la directive 2002/58 ("ePrivacy"), soumettre la demande d'accès envers l'opérateur qui est nécessaire pour effectuer ce contrôle à un contrôle préalable par une juridiction ou une autorité administrative indépendante reviendrait à contrôler le "contrôleur" et à s'immiscer dans la marge d'appréciation dont bénéfice l'IBPT pour l'exercice de ses contrôles.

Afin de permettre un contrôle interne des demandes que les membres du personnel de l'IBPT ou le Conseil adressent aux opérateurs, un inventaire de ces demandes sera tenu auprès de l'IBPT.

bepaalde metagegevens in verband met elektronische communicatie kunnen krijgen.

Wanneer deze personeelsleden niet in een strafrechtelijk kader optreden, zijn ze niet onderworpen aan het toezicht van de procureur-generaal.

Aangezien de opdrachten die ze uitvoeren niet tot het "strafrechtelijk systeem" behoren maar wel tot het administratieve systeem, wordt dus bepaald dat de noodzaak tot het gemotiveerd verzoek wordt geverifieerd door de hiërarchische meerdere, wanneer het verzoek uitsluitend betrekking heeft op gegevens betreffende de eindgebruiker of de abonnee.

Wanneer de operator niet antwoordt op het verzoek van het personeelslid, zal een soortgelijk verzoek geformuleerd kunnen worden door de Raad van het BIPT. De niet-naleving van een besluit van het BIPT wordt bestraft overeenkomstig artikel 21 van de onderhavige wet.

Wanneer een verzoek om toegang tot andere metagegevens dan de gegevens betreffende de eindgebruiker of de abonnee noodzakelijk is opdat het Instituut een van zijn opdrachten opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i), kan uitvoeren, is een validering van het gemotiveerd verzoek door de Gegevensbeschermingsautoriteit vereist.

Zoals eerder vermeld in verband met artikel 25, § 10, wanneer het BIPT optreedt als toezichthoudende autoriteit met betrekking tot de nationale bepalingen die genomen zijn overeenkomstig Richtlijn 2002/58 ("ePrivacy"), zou het feit van het verzoek om toegang aan de operator die noodzakelijk is om deze controle te verrichten, voor te leggen voor een voorafgaande controle door een rechtscollege of een onafhankelijke administratieve overheid, erop neerkomen dat de "toezichthouder" wordt gecontroleerd en dat er inmenging is in de beoordelingsmarge waarover het BIPT beschikt om zijn controles uit te voeren.

Om een interne controle mogelijk te maken van de verzoeken die de personeelsleden van het BIPT of de Raad aan de operatoren richten, zal bij het BIPT een inventaris van die verzoeken bijgehouden worden.

CHAPITRE 5

Modifications au Code d'instruction criminelle

Art. 20 (insertion de l'article 39*quinquies*)

Cette disposition introduit un nouvel article 39*quinquies* dans le Code d'instruction criminelle, qui permet au procureur du Roi d'ordonner, lors de la recherche de crimes et délits, la conservation de certaines données de trafic et de localisation pour les besoins de l'enquête.

Suite à l'arrêt de la Cour constitutionnelle n° 57/2021 du 22 avril 2021, il n'existe plus d'obligation de conservation générale et indifférenciée de toutes les données de trafic et de localisation à des fins de recherche et de poursuite d'infractions pénales.

Or, ces données jouent un rôle de plus en plus essentiel dans les enquêtes pénales, ce qui s'explique par l'utilisation croissante des nouvelles technologies. Par exemple, l'accès aux données de communication est une étape incontournable pour identifier des personnes et les liens entre celles-ci.

Les données de communication sont souvent nécessaires pour la recherche et la poursuite d'une grande variété d'infractions comme le terrorisme, la pédopornographie, le trafic de stupéfiants, le harcèlement, le piratage de comptes bancaires, le vol d'identité, les incitations à la haine ou à la violence, … (Doc. Parl., Chambre, n° DOC 54 1567/001, p. 5-6).

Sans la conservation généralisée et indifférenciée de ces données, de nombreuses données pourraient ne pas être disponibles, ce qui pourrait être extrêmement dommageable dans certaines enquêtes, où des éléments de preuves qui pourraient s'avérer essentiels seront dès lors perdus.

C'est dans cette optique que le nouvel article 39*quinquies* vient en complément, dans le cadre spécifique de la recherche de délits et de crimes, d'autres mesures de conservation des données de trafic et de localisation, telles que la conservation ciblée préventive de données afférentes à certaines zones géographiques.

Bien que cette nouvelle mesure ne permette pas de remonter dans le passé puisqu'elle intervient dans le cadre d'une enquête spécifique, l'alinéa 1er du paragraphe 1 de l'article 39*quinquies* permet néanmoins au procureur du Roi d'ordonner, dans certaines conditions et selon certaines modalités, aux opérateurs la conservation de

HOOFDSTUK 5

Wijzigingen aan het Wetboek van strafvordering

Art. 20 (invoeging van artikel 39*quinquies*)

Deze bepaling voert een nieuw artikel 39*quinquies* in het Wetboek van Strafvordering in, op grond waarvan de procureur des Konings de bewaring van bepaalde verkeers- en locatiegegevens kan bevelen tijdens het onderzoek van misdaden en wanbedrijven.

Ten gevolge van het arrest nr. 57/2021 van het Grondwettelijk Hof van 22 april 2021, bestaat er niet langer een algemene en ongedifferentieerde verplichting om alle verkeers- en locatiegegevens te bewaren met het oog op de opsporing en de vervolging van strafbare fei ten.

Deze gegevens spelen echter een steeds essentiëlere rol in strafrechtelijke onderzoeken, hetgeen te wijten is aan het toenemend gebruik van nieuwe technologieën. Zo is toegang tot communicatiegegevens een essentiële stap bij het identificeren van personen en de banden tussen hen.

Communicatiegegevens zijn vaak noodzakelijk voor het onderzoek naar en de vervolging van een breed scala van strafbare feiten, zoals terrorisme, kinderpornografie, drugshandel, belaging, hacken van bankrekeningen, identiteitsdiefstal, aanzetten tot haat of geweld, … (Parl. St., Kamer, nr. DOC 54 1567/001, blz. 5-6).

Zonder de algemene en ongedifferentieerde bewaring van dergelijke gegevens is het mogelijk dat vele gegevens niet beschikbaar zijn, hetgeen in sommige onderzoeken uiterst schadelijk kan zijn, omdat potentieel essentieel bewijsmateriaal verloren zal gaan.

In deze optiek vormt het nieuwe artikel 39*quinquies*, in de specifieke context van het onderzoek naar wanbedrijven en misdaden, een aanvulling op andere maatregelen voor de bewaring van verkeers- en locatiegegevens, zoals de gerichte preventieve bewaring van gegevens betreffende bepaalde geografische gebieden.

Hoewel met deze nieuwe maatregel niet naar het verleden kan worden teruggegrepen, aangezien deze in het kader van een specifiek onderzoek wordt toegepast, kan de procureur des Konings op grond van artikel 39*quinquies*, § 1, eerste lid, onder bepaalde voorwaarden en volgens bepaalde procedures, de bewaring bevelen van

certaines données qui pourraient être essentielles pour les besoins de l'enquête.

Une de ces conditions est que cette mesure ne peut être prise que s'il existe des indices sérieux que les infractions puissent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde.

Ainsi, le gouvernement veut s'assurer que cette mesure ne s'applique que dans le cadre de la recherche et de la poursuite d'infractions d'une certaine gravité.

Puis, l'obligation de conservation ne concerne que les données de trafic et de localisation visées à l'article 88*bis*, § 1er, alinéa 1er du Code d'instruction criminelle, soit:

"1° les données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;"

"2° les données de localisation de l'origine ou de la destination de communications électroniques."

Le procureur du Roi doit limiter son réquisitoire aux seules données qui sont susceptibles de contribuer à l'élucidation de l'infraction.

Enfin, la décision doit être écrite et motivée.

L'alinéa 2 du paragraphe 1er détermine les acteurs qui peuvent, sur ordre du procureur du Roi, directement ou par l'intermédiaire d'un service de police désigné par le Roi, être obligés de conserver les données.

Ces acteurs sont tout opérateur d'un réseau de communications électroniques, ainsi que toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques.

Cette définition est prise de l'arrêt Yahoo (arrêt de la Cour de cassation du 18/01/2011). À l'instar des articles 46*bis*, 88*bis*, 90*quater*, 464/13 et 464/25 du Code d'instruction criminelle qui reprennent cette définition, il est ajouté dans un souci de clarté "Est également compris le fournisseur d'un service de communications électroniques."

bepaalde gegevens die van essentieel belang kunnen zijn voor het onderzoek.

Een van deze voorwaarden is dat de maatregel enkel genomen kan worden als er sterke aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben.

Zo wil de regering ervoor zorgen dat deze maatregel alleen geldt voor de opsporing en vervolging van strafbare feiten van een zekere ernst.

Vervolgens heeft de verplichting tot bewaring slechts betrekking op de verkeers- en locatiegegevens bedoeld in artikel 88*bis*, § 1, eerste lid, van het Wetboek van Strafvordering, dat wil zeggen:

"1° de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;"

"2° de gegevens betreffende de oorsprong of de bestemming van elektronische communicatie."

De procureur des Konings moet zijn vordering beperken tot enkel die gegevens die kunnen bijdragen tot de opheldering van het strafbare feit.

Ten slotte moet de beslissing schriftelijk en met redenen omkleed zijn.

Het tweede lid van de eerste paragraaf bepaalt welke actoren door de procureur des Konings, rechtstreeks of door tussenkomst van een door de Koning aangewezen politiedienst, kunnen worden gevorderd de gegevens te bewaren.

Deze actoren zijn elke operator van een elektronisch communicatienetwerk, alsmede iedereen die binnen het Belgische grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt die bestaat in het overbrengen van signalen via elektronische communicatienetwerken of er in bestaat gebruikers toe te laten om informatie te verkrijgen, te ontvangen of te verspreiden via een elektronisch communicatienetwerk.

Deze definitie is overgenomen uit het Yahoo-arrest (arrest van het Hof van Cassatie van 18/01/2011). Naar het voorbeeld van de artikelen 46*bis*, 88*bis*, 90*quater*, 464/13 en 464/25 van het wetboek van strafvordering, waarin deze definitie is opgenomen, wordt omwille van de duidelijkheid het volgende toegevoegd: ""Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen"."

L'alinéa 3 du premier paragraphe énonce les mentions qui doivent figurer dans la décision du procureur du Roi.

Ces mentions sont inspirées de l'article 39*ter* du CIC.

Il est à noter que la décision doit indiquer précisément la ou les personnes, le(s) lieu(x) ou les moyens de communications qui font l'objet de la conservation. La mesure ne concerne pas seulement les données afférentes au suspect, il peut s'agir de données afférentes à la victime, à son entourage social ou professionnel, à des lieux déterminés, telles que les lieux de la commission et/ou de la préparation de l'infraction, ou encore à des moyens de communication.

Le procureur pourrait par exemple ordonner la mesure pour un périmètre autour de la maison où il y a eu un meurtre, ainsi que pour les personnes qui connaissaient la victime.

Ou, il est constaté qu'un gang de motards faisant l'objet d'une enquête pénale a déplacé le club-house dans un lieu ne relevant pas du champ d'application de l'article 126/1 de la loi relative aux communications électroniques et qu'il y a donc un risque qu'il n'y ait pas de données de communication disponibles si jamais on en a besoin dans le cadre de l'enquête. À ce moment-là, le Procureur du Roi pourrait ordonner la mesure de conservation ciblée pour un périmètre autour de ce club-house.

Il peut aussi s'agir de données recueillies par les services de police dans le cadre d'une information en cours indiquant qu'un enlèvement est projeté par une bande à l'encontre d'un mineur et dont la police a reçu via un indicateur un numéro de téléphone d'un auteur probable. À l'aide de cet unique numéro, et sur la base de la conservation ciblée, en examinant les données de trafic et de localisation, on pourra essayer de déterminer les personnes actives dans cette bande pour *in fine* empêcher cet enlèvement.

Le cas échéant, le procureur du Roi peut également indiquer dans sa décision pour quelles données ou catégories de données il demande la conservation ciblée. De cette manière, le magistrat peut limiter très clairement et spécifiquement la portée de sa décision, également en la combinant avec une ou plusieurs des personnes, moyens de communication ou lieux visés mentionnés ci-dessus. Un procureur du Roi pourrait décider qu'il ne souhaite demander que la conservation de données de localisation, et donc pas de données relatives au trafic. Il peut aussi se limiter aux données générées par les

In het derde lid van de eerste paragraaf wordt bepaald welke vermeldingen in de beslissing van de procureur des Konings moeten worden opgenomen.

Deze vermeldingen zijn gebaseerd op artikel 39*ter* van het W.Sv.

Er moet op gewezen worden dat in de beslissing specifiek moet worden aangegeven op welke perso(o)n(en), plaats(en) of communicatiemiddel(en) de bewaring betrekking heeft. De maatregel heeft niet alleen betrekking op gegevens betreffende de verdachte, maar kan ook gegevens omvatten betreffende het slachtoffer, diens sociale of professionele kring, specifieke plaatsen, zoals de plaatsen waar het strafbare feit is gepleegd en/of voorbereid, of communicatiemiddelen.

De procureur zou bijvoorbeeld de maatregel kunnen gelasten voor een perimeter rond het huis waar een moord heeft plaatsgevonden, alsook voor mensen die het slachtoffer hebben gekend.

Of er wordt vastgesteld dat een motorbende tegen wie een strafrechtelijk onderzoek loopt, het clubhuis heeft verplaatst naar een locatie die buiten de werkingssfeer valt van artikel 126/1 van de wet betreffende de elektronische communicatie en dat er dus een risico bestaat dat de communicatiegegevens niet beschikbaar zullen zijn als zij ooit nodig zijn voor het onderzoek. Op dat moment kon de procureur des Konings opdracht geven tot de gerichte bewaringsmaatregel voor een perimeter rond dit clubhuis.

Het kunnen ook gegevens zijn die door politiediensten worden verzameld in het kader van een lopend opsporingsonderzoek waaruit blijkt dat een bende een ontvoering van een minderjarige beraamt en waarbij de politie via een informant een telefoonnummer heeft gekregen van een vermoedelijke dader. Met behulp van dit ene nummer, en op basis van gerichte retentie, door het onderzoeken van de verkeers- en locatiegegevens, zal kunnen worden getracht de personen die actief zijn in deze bende te bepalen, om uiteindelijk deze ontvoering te voorkomen.

In voorkomend geval kan de procureur des Konings in zijn beslissing ook aanduiden voor welke gegevens of categorieën van gegevens hij de gerichte bewaring vraagt. Op die manier kan de magistraat heel duidelijk en gericht de draagwijdte van zijn beslissing begrenzen, ook door de combinatie met een of meerdere van de hoger vermelde beoogde personen, communicatiemiddelen of plaatsen. Een procureur des Konings zou kunnen beslissen dat hij enkel de bewaring vraagt van locatiegegevens, en dus niet van verkeersgegevens. Of hij kan zich beperken tot de gegevens die gegenereerd

pylônes qui assurent la couverture du trajet entre la résidence d'une cible et un hangar.

Le procureur du Roi pourra donc demander une conservation bien circonscrite en définissant précisément dans sa décision les personnes, les moyens de communication, les lieux et/ou les catégories de données auxquels sa décision s'applique.

La durée de la conservation des données est de 6 mois, renouvelable.

La durée de la mesure elle-même, c'est-à-dire la période pendant laquelle les opérateurs sont tenus de conserver les données, est de deux mois au maximum, sans préjudice d'un éventuel renouvellement de la mesure. Ce délai est conforme à ce qui est déjà prévu à l'article 88*bis*, § 1, alinéa 5 du code de procédure pénale. Ce délai doit également être mentionné dans la décision du procureur du Roi.

L'alinéa 4 du paragraphe 1er prévoit la possibilité, en cas d'urgence, d'ordonner verbalement la conservation des données. Dans ce cas, l'ordre doit être confirmé dans les plus brefs délais. Cette possibilité existe pour plusieurs mesures d'enquête – voir entre autres les articles 39*ter*, 46*bis*, 88*bis*. Dans ces articles, il est toujours mentionné que la confirmation écrite doit être donnée dans les plus brefs délais, sans préciser un délai concret. Dans la pratique, ces confirmations écrites ont lieu très rapidement, bien qu'il faille également tenir compte des week-ends, des jours fériés et des congés ainsi que des possibilités technologiques dont dispose le ministère public.

Le paragraphe 2 requiert des opérateurs qu'ils conservent les données de manière sécurisée. À ce moment, les autorités judiciaires n'ont pas encore accès aux données. Le but de la mesure est justement de préserver les données pour que les autorités puissent y avoir accès ensuite par le biais de l'article 88*bis* du CIC. Ce paragraphe est repris en partie de l'article 39*ter*, § 2 du CIC.

Le paragraphe 3, alinéa 1 impose une obligation de confidentialité à toute personne qui a connaissance de la mesure. Cette obligation répond à un double objectif. D'une part, elle tient compte du bon déroulement de l'enquête. Il peut être important, surtout dans le cadre de l'information, que le suspect n'ait pas connaissance de l'enquête dont il est l'objet. Puis, la confidentialité permet également d'éviter que des personnes tentent de manipuler ou d'effacer des données. D'autre part, la confidentialité de la mesure permet de contribuer à

worden door zendmasten die dekking geven aan het traject tussen de woonplaats van een target en een loods.

De procureur des Konings zal dus een zeer goed omschreven bewaring kunnen vragen door in zijn beslissing precies te omschrijven op welke personen, communicatiemiddelen, plaatsen en/of categorieën van gegevens zijn beslissing van toepassing is.

De duur van de bewaring van deze gegevens bedraagt 6 maanden, met mogelijkheid tot verlenging.

De duur van de maatregel zelf, dat wil zeggen de tijdspanne gedurende dewelke de operatoren verplicht zijn de gegevens te bewaren, is maximum twee maanden, onverminderd een mogelijke hernieuwing van de maatregel. Deze termijn sluit aan bij wat al bepaald is in artikel 88*bis*, § 1, vijfde lid van het Wetboek van strafvordering. Deze termijn moet ook vermeld worden in de beslissing van de procureur des Konings.

De vierde alinea van de eerste paragraaf voorziet in de mogelijkheid om in dringende gevallen een mondeling bevel tot bewaring van gegevens te geven. In dat geval moet de vordering zo spoedig mogelijk worden bevestigd. Deze mogelijkheid bestaat voor verscheidene onderzoeksmaatregelen – zie onder meer de artikelen 39 ter, 46 bis, 88*bis*. In die artikelen wordt telkens vermeld dat de schriftelijke bevestiging zo spoedig mogelijk dient te gebeuren, zonder daarbij een termijn te voorzien. In de praktijk gebeuren dergelijke schriftelijke bevestigingen zeer snel, al dient men hierbij ook rekening te houden met weekend-, feest-, en verlofdagen en met de technologische mogelijkheden waarover het openbaar ministerie beschikt.

De tweede paragraaf schrijft voor dat operatoren gegevens veilig moeten opslaan. Op dit ogenblik hebben de gerechtelijke autoriteiten nog geen toegang tot de gegevens. Het doel van de maatregel is juist om de gegevens te bewaren zodat de autoriteiten er later toegang toe kunnen krijgen op grond van artikel 88*bis* van het W. Sv. Deze paragraaf is gedeeltelijk overgenomen uit artikel 39*ter*, § 2, van het W. Sv.

Het eerste lid van de derde paragraaf legt aan eenieder die van de maatregel kennis heeft, een geheimhoudingsplicht op. Deze verplichting dient een tweeledig doel. Enerzijds wordt rekening gehouden met het goede verloop van het onderzoek. Het kan van belang zijn, met name in het kader van het opsporingsonderzoek, dat de verdachte geen kennis heeft van het tegen hem ingestelde onderzoek. Ten tweede helpt vertrouwelijkheid ook om te voorkomen dat mensen proberen gegevens te manipuleren of te wissen. Anderzijds draagt de vertrouwelijkheid

défendre le droit à la vie privée des personnes pouvant être concernées par ces données.

L'alinéa 2 punit le refus de collaboration, ainsi que le fait d'altérer, de détruire ou de faire disparaitre des données.

Le paragraphe 3 est notamment repris des articles 46*bis* et 88*bis* qui imposent aussi une obligation de coopération aux opérateurs.

Enfin, le paragraphe 4 limite l'accès aux données conservées. Elles ne peuvent être transmises aux autorités judiciaires que par le biais de la mesure prévue à l'article 88*bis* du Code d'instruction criminelle. Il faut donc l'intervention d'un juge d'instruction, et les infractions doivent être de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde. En limitant ainsi l'accès à ces données, le législateur veut éviter tout risque d'abus et d'accès illicite. L'accès à ces données est dès lors justifié par l'objectif d'intérêt général pour lequel la conservation a été imposée, soit la recherche, la poursuite et la sanction d'infractions pénales graves.

Bien que cette mesure ne soit pas spécifiquement reprise comme piste de solution par la Cour de Justice de l'Union européenne, cette dernière a jugé dans son arrêt qu'il est loisible pour les états d'implémenter, sous certaines conditions, des modalités de conservations ciblées comme la conservation ciblée préventive et la conservation rapide.

Concernant la conservation ciblée à titre préventif, la Cour indique au point 147 de l'arrêt du 06.10.20:

"l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire."

van de maatregel bij tot de bescherming van het recht op privacy van personen die door de gegevens kunnen betrokken zijn.

Het tweede lid bestraft de weigering om mee te werken, alsmede de wijziging, de vernietiging of het doen verdwijnen van gegevens.

De derde paragraaf is overgenomen uit de artikelen 46*bis* en 88*bis*, die de operatoren eveneens een verplichting tot medewerking opleggen.

Ten slotte wordt in de vierde paragraaf de toegang tot overeenkomstig dit artikel bewaarde gegevens beperkt. Zij kunnen alleen aan de gerechtelijke autoriteiten worden overgemaakt door middel van de maatregel voorzien in artikel 88*bis* van het Wetboek van Strafvordering. Hiervoor is de tussenkomst van een onderzoeksrechter vereist, en de strafbare feiten moeten van dien aard zijn dat zij aanleiding kunnen geven tot een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf. Door de toegang tot dergelijke gegevens op deze manier te beperken, wil de wetgever elk risico op misbruik en ongeoorloofde toegang vermijden. De toegang tot deze gegevens wordt derhalve gerechtvaardigd door het doel van algemeen belang waarvoor de bewaring is opgelegd, namelijk het onderzoeken, vervolgen en bestraffen van ernstige strafbare feiten.

Hoewel deze maatregel door het Hof van Justitie van de Europese Unie niet specifiek als mogelijke oplossing wordt genoemd, heeft het Hof in zijn arrest geoordeeld dat het de lidstaten onder bepaalde voorwaarden is toegestaan om gerichte bewaringsmethoden toe te passen, zoals preventieve gerichte bewaring en snelle bewaring.

Wat de preventieve gerichte bewaring betreft, verklaart het Hof in punt 147 van zijn arrest van 6 oktober 2020 dat:

"Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt".

La délimitation d'une telle mesure pourrait par exemple être fondée en fonction de catégories de personnes ou sur un critère géographique.

L'article 39*quinquies* diffère d'une telle réglementation de conservation ciblée de données en ce que l'ordre de conservation du procureur du Roi interviendra en principe à titre réactif et de manière circonscrite.

La conservation rapide (ou le "*quick freeze*") de données est une mesure "qui doit être prise rapidement afin de conserver les données chez la personne même (ou la personne morale) qui les détient pour éviter qu'elles ne soient endommagées ou perdues." (Doc. Parl., DOC 54 1966/001, p. 26). Les données qui font l'objet de la mesure existent et sont déjà stockées.

Cette mesure de "*quick freeze*" pour le passé existe dans notre législation à l'article 39*ter* du CIC, inséré par la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales et modifié par la loi du 5 mai 2019. Il matérialise la transposition des articles 16 et 17 de la Convention de Budapest sur la criminalité informatique.

L'article 39*quinquies* diffère notamment de l'article 39*ter* CIC en ce que les données ne sont pas encore collectées et stockées. Dès réception de l'ordre, les opérateurs doivent conserver les données demandées qu'ils génèrent. Il s'agit ici donc plutôt d'un "*quick freeze*" pour le futur.

La Cour de Justice estime au paragraphe 163 de l'arrêt du 6 octobre 2020 que les États membres peuvent prévoir dans leur législation la possibilité d'enjoindre aux fournisseurs de services de communications électroniques de procéder, sous certaines conditions, à la conservation rapide des données relatives au trafic et des données de localisation. Les conditions auxquelles cette mesure doit être subordonnée sont reprises aux points 163 à 165 de l'arrêt:

— décision de l'autorité compétente doit être soumise à un contrôle juridictionnel effectif;

— inscription dans la législation de la finalité pour laquelle la conservation rapide des données peut avoir lieu;

De afbakening van een dergelijke maatregel kan bijvoorbeeld gebaseerd zijn op categorieën van personen of op een geografisch criterium.

Artikel 39*quinquies* verschilt van dergelijke gerichte gegevensbewaringsregelgeving in die zin dat het bevel tot bewaring van de procureur des Konings in principe reactief en specifiek zal zijn.

De snelle bevriezing van gegevens ("*quick freeze*") is een maatregel "*die snel genomen moet worden om de gegevens in de schoot zelf van de persoon die ze onder zich houdt, te bewaren om te voorkomen dat ze beschadigd geraken of verloren gaan*." (Parl. Doc., DOC 54 1966/001, blz. 26). De gegevens waarop de maatregel betrekking heeft, bestaan en zijn reeds opgeslagen.

Deze "*quick freeze*"-maatregel voor het verleden bestaat in onze wetgeving in artikel 39*ter* W. Sv., ingevoegd bij de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische communicatie en telecommunicatie en tot oprichting van een gegevensbank stemafdrukken, en gewijzigd bij de wet van 5 mei 2019. Het behelst de omzetting van de artikelen 16 en 17 van het Verdrag van Boedapest inzake informaticacriminaliteit.

Artikel 39*quinquies* verschilt van artikel 39*ter* in die zin dat de gegevens nog niet verzameld en opgeslagen zijn. Vanaf de ontvangst van de vordering moeten de operatoren de gevraagde gegevens die zij genereren, bewaren. Dit is dus meer een "snelle bevriezing" voor de toekomst.

Het Hof van Justitie overweegt in punt 163 van het arrest van 6 oktober 2020 dat de lidstaten in hun wetgeving kunnen voorzien in de mogelijkheid om van de aanbieders van elektronische-communicatiediensten te verlangen dat zij onder bepaalde voorwaarden overgaan tot de snelle bewaring van verkeers- en locatiegegevens. De voorwaarden waaraan deze maatregel moet voldoen, zijn uiteengezet in de punten 163 tot en met 165 van het arrest:

— het besluit van de bevoegde autoriteit is onderworpen aan effectieve rechterlijke toetsing;

— inschrijving in de wetgeving van het doel waarvoor de snelle opslag van gegevens mag geschieden;

— limitation à la seule la lutte contre la criminalité grave et, *a fortiori*, la sauvegarde de la sécurité nationale;

— conservation des seules données de trafic et de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. Il peut s'agir de données de trafic et de localisation "afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause" – voir paragraphe 165;

— limitation de la durée de conservation au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

Selon la jurisprudence constante de la Cour, une limitation aux droits et obligations prévus dans la directive e-privacy doit être appréciée en mesurant la gravité de l'ingérence qu'elle comporte et en vérifiant que l'importance de l'objectif d'intérêt général qu'elle poursuit est en relation avec cette gravité – voir paragraphe 131 de l'arrêt du 06.10.20).

Vu que l'ingérence que comporte l'obligation de conservation ciblée prévue à l'article 39*quinquies* est assez similaire à celle que comporte une conservation rapide pour un même objectif, il peut être considéré qu'un tel article satisfait à l'exigence de proportionnalité requise si les modalités procédurales et matérielles déterminées par la Cour pour la conservation rapide sont respectées.

Or, l'article 39*quinquies* prévoit de telles modalités et conditions:

La finalité y est spécifiquement précisée, soit la recherche et la poursuite d'infractions qui sont de nature à entraîner un emprisonnement correctionnel d'un an ou une peine plus lourde;

— beperkt tot de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid;

— het bewaren van alleen die verkeers- en locatiegegevens die kunnen bijdragen tot het ophelderen van het betrokken ernstige strafbare feit of de betrokken inbreuk op de nationale veiligheid. Dit kan verkeers- en locatiegegevens omvatten "die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd" – zie paragraaf 165;

— beperking van de bewaringstermijn tot het strikt noodzakelijke, met dien verstande dat deze termijn kan worden verlengd indien de omstandigheden en het met de maatregel nagestreefde doel zulks rechtvaardigen.

Volgens vaste rechtspraak van het Hof moet een beperking van de in de e-privacyrichtlijn vastgestelde rechten en plichten worden beoordeeld door de ernst te meten van de inmenging die zij meebrengt, en door na te gaan of het belang van de doelstelling van algemeen belang die zij nastreeft, in verhouding staat tot die ernst – zie punt 131 van het arrest van het Hof van Justitie in zaak C-105/99 (zie punt 131 van het arrest van 06.10.20).

Aangezien de inmenging die de verplichting tot gerichte bewaring uit hoofde van artikel 39*quinquies* met zich meebrengt, sterk gelijkt op die welke een snelle bewaring met hetzelfde doel meebrengt, kan een dergelijk artikel worden geacht aan het evenredigheidsvereiste te voldoen indien de door het Hof voor snelle bewaring vastgestelde voorwaarden en modaliteiten in acht worden genomen.

Artikel 39*quinquies* voorziet in deze vooraarden en modaliteiten:

Het doel wordt specifiek omschreven, namelijk het onderzoeken en vervolgen van strafbare feiten die aanleiding kunnen geven tot een correctionele gevangenisstraf van één jaar of een zwaardere straf;

La durée de conservation est limitée au strict nécessaire;

Les données qui peuvent faire l'objet de la mesure sont uniquement celles qui sont susceptibles d'élucider une infraction;

Comme tout acte d'enquête, la mesure est soumise à un contrôle juridictionnel effectif.

Art. 21 (modification à l'article 88*bis*)

Par son arrêt du 22 avril 2021, la Cour Constitutionnelle a annulé la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, en ce compris l'article 9 f) qui a remplacé le § 2 de l'article 88*bis* et l'article 9 g) qui a inséré le § 3 du même article.

Or, ces paragraphes renforçaient notamment les garanties au niveau de l'accès aux données de trafic et de localisation.

Suite à l'annulation, il convient de réajuster l'article 88*bis* en conséquence et de réintroduire certaines garanties.

Le point 1° de l'article 21 réintègre l'ancien § 2 concernant l'accès aux données qui sont conservées sur la base de l'ancien article 126 de la loi relative aux communications électroniques. Bien sûr, il est désormais fait référence à l'article 126/1 de cette loi, qui est l'article de base relatif à la conservation des données de trafic et de localisation. Pour plus d'explications sur l'accès différencié aux données conservées, il convient de se référer à l'exposé des motifs de la loi du 29 mai 2016 (Doc. Parl., Chambre, DOC 54 1567/001, p. 42-43).

Le point 2° de l'article 21 réintègre l'ancien § 3 qui protège les données de communication des médecins et des avocats. La mesure ne peut porter sur leurs moyens de communication électronique que dans la cadre de certaines situations très spécifiques. Ce paragraphe est une reprise des articles 39*bis*, § 9, 56*bis*, 88*bis*, § 3 et 90*octies* CIC.

Il convient de noter que la terminologie utilisée dans l'article 88*bis* ne change pas, alors que c'est le cas dans la loi relative aux communications électroniques. Par exemple, la notion "métadonnées" y est utilisé. Le législateur rappelle que le droit pénal est autonome: lors de l'interprétation de lois pénales et de leur application, les juridictions pénales peuvent donner un sens ou une

De duur van de bewaring is beperkt tot wat strikt noodzakelijk is;

De maatregel kan alleen worden toegepast op gegevens die een strafbaar feit aan het licht kunnen brengen;

Zoals bij elk onderzoekshandeling is de maatregel onderworpen aan effectieve rechterlijke toetsing.

Art. 21 (wijziging aan artikel 88*bis*)

Bij het arrest van 22 april 2021 heeft het Grondwettelijk Hof de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van gegevens in de sector van de elektronische communicatie vernietigd, met inbegrip van artikel 9, onder f), dat § 2 van artikel 88 bis heeft vervangen, en artikel 9, onder g), dat § 3 van datzelfde artikel heeft ingevoegd.

Deze paragrafen versterkten echter onder meer de waarborgen voor de toegang tot verkeers- en locatiegegevens.

Na de nietigverklaring moet artikel 88*bis* dienovereenkomstig worden aangepast en moeten bepaalde waarborgen opnieuw worden ingevoerd.

In het 1° van artikel 21 wordt de vroegere paragraaf 2, betreffende de toegang tot de gegevens die bewaard worden krachtens het vroegere artikel 126 van de wet betreffende de elektronische communicatie, opnieuw opgenomen. Uiteraard wordt er nu wel verwezen naar artikel 126/1 van die wet, het basisartikel in verband met de bewaring van verkeers- en lokalisatiegegevens. Voor meer uitleg over de gedifferentieerde toegang tot de bewaarde gegevens kan verwezen worden naar de memorie van toelichting bij de wet van 29 mei 2016 (Parl. St., Kamer, DOC 54 1567/001, blz. 42-43).

In het 2° van artikel 21 wordt de vroegere paragraaf 3, dat de communicatiegegevens van artsen en advocaten beschermt, opnieuw opgenomen. De maatregel kan alleen betrekking hebben op hun elektronische communicatiemiddelen in bepaalde zeer specifieke situaties. Deze paragraaf is een herhaling van de artikelen 39*bis*, § 9, 56*bis*, 88*bis*, § 3 en 90*octies* W. Sv.

Er dient op gewezen te worden dat de terminologie die gebruikt wordt in artikel 88*bis* niet wijzigt, hoewel dit wel het geval is in de wet betreffende de elektronische communicatie. Zo wordt daar bijvoorbeeld de term "metagegevens" gebruikt. De wetgever wijst erop dat het strafrecht autonoom is: de strafrechter mag bij de interpretatie van de strafwetten en hun toepassing aan

portée propre à des concepts provenant d'autres branches du droit ou d'autres lois (autonomie conceptuelle du droit pénal). Par exemple, le concept d'"opérateur" dans le code d'instruction criminelle n'était pas le même que celui qui était alors utilisé dans la LCE, mais le concept a été étoffé par la jurisprudence dite "Yahoo". Il en va donc de même pour les concepts utilisés ici.

Il n'y a donc pas de définition des données relatives au trafic et des données de localisation dans le Code d'instruction criminelle. Cela ne correspond pas à notre tradition juridique, et ça pourrait d'ailleurs avoir un effet contreproductif. La terminologie employée se veut particulièrement neutre du point de vue technologique afin d'éviter que les concepts soient trop rapidement dépassés par l'évolution de la technologie de l'information (voir l'exposé des motifs de la loi sur la criminalité informatique, Doc. Parl., DOC 50 0213/001, p. 12). Ainsi, la manière dont les termes "communication", "données de trafic", "données de connexion", "métadonnées" et autres concepts sont définis dans la LCE est en soi sans importance pour l'application des articles du Code d'instruction criminelle.

CHAPITRE 6

Modifications a la loi du 5 août 1992 sur la fonction de police

Art. 22 (modification à l'article 42)

L'article 22 introduit deux nouveaux paragraphes dans l'article 42 de la loi sur la fonction de police qui régit spécifiquement l'accès par la Cellule personnes disparues de la Police Fédérale à certaines données de communication.

Ces nouveaux paragraphes reprennent en grande partie la compétence déjà existante de la Cellule, prévue à l'article 126, § 2, 5° de la loi relatives aux communications électroniques, remplacé par la loi du 29 mai 2016 et annulé par la Cour Constitutionnelle.

Déjà en 2016, le législateur estimait qu'il était important de permettre à la Cellule des personnes disparues de la Police Fédérale de pouvoir directement demander l'accès de certaines données aux opérateurs: "Il n'est pas approprié d'obliger la cellule de disparition de la police fédérale à solliciter un réquisitoire d'un procureur du Roi ou d'un juge d'instruction pour obtenir des données conservées par l'opérateur ou le fournisseur en vertu du présent article, lorsque la disparition inquiétante n'est pas le fait d'une infraction pénale (fugue, tentative de

begrippen die afkomstig zijn uit andere rechtstakken of andere wetten een eigen betekenis of draagwijdte geven (conceptuele autonomie van het strafrecht). Zo was het begrip "operator" in het Wetboek van strafvordering niet hetzelfde als het begrip dat destijds gebruikt werd in de WEC, maar werd het begrip ingevuld door de zogenaamde Yahoo-rechtspraak. Hetzelfde geldt dus voor de hier gehanteerde begrippen.

Er zijn dus geen definities van verkeersgegevens en lokalisatiegegevens in het Wetboek van Strafvordering. Dit past niet in onze juridische traditie en zou overigens contraproductief zijn. De gehanteerde terminologie beoogt in het bijzonder technologie-neutraal te zijn, om aldus te vermijden dat de concepten al te snel achterhaald worden door de evolutie van de informatietechnologie (zie memorie van toelichting bij de wet op de informaticacriminaliteit, Parl. St. DOC 50 0213/001, blz. 12). Hoe de termen "communicatie", "verkeersgegevens", "connectiegegevens", "metagegevens" en andere begrippen dus gedefinieerd worden in de WEC, is op zich van geen belang voor de toepassing van de artikelen in het Wetboek van strafvordering.

HOOFDSTUK 6

Wijzigingen aan de wet van 5 augustus 1992 op het politieambt

Art. 22 (wijziging aan artikel 42)

Artikel 22 voert twee nieuwe paragraven in bij het artikel 42 van de Wet op het politieambt over het verzamelen van gegevens met betrekking tot elektronische communicatie door de Cel Vermiste Personen van de federale politie.

Deze nieuwe paragraven nemen de al bestaande bevoegdheid van de Cel voorzien in artikel 126, § 2, 5° van de wet betreffende de elektronische communicatie, vervangen door de wet van 29 mei 2016 en vernietigd door het Grondwettelijk Hof, grotendeels over.

Reeds in 2016 heeft de wetgever geoordeeld dat het belangrijk was om de Cel Vermiste Personen van de federale politie toe te laten om aan de operatoren direct toegang te vragen tot bepaalde gegevens: "Het is niet gepast om de cel Vermiste Personen van de federale politie te verplichten een requisitoir van een procureur des Konings of van een onderzoeksrechter te vragen om gegevens te krijgen die door de operator of de aanbieder worden bewaard krachtens het onderhavige artikel, wanneer de onrustwekkende verdwijning niets

suicide, etc.). Le paragraphe deux prévoit dès lors que l'officier de police judiciaire de la cellule disparition peut obtenir certaines données conservées de l'opérateur ou du fournisseur par l'intermédiaire d'un service de police désigné par le Roi." (Doc Parl, DOC 54 1567/001, p. 29).

L'article reprend les modalités et conditions d'accès aux données, qui sont déjà prévues à l'article 126, § 2, 5° de la loi relatives aux communications électroniques.

Suite aux arrêts de la CJUE du 6 octobre 2020 et de la Cour Constitutionnelle n° 57/2021 du 22 avril 20 21, le gouvernement a décidé d'établir les conditions matérielles et procédurales d'accès aux données dans la loi organique de la police.

À l'instar des articles 46*bis*, 88*bis*, 90*quater*, 464/13 et 464/25 du Code d'instruction criminelle, la notion "fournisseurs" est remplacée par la définition qui se trouve dans l'arrêt Yahoo (arrêt de la Cour de cassation du 18 janvier 2011): toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques.

Il y est également ajouté dans un souci de clarté "Est également compris le fournisseur d'un service de communications électroniques."

Les services réquisitionnés sont tenus de coopérer à la réquisition légale émise par l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, faute de quoi ils s'exposent à des poursuites sur la base de l'article 422*ter* Code pénal.

Dans tous les cas où une réquisition de données est faite, cette demande sera notifiée à l'Organe de contrôle.

Si l'Organe de contrôle estime que les conditions d'obtention des données n'ont pas été respectées, il peut ordonner que les données obtenues ne puissent être traitées et doivent être détruites.

Cette décision de l'Organe de contrôle sera motivée et immédiatement notifiée à la Cellule des personnes disparues.

te maken heeft met een strafbaar feit (vlucht, poging tot zelfmoord, enz.). Paragraaf twee bepaalt daarom dat de officier van gerechtelijke politie van de cel Vermiste Personen, via de door de Koning aangewezen politiedienst, bepaalde gegevens kan krijgen die worden bewaard door de operator of de aanbieder." (Parl. St., DOC 54 1567/001, blz. 29).

Het artikel bevat de modaliteiten en de voorwaarden voor de toegang tot de gegevens, zoals nu al voorzien in artikel 126, § 2, 5° van de wet betreffende de elektronische communicatie.

Naar aanleiding van de arresten van het HvJ-EU van 6 oktober 2020 en van het Grondwettelijk Hof nr. 5 7/2021 van 22 april 2021 heeft de regering besloten de materiële en procedurele voorwaarden voor toegang tot gegevens vast te leggen in de organieke wet van de politie.

Naar het voorbeeld van de artikelen 46*bis*, 88*bis*, 90*quater*, 464/13 en 464/25 van het Wetboek van Strafvordering wordt het begrip "aanbieders" vervangen door de definitie in het Yahoo-arrest (arrest van het Hof van Cassatie van 18 januari 2011): iedereen die binnen het Belgische grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt die bestaat in het overbrengen van signalen via elektronische-communicatienetwerken of er in bestaat gebruikers toe te laten informatie te verkrijgen, te ontvangen of te verspreiden via een elektronisch-communicatienetwerk.

Voor de duidelijkheid wordt ook toegevoegd: "Hieronder wordt ook de verstrekker van een elektronische-communicatiedienst begrepen."

De opgevorderde diensten zijn verplicht hun medewerking te verlenen aan de wettelijke vordering uitgevaardigd door de officier van gerechtelijke politie van de Cel Vermiste Personen van de Federale Politie, zoniet stellen zij zich open voor vervolging op grond van artikel 422*ter* Strafwetboek.

In alle gevallen waarin een vordering tot bekomen van gegevens plaatsvindt, zal deze vordering ter kennis gebracht worden van het Controleorgaan.

Wanneer het Controleorgaan van mening is dat de voorwaarden tot het bekomen van de gegevens niet werden gerespecteerd, zal zij kunnen bevelen dat de verkregen gegevens niet kunnen verwerkt worden en moeten vernietigd worden.

Deze beslissing van het Controleorgaan zal gemotiveerd zijn en onmiddellijk worden betekend aan de Cel Vermiste Personen.

CHAPITRE 7

Modifications à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 23 (modification à l'article 3)

La définition de "communications" reprise à l'article 3, 10° est modifiée afin de répondre à la nouvelle réalité technologique et ainsi préciser que les communications "*Machine-to-Machine*" relèvent de la notion de - communications- telle que visée dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (LRS).

Initialement, une définition du concept d'"opérateur" avait été insérée dans l'avant-projet. À la suite des remarques du Comité permanent R (Avis n° 003/CPR/2021 du 15 juin 2021, points 30 – 32), les auteurs ont choisi de ne pas définir le concept d'"opérateur" et de donner ainsi une interprétation autonome aux concepts d'"opérateur d'un réseau de communications électroniques" et de "fournisseur d'un service de communications électroniques". C'est d'ailleurs également le cas en droit pénal. L'objectif est que la définition soit aussi large que possible et qu'elle évolue avec les progrès technologiques. Ainsi, ce ne sont pas uniquement les acteurs traditionnels de communications électroniques qui sont visés mais aussi les fournisseurs de services de communications interpersonnelles, de services permettant la communication comme élément accessoire à l'activité principale (exemple, le chat pendant les jeux), ou les fournisseurs d'un réseau privé (par exemple, un réseau interne d'entreprise). Étant donné que les formulations existantes d'"opérateur d'un réseau de communications électroniques" et de "fournisseur d'un service de communications électroniques" sont conservées, les modifications initialement apportées aux articles 16/2, 18/7, 18/8 et 18/17 de la LRS sont abandonnées.

Art. 24 (modification à l'article 7)

Premièrement, les mots "chargée de la sécurité nationale" sont ajoutés à l'article 7 de la LRS. Cette adaptation ne modifie pas la substance des tâches du service de renseignement et de sécurité, mais vise à préciser que les missions de renseignement et de sécurité de la Sûreté de l'État sont exécutées en vue de sauvegarder la sécurité nationale.

Pour répondre à la remarque du Comité permanent R (point 3), il convient de préciser que les auteurs du

HOOFDSTUK 7

Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Art. 23 (wijziging aan artikel 3)

De definitie van "communicatie" in artikel 3, 10° wordt gewijzigd om te beantwoorden aan de nieuwe technologische realiteit zodat duidelijk is dat ook de "*Machine-to-Machine*"-communicatie valt onder hetgeen in de wet van 30 november 1998 houdende regeling van de inlichtingendiensten (WIV) bedoeld wordt met "communicatie".

In het voorontwerp werd initieel een definitie van het begrip "operator" ingevoegd. Als gevolg van de opmerkingen van het Vast Comité I (Advies nr. 003/VCI/2021 van 15 juni 2021, punten 30 – 32) hebben de auteurs ervoor gekozen om "operator" niet te definiëren en aldus een autonome invulling te geven aan de begrippen "operator van een elektronisch communicatienetwerk" en "verstrekker van een elektronische communicatiedienst". Dit is trouwens ook het geval in het strafprocesrecht. Bedoeling is dat de omschrijving zo breed mogelijk is en mee evolueert met de technologische vooruitgang. Niet alleen de traditionele actoren op het gebied van elektronische communicatie worden dus beoogd, maar ook de aanbieders van interpersoonlijke communicatiediensten, van diensten die communicatie mogelijk maken als een bijkomstig element bij de hoofdactiviteit (bijvoorbeeld chatten tijdens het gamen), of aanbieders van een privaat netwerk (bijvoorbeeld een intern bedrijfsnetwerk). Gezien de bestaande bewoording "operator van een elektronisch communicatienetwerk" en "verstrekker van een elektronische communicatiedienst" behouden blijft, vervallen de wijzigingen die initieel werden aangebracht aan de artikelen 16/2, 18/7, 18/8 en 18/17 WIV.

Art. 24 (wijziging aan artikel 7)

De woorden "belast met de nationale veiligheid" worden toegevoegd aan artikel 7 WIV. Deze aanpassing brengt geen inhoudelijke wijziging aan de opdrachten van de inlichtingen- en veiligheidsdienst met zich mee maar beoogt enkel een verduidelijking dat de inlichtingen- en veiligheidsopdrachten van de Veiligheid van de Staat plaatsvinden met het oog op de vrijwaring van de nationale veiligheid.

Als antwoord op de opmerking van het Vast Comité I (punt 3) dient erop te worden gewezen dat de auteurs

projet ont sciemment préféré les termes “chargé(e) de la sécurité nationale” plutôt que “pour la sauvegarde de la sécurité nationale” pour éviter une éventuelle diminution des compétences des services de renseignement et de sécurité.

En effet, ce n’est pas le but, par exemple, que le SGRS ne soit plus compétent pour faire du renseignement pour lutter contre une menace à l’encontre d’un intérêt militaire car la menace ne serait pas ou pourrait ne pas être considérée comme une menace contre la sécurité nationale.

Le but de cet ajout est de maintenir un statut quo par rapport aux missions des deux services mais de préciser que les deux services agissent bien dans le cadre de la sécurité nationale.

En outre, le Comité permanent R indique que la formulation proposée “laisse trop de place au doute quant à l’existence éventuelle d’autres tâches de sécurité nationale pour la VSSE et le SGRS en dehors de celles énumérées dans (ou basées sur) les articles 7 et 11 de la LRS. Ce qui n’est pas le cas.” Le Comité permanent R se trompe pourtant car les deux services de renseignement ont des missions prévues dans d’autres lois sectorielles, à commencer par la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, qui sont également des tâches de sécurité nationale.

Art. 25 (modification à l’article 11)

Les mots “chargé de la sécurité nationale” sont ajoutés à l’article 11 de la LRS définissant les missions du Service Général du Renseignement. Cela ne modifie pas la substance des missions du SGRS mais vise uniquement à préciser que ces missions se situent toutes dans le cadre de la sécurité nationale. Pour la justification, les auteurs du projet renvoient aux remarques concernant la modification de l’article 7 de la LRS.

Art. 26 (insertion de la section 3/1)

Dans le texte initial du projet, les auteurs avaient placé la disposition relative à l’obligation de conservation dans le chapitre III, section 4 de la LRS, qui traite des méthodes de recueil des données. Par le biais d’une nouvelle méthode ordinaire, les “*quick freeze*” et “future freeze” ont été introduits (nouvel article 16/2/1). Par le biais d’une nouvelle méthode exceptionnelle, les services de renseignement ont été habilités à imposer

van het ontwerp bewust hebben gekozen voor de formulering “belast met de nationale veiligheid” in plaats van “voor de bescherming van de nationale veiligheid”, om een mogelijke beperking van de bevoegdheden van de inlichtingen- en veiligheidsdiensten te voorkomen.

Het is immers niet de bedoeling dat de ADIV niet langer bevoegd zou zijn om inlichtingen te verstrekken om een bedreiging van een militair belang tegen te gaan omdat de bedreiging niet als een bedreiging van de nationale veiligheid zou worden beschouwd of zou kunnen worden beschouwd.

Doel van deze toevoeging is een status quo te handhaven met betrekking tot de opdrachten van de twee diensten, maar duidelijk te maken dat beide diensten optreden in het kader van de nationale veiligheid.

Voorts stelt het Vast Comité I dat de voorgestelde formulering te veel ruimte laat voor twijfel over de vraag of er naast de in (of op basis van) de artikelen 7 en 11 WIV genoemde taken nog andere nationale veiligheidstaken voor de VSSE en de ADIV zijn weggelegd en dat dat niet het geval is. Het Vast Comité I heeft echter ongelijk, omdat beide inlichtingendiensten taken hebben die in andere sectorale wetgeving zijn voorzien, te beginnen met de wet van 11 december 1998 inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, die ook taken van nationale veiligheid zijn.

Art. 25 (wijziging aan artikel 11)

De woorden “belast met de nationale veiligheid” worden toegevoegd aan artikel 11 WIV dat de opdrachten van de Algemene Dienst Inlichting en Veiligheid bepaalt. Deze aanpassing brengt geen substantiële wijziging aan de opdrachten van de ADIV met zich mee maar beoogt enkel een verduidelijking dat deze opdrachten zich situeren binnen het kader van de nationale veiligheid. Voor de verantwoording verwijzen de auteurs van het ontwerp naar de opmerkingen bij de wijziging aan artikel 7 WIV.

Art. 26 (invoeging van afdeling 3/1)

In de initiële tekst van het ontwerp hadden de auteurs de regeling van de bewaarplicht ingeschreven in hoofdstuk III, afdeling 4 WIV, dat de methoden voor het verzamelen van gegevens betreft. Via een nieuwe gewone methode werden de zogenaamde “*quick freeze*” en “future freeze” ingevoerd (nieuw artikel 16/2/1). Via een nieuwe uitzonderlijke methode werd aan de inlichtingendiensten de bevoegdheid toegekend om een

une obligation de conservation générale et indifférenciée (nouvel article 18/17/1).

Compte tenu des avis remis et après réflexion, les auteurs sont d'avis que l'ordre de simple conservation des données de communications électroniques ne constitue pas une exploitation des données mais est une étape préliminaire dans la procédure de collecte. Il est ainsi choisi de placer les réquisitions de conservation dans le chapitre III, sous une nouvelle section 3/1, intitulée "Les réquisitions de conservation". Cette section comprend un nouvel article 13/6 pour la conservation ciblée ("*quick freeze*" et "future freeze") et un nouvel article 13/7 pour l'obligation de conservation générale et indifférenciée.

Dès lors, on ne parle plus de "méthodes" mais de "réquisitions de conservation" et un certain nombre de modifications initialement prévues dans la LRS sont abandonnées. Partant, certaines remarques formulées par le Comité permanent R deviennent sans objet.

Les auteurs du projet soulignent que les garanties procédurales entourant cette réquisition de conservation, sont équivalentes à celles initialement prévues (c'est-à-dire celles relatives à une méthode de recueil de données). En effet, les finalités pour mettre en œuvre cette mesure de conservation restent les mêmes; et les exigences de proportionnalité et de subsidiarité sont également d'application. En outre, l'accord de la Commission est toujours nécessaire avant de pouvoir procéder à une réquisition de conservation de données généralisée et indifférenciée. De même, le Comité permanent R reste compétent pour contrôler toutes les réquisitions de conservation.

Art. 27 (insertion de l'article 13/6)

L'introduction d'une réquisition de conservation ciblée (nouvel article 13/6, article 16/2/1 dans le projet initial) fait suite à l'arrêt de la Cour de justice européenne du 6 octobre 2020, selon lequel une conservation générale et indifférenciée de données relatives au trafic et à la localisation des communications électroniques est contraire au droit européen (et notamment au droit à la vie privée). La modification de la loi vise à atteindre un meilleur équilibre entre le droit du citoyen à la vie privée, d'une part, et le devoir du gouvernement de garantir la sécurité nationale, d'autre part.

Dans son arrêt, la Cour mentionne un certain nombre de possibilités de conservation différenciée des données.

Premièrement, le dénommé "*quick freeze*", qui permet à un service de renseignement d'ordonner une

algemene en ongedifferentieerde bewaarplicht op te leggen (nieuw artikel 18/17/1).

Rekening houdende met de uitgebrachte adviezen en bij nader inzien, zijn de indieners van oordeel dat het bevel tot de loutere bewaring van elektronische communicatiegegevens, geen exploitatie van gegevens inhoudt maar een voorafgaande fase is in het collecteproces. Er wordt dan ook voor geopteerd om de vorderingen tot bewaring onder te brengen in een nieuwe afdeling 3/1 binnen hoofdstuk III, met als opschrift "De vorderingen tot bewaring". Deze afdeling omvat een nieuw artikel 13/6 voor de gerichte bewaring ("*quick freeze*" en "future freeze") en een nieuw artikel 13/7 voor de algemene en ongedifferentieerde bewaarplicht.

Dit heeft als gevolg dat er niet meer gesproken wordt over "methoden" maar over "vorderingen tot bewaring" en dat een aantal initieel geplande wijzigingen aan de WIV vervallen. Hierdoor worden ook sommige opmerkingen van het Vast Comité I zonder voorwerp.

De auteurs van het ontwerp benadrukken dat de procedurele waarborgen om een vordering tot bewaring in te stellen, evenwaardig zijn aan deze die oorspronkelijk waren voorzien (zijnde degene die gelden voor een inlichtingenmethode). De finaliteiten waarvoor deze bewaringsmaatregel afgekondigd kan worden blijven dezelfde; de proportionaliteits- en subsidiariteitsvereiste blijven van kracht. Hierbij wordt dus nog steeds vereist dat de Commissie haar akkoord moet geven alvorens een vordering tot algemene en ongedifferentieerde bewaring van gegevens kan worden uitgevoerd. Ook blijft het Vast Comité I bevoegd om alle vorderingen tot bewaring te controleren.

Art. 27 (invoeging van artikel 13/6)

De invoering van een vordering tot gerichte bewaring (nieuw artikel 13/6, in het initieel ontwerp: artikel 16/2/1) is het gevolg van de uitspraak van het Europees Hof van Justitie van 6 oktober 2020, dat stelt dat een algemene en ongedifferentieerde bewaring van verkeers- en lokalisatiegegevens van elektronische communicatie strijdig is met EU-recht (o.a het recht op privacy). De wetswijziging beoogt een beter evenwicht tussen het recht op privacy van de burger enerzijds, en de plicht van de overheid om de nationale veiligheid te garanderen, anderzijds.

In zijn arrest geeft het Hof een aantal mogelijkheden voor een gedifferentieerde dataretentie.

Vooreerst is er de zogenaamde "*quick freeze*" waarbij een inlichtingendienst een snelle bewaring kan bevelen

conservation rapide de données relatives à une cible déterminée lorsque cela s'impose pour protéger la sécurité nationale.

La Cour autorise également une conservation ciblée pour le futur ("targeted") ou "future freeze" de certaines catégories de données. Ces catégories sont définies sur la base d'éléments objectifs et non discriminatoires. Les données ainsi collectées ne peuvent être conservées plus longtemps que ce qui est strictement nécessaire.

Ces "windows of opportunity" (fenêtres d'opportunité) proposées par la Cour pour une obligation différenciée de conservation des données sont concrétisées dans un nouvel article 13/6 (initialement: 16/2/1).

L'obligation de conservation comprend deux possibilités:

1° la réquisition de conservation des données de trafic et de localisation déjà générées ("*quick freeze*"). Dans ce cas, l'opérateur est tenu de conserver les données qu'il possède déjà au moment de la réquisition. Il s'agit en l'espèce des données conservées pour des raisons techniques, ainsi qu'à des fins de facturation, de marketing, de lutte contre la fraude, de sécurité des réseaux, etc. Ces données ne sont normalement conservées que le temps nécessaire à leurs propres finalités. Cela peut varier de quelques minutes (dans le cas de données techniques volatiles) à plusieurs années (afin pouvoir contester une facture, par exemple). Dans l'intérêt des missions de renseignement, un opérateur peut être requis de "figer" et de conserver ces données (durée de conservation de maximum 6 mois, avec possibilité de prolonger). De cette façon, ce sont au moins les données historiques disponibles qui seront sécurisées.

Les données historiques sont indispensables dans le cadre d'une enquête de renseignement. Elles permettent de vérifier qui a contacté qui, par quel moyen, à quel moment et où ce contact a eu lieu. Jusqu'à l'arrêt de la Cour européenne, les services concernés n'avaient pas à s'inquiéter de la disponibilité de ces données puisque tout était conservé pendant 12 mois. La méthode spécifique de renseignement mentionnée à l'article 18/8 LRS permettait au service de renseignement concerné d'accéder aux données importantes pour l'enquête.

En raison de la jurisprudence européenne, les résultats dépendront de l'ensemble des données détenues par l'opérateur pour ses propres finalités.

2° la réquisition de conservation des données de trafic et de localisation générées à dater de la réception de la réquisition (conservation des données futures ou "future

van de gegevens over een bepaalde target wanneer dat noodzakelijk is voor de bescherming van de nationale veiligheid.

Daarnaast laat het Hof ook een gerichte ("targeted") bewaring of "future freeze" van bepaalde categorieën van gegevens toe. Deze categorieën worden bepaald op basis van objectieve en niet-discriminatoire elementen. Hierbij mogen de gegevens niet langer bewaard worden dan strikt noodzakelijk is.

Deze "windows of opportunity" die het Hof aanreikt voor een gedifferentieerde bewaarplicht, worden geconcretiseerd in een nieuw artikel 13/6 (initieel:16/2/1).

De bewaarplicht behelst twee mogelijkheden:

1° de vordering tot bewaring van reeds gegenereerde verkeers- en lokalisatiegegevens ("*quick freeze*"). Met deze vordering wordt de operator bevolen gegevens te bewaren die hij sowieso in zijn bezit heeft op het moment van de vordering. Het gaat hier om gegevens die bijgehouden worden om technische redenen, maar ook om redenen van facturatie, marketing, strijd tegen fraude, voor de beveiliging van het netwerk, e.a. Deze gegevens worden normaal gezien slechts bijgehouden zolang nodig voor de eigen doeleinden. Dit kan variëren van enkele minuten (in geval van vluchtige technische gegevens) tot meerdere jaren (bijvoorbeeld om een factuur te kunnen betwisten). In het belang van de inlichtingenopdrachten, kan een operator gevorderd worden om deze gegevens te "parkeren" en bij te houden (bewaartermijn van maximum 6 maanden, met de mogelijkheid tot verlenging). Op deze manier worden dus tenminste de beschikbare historische gegevens veiliggesteld.

Historische gegevens zijn cruciaal in een inlichtingenonderzoek om na te gaan wie contact had met wie, met welk middel, op welk moment en waar dat contact plaatsvond. Tot de uitspraak van het Europees Hof hoefden de betrokken diensten zich geen zorgen te maken over de beschikbaarheid van deze gegevens, aangezien alles voor 12 maand werd bijgehouden. Via de specifieke inlichtingenmethode overeenkomstig artikel 18/8 WIV kon de betrokken inlichtingendienst toegang nemen tot de gegevens die van belang waren voor het onderzoek.

Als gevolg van de Europese rechtspraak, zullen de resultaten afhankelijk zijn van de dataset die de operator voor eigen doeleinden bezit.

2° de vordering tot bewaring van verkeers- en lokalisatiegegevens die gegenereerd worden vanaf de ontvangst van de vordering (bewaring van toekomstige

freeze"). Dès qu'une personne, un outil de communication, etc. apparaît sur le radar d'un service de renseignement, l'opérateur peut être requis de conserver les données de trafic et de localisation y relatives pour une durée maximale de 6 mois (renouvelable). Le recours à la méthode spécifique de recueil de données 18/8 de la LRS permet, comme toujours, d'accéder à ces données.

Après l'expiration du délai de conservation, l'opérateur de réseau ou le fournisseur d'un service de communications électroniques détruit les données dans la mesure où elles ne sont plus pertinentes pour d'autres finalités. La mesure est valable pendant 6 mois maximum à compter de la date de la réquisition et est également prolongeable.

À la demande du Conseil d'État (avis 69.381/4 du 28 juin 2021, commentaire de l'art. 24 du projet initial, entre-temps renumérotée en art. 27) la distinction entre le délai de conservation et la durée de la mesure est précisée dans la réquisition.

La réquisition adressée à l'opérateur doit également mentionner clairement quelles données de trafic et de localisation doivent être conservées (conservation des données ciblée et différenciée).

Les éléments mentionnés dans la réquisition sont des données d'identification (nom, adresse…), des caractéristiques techniques (numéro d'appel, IMSI, IMEI…), une localisation précise (emplacement de l'antenne, coordonnées…) ou le mode d'utilisation détaillé d'un moyen (carte SIM prépayée dans un certain type de GSM qui n'est utilisé qu'une fois par semaine dans une région).

S'il venait à être informé par un correspondant national ou étranger de l'existence d'une personne A employée à l'aéroport et potentiellement impliquée dans les préparatifs d'un attentat à cet endroit, le service établirait les réquisitions de conservation suivantes:

— conservation des données de trafic et de localisation de la personne A;

— conservation des données de trafic et de localisation du site de l'aéroport de Zaventem.

Au cours de l'enquête, il est possible que des personnes ou des moyens apparaissent, légitimant la conservation des données de trafic et de localisation y relatives, et, par voie de conséquence, l'envoi de réquisitions de conservation à cette fin.

gegevens of "future freeze"). Zodra een persoon, een communicatiemiddel e.d. op de radar van een inlichtingendienst verschijnt, kan de operator bevolen worden om de verkeers- en lokalisatiegegevens ervan te bewaren voor een periode van maximaal 6 maanden (die verlengbaar is). Door gebruik te maken van de specifieke methode voor het verzamelen van gegevens bedoeld in artikel 18/8 WIV, is het zoals steeds mogelijk om toegang te krijgen tot die gegevens.

Na verloop van de bewaartermijn vernietigt de netwerkoperator of de dienstenaanbieder de gegevens voor zover ze niet meer relevant zijn voor andere doeleinden. De maatregel geldt voor maximum 6 maanden te rekenen vanaf de vordering en is eveneens verlengbaar.

Op vraag van de Raad van State (advies 69.381/4 van 28 juni 2021, opmerking bij art. 24 van het initiële ontwerp, intussen vernummerd tot art. 27), wordt in de vordering het onderscheid tussen de bewaartermijn en de duur van de maatregel verduidelijkt.

De vordering aan de operator moet ook duidelijk aangeven welke verkeers- en lokalisatiegegevens moeten bewaard worden (gerichte en gedifferentieerde dataretentie).

De elementen die in de vordering vermeld worden, zijn identificatiegegevens (naam, adres, …), technische kenmerken (oproepnummer, IMSI, IMEI, …), een precieze locatie (antennelocatie, coördinaten, etc) of de gedetailleerde gebruikswijze van een middel (prepaid sim in een bepaald type gsm dat in een regio slechts 1 keer per week wordt aangezet).

Wanneer de dienst wordt ingelicht door een binnen- of buitenlandse correspondent over een persoon A die werkt op de luchthaven en die betrokken zou zijn bij voorbereidingen van een aanslag op de luchthaven, dan zou de dienst volgende vorderingen tot bewaring opmaken:

— bewaring van verkeers- en lokalisatiegegevens van persoon A;

— bewaring van verkeers- en lokalisatiegegevens van de locatie Zaventem-luchthaven.

In de loop van het onderzoek kunnen er dan nog personen of middelen opduiken waarvan de bewaring van de verkeers- en lokalisatiegegevens gewettigd is, en waarvoor er dan ook vorderingen tot bewaring zullen worden verstuurd.

Un service de renseignement peut également demander à un opérateur la conservation de données d'un groupe déterminé de personnes. Par exemple, une liste de numéros d'appel de personnes connues dans les milieux religieux radicaux pourrait faire l'objet d'une réquisition de conservation renouvelée tous les 6 mois, tant que les personnes concernées représentent une menace pour les intérêts de l'État.

Lorsque le service ne dispose que d'informations relatives à une utilisation particulière de moyens de communication, cela peut également donner lieu à une réquisition de conservation des données. Dans l'affaire Encrochat, par exemple, les utilisateurs de ce service de messagerie chiffrée actif dans la sphère criminelle ont pu être identifiés à l'aide d'une combinaison entre le type d'appareil (code TAC, qui représente une partie du code IMEI unique répertoriant le type d'appareil et le numéro de série), la carte SIM (certaines cartes SIM néerlandaises) et l'utilisation du moyen de communication (uniquement data, impossibilité de recevoir/envoyer des SMS). Des modèles d'utilisation similaires peuvent être observés lors des enquêtes d'espionnage lors desquelles des "burner phones" peuvent être détectés grâce à une combinaison de caractéristiques techniques, géographiques et temporelles (pour contacter des sources clandestines).

Les services de renseignement peuvent ensuite demander ces données conformément à l'article 18/8 de la LRS, de façon dûment motivée et conformément à la procédure requise pour la mise en œuvre de cette méthode spécifique de recueil de données.

Suite à la remarque du Comité permanent R en son point 18, les auteurs du projet réintroduisent l'obligation de motiver la durée de la période à laquelle a trait la collecte de données basées sur l'article 18/8. Cette obligation était supprimée dans le projet initial.

Par analogie avec les réquisitions d'identification de l'utilisateur d'un moyen de communication (article 16/2 de la LRS), les services de renseignement ont l'obligation de tenir à jour un registre de l'ensemble des réquisitions de conservation des données de trafic et de localisation. En outre, chaque décision de réquisition est transmise, avec sa motivation, au Comité R qui peut mettre fin immédiatement à la méthode en cas d'illégalité.

S'il est mis fin à la mesure, le service de renseignement et de sécurité concerné en informe immédiatement l'opérateur afin que la conservation des données prenne fin.

Een inlichtingendienst kan ook vragen dat een operator de gegevens van een bepaalde groep van personen bijhoudt. Een lijst van de oproepnummers van gekende personen in de radicaal-religieuze scene zou bijvoorbeeld het onderwerp kunnen vormen van een vordering tot bewaring die elke 6 maand wordt verlengd, zolang de betrokkenen een bedreiging vormen voor de belangen van de Staat.

Ook wanneer de dienst enkel beschikt over informatie over het bijzondere gebruik van communicatiemiddelen, kan dit leiden tot een vordering tot het bewaren van gegevens. In de Encrochat-zaak, bijvoorbeeld, konden de gebruikers van deze versleutelde berichtendienst in de criminele sfeer worden opgelijst aan de hand van een combinatie van toesteltype (de TAC-code, een onderdeel van de unieke IMEI die het toesteltype en serienummer aangeeft), de simkaart (bepaalde Nederlandse simkaarten) en het type gebruik van het communciatiemiddel (enkel datagebruik, geen in- of uitgaande SMS mogelijk). Gelijkaardige gebruikspatronen zijn op te merken bij spionageonderzoeken waar "burner phones" op te sporen zijn via een combinatie van technische, geografische en temporele kenmerken (voor de contactname met clandestiene bronnen).

De inlichtingendiensten kunnen deze gegevens vervolgens opvragen overeenkomstig artikel 18/8 WIV, met inachtname van de afdoende motivatie en de procedure vereist voor de inzet van deze specifieke BIM-methode.

Naar aanleiding van de opmerking van het Vast Comité I bij punt 18 voeren de auteurs van het ontwerp de motivatieplicht opnieuw in wat betreft de duur van de periode waarop de verzameling van gegevens op grond van artikel 18/8 betrekking heeft. Deze verplichting was geschrapt in het initieel ontwerp.

Naar analogie met de vorderingen tot identificatie van de gebruiker van een communicatiemiddel (artikel 16/2 WIV), moeten de inlichtingendiensten ook een register bijhouden van alle vorderingen tot bewaring van verkeers- en lokalisatiegegevens. Bovendien wordt elke beslissing tot vordering samen met de motivering, overgemaakt aan het Comité I dat, in geval van onwettigheid, de methode onmiddellijk kan stopzetten.

Indien de maatregel wordt stopgezet, informeert de betrokken inlichtingen– en veiligheidsdienst hiervan onverwijld de operator opdat de bewaring van gegevens beëindigd wordt.

Dans le cadre de ces réquisitions de conservation, les auteurs souhaitent également fournir des explications supplémentaires à l'égard des remarques du Comité permanent R (points 6-9), selon lesquelles ces réquisitions ne bénéficieraient pas de la même protection juridique que celles contenues dans le projet d'article 39*quinquies* CIC. Le Comité fait ici – à tort – une comparaison entre les enquêtes de renseignement et les enquêtes pénales.

Les finalités des deux types de procédures sont totalement différentes. Le but de l'enquête de renseignement n'est pas de rassembler des preuves pour faire condamner quelqu'un. L'objectif est d'anticiper des menaces et de faire en sorte qu'elles ne se réalisent pas.

Les services de renseignement collectent de l'information, les services de police collectent des preuves. Les informations provenant des services de renseignement ne peuvent pas constituer les motifs exclusifs ni la mesure prépondérante conduisant à la condamnation d'une personne. Les éléments doivent être étayés de manière prédominante par d'autres éléments de preuve (voir notamment l'article 19/1 de la loi organique du 30/11/1998 des services de renseignement qui le précisent expressément). C'est donc une restriction importante à la valeur probante des informations récoltées par les services de renseignement. Il existe donc un critère objectif raisonnablement justifié qui permet une différence de traitement entre les informations recueillies par les services de renseignement et les preuves récoltées par les services de police. Si le raisonnement avancé ici par le Comité R était retenu, cela reviendrait à considérer les services de police et de renseignement comme identiques alors que leur travail, leurs missions et leurs finalités sont différents.

En réponse à cet argument, la Cour constitutionnelle a confirmé notre point de vue dans un arrêt récent n° 64/2021 du 22 avril 2021 (question préjudicielle du Comité R):

"B.10.1. Il ressort des travaux préparatoires de la loi du 4 février 2010 "que les finalités des services de renseignement et de sécurité diffèrent fondamentalement de celles des services de police, dans leur composante judiciaire" (Doc. parl., Sénat, 2008-2009, n° 4-1053/1, p. 12).

Ainsi qu'il est exposé dans ces travaux préparatoires, le travail des services de renseignement et de sécurité est plutôt de nature analytique et vise à permettre de comprendre les structures et les réseaux présents en Belgique, alors que les autorités judiciaires et policières recherchent toujours des preuves liées à un fait punissable concret (déjà commis ou non). Dès lors, l'enquête

In het kader van deze bewaarbevelen wensen de auteurs ook nadere toelichting te geven bij de opmerkingen van het Vast Comité I (punt 6-9) als zouden deze vorderingen niet dezelfde rechtsbescherming genieten als deze in het ontworpen artikel 39 *quinquies* Sv. Het Comité maakt hier –ten onrechte- een vergelijking tussen inlichtingenonderzoeken en strafonderzoeken.

De doeleinden van beide procedures zijn totaal verschillend. Het doel van een inlichtingenonderzoek is niet om bewijzen te verzamelen om iemand te laten veroordelen. Het doeleinde is te anticiperen op dreigingen en ervoor te zorgen dat die geen werkelijkheid worden.

De inlichtingendiensten verzamelen informatie, de politiediensten verzamelen bewijzen. De informatie die van de inlichtingendiensten komt, mag niet de enige grond noch de overheersende maatregel zijn voor de veroordeling van een persoon. De elementen moeten in overheersende mate steun vinden in andere bewijsmiddelen (zie inzonderheid artikel 19/1 van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten van 30 november 1998, waarin dat uitdrukkelijk wordt bepaald). Het is dus een belangrijke beperking op de bewijskracht van de door de inlichtingendiensten verzamelde informatie. Er bestaat dus een redelijkerwijs gerechtvaardigd objectief criterium op basis waarvan een verschil in behandeling mogelijk is tussen de informatie die door de inlichtingendiensten is verzameld en de bewijzen die door de politie zijn verzameld. Als de redenering die het Comité I hier naar voren brengt, was gevolgd, zou het erop neerkomen dat de politiediensten en de inlichtingendiensten als identiek worden beschouwd, terwijl hun werkzaamheden, opdrachten en doeleinden verschillend zijn.

Als antwoord op dat argument heeft het Grondwettelijk Hof ons standpunt bevestigd in een recent arrest nr. 64/2021 van 22 april 2021 (prejudiciële vraag van Comité I):

"B.10.1. Uit de parlementaire voorbereiding van de wet van 4 februari 2010 blijkt "dat de doelstellingen van de inlichtingen-en veiligheidsdiensten, op het vlak van het gerechtelijk werk, fundamenteel verschillen van die van de politiediensten" (Parl. St., Senaat, 2008-2009, nr. 4-1053/1, blz. 12).

Zoals in dezelfde parlementaire voorbereiding wordt uiteengezet, is het werk van de inlichtingen-en veiligheidsdiensten veeleer analytisch van aard en erop gericht inzicht te verwerven in de structuren en de netwerken die in België voorkomen, terwijl de gerechtelijke en politionele autoriteiten steeds bewijzen zoeken in verband met een (al dan niet reeds gepleegd) concreet strafbaar

pénale est toujours menée en vue de rechercher et de poursuivre des infractions qui ont été commises par des personnes déterminées, ou le seront, ou qui ont déjà été commises mais ne sont pas encore connues, alors que l'enquête de renseignement vise à recueillir des informations sur une série d'événements qui ne concernent pas forcément des faits punissables mais qui peuvent représenter un danger pour la sécurité de l'État, pour les intérêts militaires ou pour des intérêts fondamentaux du pays (ibid., p. 12).

La diversité de ces missions légales se reflète dans les natures clairement différentes des données recueillies dans les deux types d'enquêtes. La recherche de renseignements dans le cadre d'une information ou d'une instruction vise à recueillir des éléments de preuve concernant une infraction qui soient effectivement utilisables dans une procédure pénale devant le juge du fond. Les données que les services de renseignement et de sécurité recueillent ne visent pas à convaincre un juge du fond de la "culpabilité" pénale d'un prévenu mais à permettre à l'autorité publique de prendre les mesures qui s'imposent en vue de préserver les intérêts fondamentaux du pays. (…)"

Il en découle que la Cour a considéré que la différence de traitement entre ce qui était prévu par la loi du 30 novembre 1998 et ce qui était prévu dans le Code d'instruction criminelle repose sur une justification objective et raisonnable.

Par ailleurs, la comparaison se base sur l'équivalence ou la non-équivalence des procédures de contrôle. Pour ce faire, le Comité R semble ne pas tenir compte d'éléments importants.

Ainsi, il est inadéquat de comparer un procureur du Roi ou un juge d'instruction à la Commission BIM. Un procureur du Roi est à la tête de l'enquête pénale et un juge d'instruction mène, par définition, l'instruction. Ils ne sont pas indépendants par rapport à l'enquête, ils la gèrent. À l'inverse, la Commission BIM est composée de trois magistrats dont l'unique fonction est d'exercer un contrôle indépendant sur les méthodes BIM et les réquisitions de conservation généralisée et indifférenciée. Ces magistrats ne sont pas chargés de l'enquête et n'y sont d'aucune manière impliqués.

Par ailleurs, il convient de rappeler que le Comité permanent R, qui est également un organe de contrôle indépendant, exerce un contrôle effectif sur toutes les méthodes de recueil de données par les services de renseignement, ce qui n'est pas le cas du Comité permanent P

feit. Derhalve wordt het strafonderzoek steeds gevoerd met het oog op het opsporen en het vervolgen van misdrijven die door welbepaalde personen, hetzij zijn gepleegd, hetzij zullen worden gepleegd of reeds zijn gepleegd maar nog niet aan het licht zijn gekomen, terwijl een inlichtingenonderzoek strekt tot het verzamelen van informatie omtrent een reeks gebeurtenissen, die niet per definitie strafbare feiten betreffen, doch een gevaar kunnen betekenen voor de veiligheid van de Staat, voor de militaire belangen of voor fundamentele belangen van het land (ibid., blz.12).

De onderscheidenheid van die wettelijke opdrachten komt tot uiting in de duidelijk verschillende aard van de in de beide types van onderzoek verzamelde gegevens. De zoektocht naar gegevens in het kader van een opsporings-of gerechtelijk onderzoek is erop gericht bewijselementen te verzamelen met betrekking tot een misdrijf, die daadwerkelijk bruikbaar zijn in een strafprocedure voor de rechter ten gronde. De gegevens die de inlichtingen-en veiligheidsdiensten verzamelen, strekken niet ertoe een rechter ten gronde te overtuigen van de strafrechtelijke "schuld" van een beklaagde, maar wel de overheid toe te laten de noodzakelijke maatregelen te nemen ter vrijwaring van de fundamentele belangen van het land (…)".

Daaruit blijkt dat het Hof van oordeel was dat het verschil in behandeling tussen wat door de wet van 30 november 1998 was bepaald en wat in het Wetboek van Strafvordering was bepaald, op een objectieve en redelijke rechtvaardiging berust.

De vergelijking is overigens gebaseerd op de gelijkwaardigheid of de niet-gelijkwaardigheid van de controleprocedures. Daarbij lijkt Comité I geen rekening te houden met belangrijke elementen.

Zo is het inadequaat om een procureur des Konings of een onderzoeksrechter te vergelijken met de BIM-commissie. Een procureur des Konings staat aan het hoofd van het strafrechtelijk onderzoek en een onderzoeksrechter leidt per definitie het gerechtelijk onderzoek. Zij zijn niet onafhankelijk ten opzichte van het onderzoek, ze beheren het. De BIM-commissie is daarentegen samengesteld uit drie magistraten met als enige functie onafhankelijk toezicht te houden op de BIM-methoden en de vorderingen tot de algemene en ongedifferentieerde bewaring. Die magistraten zijn niet belast met het onderzoek en zijn er op geen enkele manier bij betrokken.

Voorts moet erop worden gewezen dat het Vast Comité I, dat ook een onafhankelijk controleorgaan is, daadwerkelijk toezicht uitoefent op alle methoden voor het verzamelen van gegevens door de inlichtingendiensten, en dat het Vast Comité P geen toezicht

qui n'exerce pas de contrôle sur les méthodes de collecte utilisées lors d'enquêtes pénales. En outre, l'Organe de contrôle de l'information policière ne contrôle pas le Procureur du Roi et le juge d'instruction. Le dirigeant d'un service de renseignement est, quant à lui, contrôlé par le Comité R, tant dans sa fonction d'organe de contrôle des services de renseignement, que dans sa fonction d'Autorité de protection des données.

Au vu de ce qui précède, il n'est donc pas correct de dire qu'il y aurait une protection "inférieure" offerte par le projet d'article 13/6 (initialement 16/2/1); il est clair que c'est même le contraire.

Les auteurs du projet tiennent à souligner qu'il n'y a pas vraiment de différence entre les mentions prévues dans la décision sur la base de l'article 13/6 et celles prévues sur la base de l'article 39*quinquies* CIC.

En effet, il est prévu à l'article 13/6 que la décision doit être motivée: il va de soi que cette motivation portera sur les faits représentant une éventuelle menace et sur le contexte. Dans l'art. 39*quinquies* CIC figurent également la mention des circonstances de fait de la cause qui justifient la conservation. Par discrétion et pour protéger les enquêtes de renseignement, ces informations ne sont jamais reprises dans les réquisitions. Les circonstances de fait et le contexte se trouveront dans la décision, et non dans la réquisition.

Il est ensuite prévu que la réquisition mentionne l'objet de la conservation (personnes, moyens de communication, etc.) et la durée de celle-ci.

Pour répondre à la crainte du Comité permanent R par rapport au mécanisme de contrôle (point 8), les auteurs du projet ont adapté la notification au Comité R: celle-ci devra avoir lieu lors de chaque application de l'article 13/6 et non à la fin de chaque mois. Cela rend le contrôle du Comité R encore plus effectif et actuel.

Dans son avis (points 10-14), le Comité permanent R critique la possibilité pour le dirigeant de service de faire signer les réquisitions des opérateurs de télécommunications par un délégué. Les auteurs souhaitent souligner que la définition de "son délégué" est introduite dans un autre projet de modification de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité: "l'agent, autre que le gestionnaire du dossier, désigné par le dirigeant du service pour prendre habituellement certaines décisions à sa place".

uitoefent op de tijdens strafrechtelijke onderzoeken gebruikte verzamelmethoden. Bovendien controleert het Controleorgaan op de politionele informatie de procureur des Konings en de onderzoeksrechter niet. Het hoofd van een inlichtingendienst wordt gecontroleerd door Comité I, zowel in diens functie van orgaan voor de controle op de inlichtingendiensten als in diens functie van gegevensbeschermingsautoriteit.

Gelet op het voorgaande is het niet correct om te zeggen dat het ontwerp van artikel 13/6 (oorspronkelijk 16/2/1) "minder" bescherming biedt; het is duidelijk dat zelfs het tegendeel waar is.

De auteurs van het ontwerp wensen erop te wijzen dat er niet echt een verschil is tussen de vermeldingen waarin is voorzien in de beslissing op grond van artikel 13/6 en degene waarin op grond van artikel 39*quinquies* Sv. is voorzien.

In artikel 13/6 is immers bepaald dat de beslissing gemotiveerd moet zijn: het spreekt dus voor zich dat die motivatie betrekking moet hebben op de feiten die een eventuele dreiging inhouden en op de context. In art. 39*quinquies* Sv staat ook de vermelding van feitelijke omstandigheden van de zaak die de bewaring rechtvaardigen. Voor de discretie en ter bescherming van een inlichtingenonderzoek, wordt dergelijke informatie nooit in een vordering opgenomen. De feitelijke omstandigheden en de context zullen in de beslissing staan en niet in de vordering.

Er wordt vervolgens voorzien dat de vordering het voorwerp van de bewaring (personen, communicatiemiddelen, enz.) vermeldt, evenals de duur ervan.

Om tegemoet te komen aan de vrees van het Vast Comité I met betrekking tot het controlemechanisme (punt 8), hebben de auteurs van het ontwerp de kennisgeving aan het Comité I aangepast: die zal moeten gebeuren bij elke toepassing van artikel 13/6 en niet op het einde van elke maand. Dat maakt de controle van het Comité I nog effectiever en actueler.

In zijn advies (punt 10-14) bekritiseert het Vast Comité I de mogelijkheid voor het diensthoofd om vorderingen aan de telecomoperatoren te laten ondertekenen door een gedelegeerde. De auteurs wensen erop te wijzen dat de definitie van "zijn gedelegeerde" is opgenomen in een ander ontwerp tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten: - de agent, andere dan de dossierbeheerder, aangesteld door het diensthoofd om bepaalde beslissingen gewoonlijk in zijn plaats te nemen".

Une personne désignée pour prendre la décision ne pouvant pas être juge et partie, le gestionnaire du dossier est écarté des personnes qui peuvent être habilitées. Il est précisé, à l'instar de ce qui a été indiqué dans l'exposé des motifs de l'article 16/4 (doc 54-2855), que le terme de "gestionnaire de dossier" vise la personne qui traite un dossier ou une affaire et qui exprime le besoin de la mesure qui est soumise à l'autorisation.

Une personne désignée jouira d'une position hiérarchique supérieure à celle du gestionnaire du dossier, lorsque la structure hiérarchique du service le permet.

La désignation doit avoir un caractère aussi permanent que possible, en fonction des moyens du service. Des changements journaliers sont exclus. La délégation est faite par écrit par le dirigeant du service et est transmise au Comité R.

Il est évident que la désignation d'une personne habilitée à prendre certaines décisions à sa place, n'exclut pas la faculté pour le dirigeant du service de prendre lui-même ces décisions.

Enfin, afin de répondre à la note de bas de page 7 de l'avis du Comité permanent R et d'améliorer la cohérence du texte, le premier paragraphe de l'article 13/6 a été reformulé.

Art. 28 (insertion de l'article 13/7)

Dans son arrêt du 6 octobre 2020, la Cour de Justice précise que, dans des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le concours des opérateurs peut être requis pour procéder à la conservation généralisée et indifférenciée des données de télécommunication. La condition connexe prévoit que les données ne seront pas conservées plus longtemps que le strict nécessaire et que la réquisition fait l'objet d'un contrôle effectif, soit par un tribunal, soit par un organe administratif indépendant. Conformément à cette jurisprudence, une telle réquisition de conservation généralisée et indifférenciée est insérée dans une nouvelle section 3/1 du chapitre III, intitulée - Réquisitions de conservation- .

Conformément au nouvel article 13/7 (article 18/17/1 dans le projet initial), cette mesure ne peut être prise qu'en cas de menace très grave pour la sécurité de l'État, qui est de plus réelle et actuelle ou prévisible, et après l'accord de la Commission BIM (organe administratif

Aangezien een persoon die is aangewezen om de beslissing te nemen niet tegelijk rechter en partij mag zijn, wordt de dossierbeheerder uitgesloten als persoon die kan worden gemachtigd. In navolging van wat werd vermeld in de memorie van toelichting bij artikel 16/4 (doc. 54-2855) wordt er verduidelijkt dat met "dossierbeheerder" de persoon wordt bedoeld die een dossier of een zaak behandelt en die de behoefte uitdrukt aan de maatregel die aan de toelating is onderworpen.

De aangewezen persoon zal een hogere hiërarchische positie hebben dan de dossierbeheerder wanneer de hiërarchische structuur van de dienst daartoe de mogelijkheid biedt.

De aanwijzing moet een zo permanent mogelijk karakter hebben, naargelang van de middelen van de dienst. Dagelijkse wissels zijn uitgesloten. De delegatie gebeurt op schriftelijke wijze door het diensthoofd en wordt overgezonden aan het Comité I.

Het is duidelijk dat de aanwijzing van een persoon die gemachtigd is om bepaalde beslissingen te nemen in de plaats van de leidinggevende van de dienst het voor die laatstgenoemde niet onmogelijk maakt om zelf de beslissingen te nemen.

Om, tot slot, tegemoet te komen aan voetnoot 7 van het advies van het Vast Comité I, en ter bevordering van de coherentie van de tekst, werd het eerste lid van artikel 13/6, geherformuleerd.

Art. 28 (invoeging van artikel 13/7)

In zijn arrest van 6 oktober 2020 stelt het Hof van Justitie dat in situaties waarbij de lidstaat wordt geconfronteerd met een ernstige bedreiging voor de nationale veiligheid die reëel en actueel of voorzienbaar is, er een bevel kan worden opgelegd aan operatoren om telecommunicatiegegevens algemeen en ongedifferentieerd te bewaren. Als voorwaarde hiervoor geldt dat de gegevens niet langer bewaard worden dan strikt noodzakelijk is en het bevel het voorwerp uitmaakt van een effectieve controle, hetzij door een rechtbank, hetzij door een onafhankelijk administratief orgaan. In lijn met deze rechtspraak wordt de bevoegdheid om een algemene en ongedifferentieerde bewaring op te leggen, ingevoegd in de nieuwe afdeling 3/1, van hoofdstuk III, met als opschrift "De vorderingen tot bewaring".

Luidens het nieuwe artikel 13/7 (in het initieel ontwerp: artikel 18/17/1) kan deze maatregel slechts genomen worden ingeval van een zeer ernstige dreiging tegen de veiligheid van de staat die bovendien reëel en actueel of voorzienbaar is en na akkoord van de BIM-Commissie

indépendant). Cette Commission évalue non seulement la légalité de la réquisition, mais également la proportionnalité et la subsidiarité. En outre, par le biais d'une procédure d'extrême urgence, la Commission peut intervenir très rapidement, tout en conservant sa fonction de contrôle, ce qui est nécessaire dans le cas d'une menace grave réelle et actuelle. Une fois la réquisition accordée, le Comité permanent R peut également exercer sa compétence de contrôle.

Suite aux remarques formulées par le Conseil d'État, les auteurs ont révisé la procédure initialement prévue pour la réquisition de conservation généralisée. Dans la version actuelle, il est prévu que toute réquisition généralisée émanant d'un service de renseignement doit toujours être confirmée par le Roi. Une telle réquisition constitue en effet un acte réglementaire qui impose des obligations aux opérateurs et fournisseurs de télécommunications de manière générale et abstraite. Cet arrêté royal ne doit ni être soumis à l'avis du Conseil d'État, ni à celui du Comité permanent R car il ne crée pas une nouvelle règle de droit. Cette modification rend les points 23-24 de l'avis du Comité R sans objet.

Afin de ne pas porter préjudice aux enquêtes menées par les services de renseignement, la réquisition ne mentionnera que la date de l'accord de la Commission, la date de la réquisition, la nature des données de trafic et de localisation à conserver, la durée de la mesure et le délai de conservation. La réquisition de conservation est valable pour une durée maximale de six mois à compter de la date de la réquisition et peut être prolongée. Les données-mêmes seront conservées pendant six mois maximum à compter du moment de la communication. Ce délai de conservation peut également être prolongée. Comme demandé par le Conseil d'État, la distinction entre la durée de la mesure et la durée de conservation a été précisée dans la loi.

La réquisition prend fin si elle n'est pas confirmée dans un délai d'un mois par la signature de l'arrêté royal. Le service de renseignement en informe les opérateurs dans les plus brefs délais.

Si la réquisition prend fin prématurément, par exemple si la menace a disparu ou lorsqu'une illégalité est constatée, cette décision est portée à la connaissance des opérateurs dès que possible. Cela peut se faire par une publication au *Moniteur belge* ou par l'intermédiaire du website de l'IBPT.

Les opérateurs mettent fin à la conservation et détruisent les données conservées de manière injustifiée dans la mesure où leur conservation n'est pas nécessaire à d'autres finalités (pour des raisons commerciales,

(onafhankelijk administratief orgaan). Deze commissie beoordeelt niet alleen de wettelijkheid van de vordering, maar ook de proportionaliteit en de subsidiariteit. Via een hoogdringendheidsprocedure kan de Commissie bovendien zeer snel optreden, zonder aan haar controlefunctie in te boeten, hetgeen noodzakelijk is in geval van een reële en actuele ernstige bedreiging. Eens de vordering is ingesteld, kan ook het Vast Comité I zijn toezichtsbevoegdheid uitoefenen.

Op aangeven van de Raad van State hebben de auteurs de initieel voorziene procedure voor het algemene bewaarbevel herzien. In de huidige versie is bepaald dat de algemene vordering uitgaande van een inlichtingendienst, steeds bekrachtigd moet worden door de Koning. Dergelijke vordering is immers een reglementaire handeling die op algemene en abstracte wijze verplichtingen oplegt in hoofde van de telecomoperatoren en –aanbieders. Dit koninklijk besluit moet niet voorgelegd worden voor advies aan de Raad van State, noch aan het Vast Comité I omdat het geen nieuwe rechtsregels invoert. Door deze wijziging worden de punten 23-24 uit het advies van het Comité I zonder voorwerp.

Om de onderzoeken van de inlichtingendiensten niet in het gedrang te brengen, wordt in de vordering enkel de datum van het akkoord van de Commissie vermeld, de datum van de vordering, de aard van de verkeers- en lokalisatiegegevens die bewaard moeten worden, de duur van de maatregel en de bewaartermijn. Het bewaarbevel geldt voor maximum zes maanden te rekenen vanaf de vordering en kan verlengd worden. De gegevens zelf worden maximum zes maanden bijgehouden te rekenen vanaf de communicatie. Ook deze bewaartermijn kan verlengd worden. Zoals gevraagd door de Raad van State, werd het onderscheid tussen de duur van de maatregel en de bewaartermijn verduidelijkt in de wet.

De vordering vervalt als ze niet bekrachtigd wordt binnen de maand door de ondertekening van het koninklijk besluit. De inlichtingendienst brengt de operatoren hiervan zo snel mogelijk op de hoogte.

Indien de vordering voortijdig wordt stopgezet, bijvoorbeeld als de dreiging is weggevallen of in geval van een onwettigheid, wordt deze beslissing zo snel mogelijk bekendgemaakt aan de operatoren. Dit kan gebeuren via een publicatie in het *Belgisch Staatsblad* of via de website van het BIPT.

De operatoren stoppen de bewaring en vernietigen de onterecht bijgehouden gegevens voor zover deze niet moeten bijhouden worden voor andere doeleinden (voor commerciële redenen, netwerkveiligheid, ter bescherming

pour la sécurité du réseau, pour protéger les clients, pour se conformer aux réquisitions fondées sur d'autres législations).

En réponse au point 26 de l'avis du Comité permanent R, les auteurs du projet souhaitent souligner que les services de renseignement mènent des enquêtes à long terme sur des réseaux et des tendances, et non sur des faits concrets dans le cadre d'une affaire pénale devant être clôturée au plus vite. C'est pourquoi une conservation généralisée de maximum 6 mois peut être imposée. Si la Commission estime qu'une durée de 6 mois est disproportionnée, elle ne donnera son accord que pour une durée de conservation plus courte.

Afin de satisfaire aux recommandations formulées au point 27 dans l'avis du Comité permanent R, un rapport sur l'évolution de la menace sera rendu toutes les deux semaines, et non – comme initialement prévu – tous les deux mois.

Étant donné que la réquisition de conservation indifférenciée et généralisée n'est plus une méthode exceptionnelle de renseignement, comme cela était prévu initialement, les règles particulières pour l'utilisation de ces méthodes à l'égard des médecins, des avocats et des journalistes ne s'appliquent pas. Toutefois, ces catégories professionnelles, tout comme le secret professionnel et le secret des sources qui leur sont associés, restent soumis aux garanties supplémentaires de l'article 2, § 2 de la LRS. Les auteurs souhaitent souligner une fois de plus que les réquisitions de conservation ne sont pas liées à une exploitation ultérieure systématique. Ceci est une réponse aux préoccupations du Comité R (point 28).

Le Comité permanent R demande si la Commission et le Comité sont autorisés, dans le cadre de la mission de surveillance de la BIM, à visi*ter* les lieux où les opérateurs télécoms conservent les données demandées (point 29). Dans le cadre de la protection des données, le principe est que le traitement des données à caractère personnel est soumis au contrôle de l'autorité de contrôle compétente. En l'occurrence, le traitement des données à caractère personnel par les opérateurs de réseaux et les fournisseurs de services est soumis au contrôle de l'Autorité de protection des données.

Les auteurs du projet ne suivent pas la proposition du Comité R développée au point 21 de son avis car ils ont pris le parti de respecter pleinement les "suggestions" de la CJUE.

Pour répondre au point 22 de l'avis du Comité R sur l'utilisation des données conservées pour d'autres finalités, les auteurs du projet rappellent que, comme le permet l'article 15, § 1 de la directive 2002/58 ("ePrivacy"),

van de klanten, om te voldoen aan vorderingen op basis van andere wetgeving).

Als antwoord op punt 26 op het advies van het Vast Comité I wensen de auteurs van het ontwerp te benadrukken dat inlichtingendiensten langlopende onderzoeken voeren naar netwerken en tendensen, en niet naar concrete feiten in een strafdossier dat zo snel mogelijk wordt afgesloten. Om die reden kan een algemene bewaring van maximum 6 maanden opgelegd worden. Indien de Commissie van oordeel is dat 6 maanden disproportioneel lang is, zal zij haar akkoord slechts geven voor een kortere bewaartermijn.

Om tegemoet te komen aan punt 27 van het advies van het Vast Comité I, wordt een tweewekelijks verslag over de evolutie van de dreiging voorzien, en niet – zoals initieel bepaald – een verslag om de twee maanden.

Gezien de vordering tot algemene en ongedifferentieerde bewaring geen uitzonderlijke inlichtingenmethode meer is, zoals initieel voorzien, is de bijzondere regeling voor de inzet van deze methoden ten opzichte van artsen, advocaten en journalisten, niet van toepassing. Deze beroepscategorieën en daaraan gelieerd, het beroepsgeheim en het bronnengeheim, blijven evenwel onderworpen aan de extra garanties van artikel 2, § 2 WIV. De auteurs wensen hierbij nogmaals te benadrukken dat de bewaarbevelen los staan van de systematische exploitatie achteraf. Hiermee wordt tegemoetgekomen aan de bezorgdheid van het Comité I (punt 28).

Het Vast Comité I stelt de vraag of de Commissie en het Comité bevoegd zijn om in het kader van hun BIM-toezicht de plaatsen te bezoeken waar de telecomoperatoren de gevorderde gegevens bewaren (punt 29). In principe is in het kader van de gegevensbescherming de verwerking van de persoonsgegevens onderworpen aan de controle van de bevoegde gegevensbeschermingsautoriteit. Bijgevolg is de verwerking van persoonsgegevens door netwerkoperatoren en dienstenaanbieders onderworpen aan de controle van de Gegevensbeschermingsautoriteit.

De auteurs van het ontwerp gaan niet mee in het voorstel dat het Comité I heeft uitgewerkt in punt 21 van zijn advies omdat zij ervoor hebben gekozen ten volle rekening te houden met de "suggesties" van het HvJ-EU.

Om tegemoet te komen aan punt 22 van het advies van het Comité I betreffende het gebruik van de bewaarde gegevens voor andere doeleinden, herinneren de auteurs van het ontwerp eraan dat, zoals wordt toegelaten

l'article 18/8 LRS (ainsi que l'article 127/1 LCE) constitue la base juridique qui autorise un traitement ultérieur pour d'autres finalités que celles qui étaient initialement prévues et qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23 du RGPD, lesquels comprennent la sécurité nationale, la sécurité publique, la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

L'accès est nécessaire et proportionné vu que:

— celui-ci n'est accordé que pour les finalités ultérieures reprises de manière exhaustive à l'article 18/8 de la LRS, lequel précise - les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions- , pour lesquelles il est renvoyé aux articles 7 et 11 de la LRS;

— il est fondé sur une base juridique prévue dans une loi organique et doit satisfaire aux conditions d'accès spécifiques fixées par cette loi.

En d'autres termes, les services de renseignement et de sécurité peuvent disposer d'un accès en vue d'un traitement ultérieur de ces données dans la mesure où cet accès est régi par une loi organique ou sectorielle, laquelle donne le pouvoir d'obtenir ces données de l'opérateur et fixe les conditions d'accès des deux services aux données, et dans la mesure où ce traitement de données répond aux finalités visées aux articles 7 et 11 de la LRS.

En outre, conformément à la jurisprudence de la Cour de Justice de l'Union européenne (cf. en particulier les points 166 et 167 de l'arrêt La Quadrature du Net de la CJUE du 6 octobre 2020), cette demande d'accès pour une finalité ultérieure, devra répondre à un examen de proportionnalité entre les finalités pour lesquelles la conservation est imposée et les finalités ultérieures poursuivies par la demande d'accès aux données de localisation et de trafic.

L'article 18/8 est conforme à cette jurisprudence européenne vu que le principe de proportionnalité est *in concreto* rencontré: en effet, si la conservation des données est justifiée originellement pour lutter contre une menace précise contre la sécurité nationale, ces mêmes données peuvent également être traitées ultérieurement pour d'autres menaces contre la sécurité nationale.

door artikel 15, § 1, van Richtlijn 2002/58 ("ePrivacy"), artikel 18/8 WIV (evenals artikel 127/1 van de WEC) de rechtsgrondslag vormt die een latere verwerking voor andere dan de oorspronkelijke doeleinden mogelijk maakt, wat in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van wat in artikel 23 van de AVG wordt beoogd, waaronder de nationale veiligheid, de openbare veiligheid en de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De toegang is noodzakelijk en evenredig aangezien:

— hij slechts wordt toegestaan voor de latere doeleinden die op exhaustieve wijze zijn opgesomd in artikel 18/8 WIV, dat begint met "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten", waarmee wordt verwezen naar de artikelen 7 en 11 WIV

— hij stoelt op een rechtsgrondslag waarin is voorzien in een organieke wet en voldoet aan de specifieke toegangsvoorwaarden waarin deze wet voorziet.

De inlichtingen- en veiligheidsdiensten kunnen met andere woorden toegang krijgen voor een latere verwerking van de gegevens voor zover die toegang wordt geregeld door een organieke of sectorspecifieke wet, waarin de bevoegdheid wordt verleend om de gegevens van de operator te verkrijgen en waarin de voorwaarden voor de toegang van beide diensten tot de gegevens worden vastgelegd, en voor zover de gegevensverwerking in overeenstemming is met de doeleinden vermeld in de artikelen 7 en 11 WIV.

Overeenkomstig de rechtspraak van het Hof van Justitie van de Europese Unie (cf. inzonderheid de punten 166 en 167 van het arrest *La Quadrature du Net* van het HvJ-EU van 6 oktober 2020), moet in het kader van het verzoek tot toegang om een ander doeleinde de evenredigheid worden onderzocht tussen de doeleinden waarvoor de bewaring is opgelegd en de latere doeleinden die worden nagestreefd in het kader van het verzoek tot toegang tot de verkeers- en locatiegegevens.

Artikel 18/8 is in overeenstemming met die Europese rechtspraak aangezien *in concreto* aan het evenredigheidsbeginsel wordt voldaan: als de bewaring van de gegevens oorspronkelijk haar rechtvaardiging vindt in de bestrijding van een specifieke gevaar voor de nationale veiligheid, kunnen diezelfde gegevens later ook worden verwerkt voor andere gevaren voor de nationale veiligheid.

In fine, il n'est pas inutile de rappeler que ces finalités ultérieures correspondent non seulement à celles prévues à l'article 23, § 1er du RGPD mais aussi avec celles prévues par l'article 15, § 1 de la directive ePrivacy.

Le contrôle par la Commission BIM sur l'accès aux données de trafic ou de localisation conservée reste de mise. En cas de conservation généralisée basée sur l'article 13/7 en raison d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, un service de renseignement peut demander ces données historiques dans le cadre d'une enquête de renseignement.

Au point 22 de son avis, le Comité permanent R s'interroge également sur l'accès par les autorités judiciaires aux données conservées à la demande d'un service de renseignement.

Comme mentionné au regard de l'article 127/1 LCE quant à l'accès aux données par les autorités publiques, Il convient tout d'abord de rappeler effectivement le principe établit par la CJE de proportionnalité entre les finalités de conservation et finalités d'accès en vertu duquel l'accès aux données conservées est uniquement possible pour les mêmes finalités que celles de la conservation initiale ou pour un objectif d'intérêt général d'importance au moins équivalente. La CJUE indique en outre explicitement que des données conservées aux fins de sécurité nationale ne peuvent être accessibles pour des finalités de criminalité ordinaire.

En application de ce principe issu de la jurisprudence de la CJE, dès lors que les services de renseignement ont opéré sur la base de leur loi organique une conservation généralisée ou ciblée des données de communication (/trafic/localisation), ces mêmes données ne peuvent être accessibles à d'autres autorités publiques que dans des cas dans lesquels la finalité de l'accès poursuit un objectif général d'importance au moins équivalente. Ce point ne trouve bien entendu pas à s'appliquer si ces mêmes données sont, par ailleurs, déjà conservées sur pied d'une autre disposition (ex article 126/1 de la loi télécom).

Illustrons notre propos.

En cas de menace grave pour la sécurité nationale, qui s'avère réelle et actuelle ou prévisible, comme une menace terroriste ou une menace d'ingérence d'autorité étrangère, une conservation généralisée et indifférenciée peut avoir lieu pendant 6 mois renouvelable. Si cette menace se concrétise (ex une bombe explose dans le métro, l'autorité étrangère contrôle des médias sociaux), pour les besoins de l'enquête judiciaire qui va

In fine is het nuttig erop te wijzen dat die latere doeleinden niet alleen in overeenstemming zijn met die waarin is voorzien in artikel 23, lid 1, van de AVG, maar ook met die waarin is voorzien in artikel 15, lid 1, van de richtlijn "ePrivacy".

De controle door de BIM-commissie van de toegang tot de bewaarde verkeers- of lokalisatiegegevens blijft behouden. In geval van een algemene bewaring gebaseerd op artikel 13/7 wegens een ernstige, reële, actuele of voorzienbare dreiging tegen de nationale veiligheid, kan een inlichtingendienst deze historische gegevens opvragen in het kader van een inlichtingenonderzoek.

In punt 22 van zijn advies werpt het Comité I ook de vraag op over de toegang van de gerechtelijke overheden tot de gegevens die bewaard worden op vraag van een inlichtingendienst.

Zoals reeds vermeld is bij artikel 127/1 WEC over de toegang tot de gegevens door openbare overheden, moet vooreerst het principe van het EHJ herhaald worden over de proportionaliteit tussen de doeleinden van bewaring en de doeleinden van toegang. Volgens dit principe is de toegang tot de bewaarde gegevens enkel mogelijk voor dezelfde doeleinden als deze van de initiële bewaring of voor een doeleinde van algemeen belang dat minstens gelijkwaardig is. Het HvJ-EU stelt bovendien uitdrukkelijk dat de gegevens die bewaard worden voor nationale veiligheidsredenen niet toegankelijk zijn voor redenen van gewone misdrijven.

Wanneer de inlichtingendiensten op basis van hun organieke wet overgaan tot een algemene of gerichte bewaring van communicatiegegevens (verkeers- en lokalisatie), dan zijn deze gegevens – in toepassing van dit principe dat voortvloeit uit de rechtspraak van het EHJ- slechts toegankelijk voor andere publieke overheden in de gevallen waarin de toegang een algemeen doel nastreeft dat minstens een evenwaardig belang vertoont. Dit is welteverstaan niet van toepassing indien deze gegevens daarnaast al bewaard worden op basis van een andere bepaling (bijvoorbeeld artikel 126/1 WEC).

Ter illustratie van deze opmerking.

In geval van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, zoals een terroristische dreiging of een dreiging uitgaande van buitenlandse staatsinmenging, kan een algemene en ongedifferentieerde bewaring afgekondigd worden voor een hernieuwbare termijn van 6 maanden. Wanneer deze dreiging concreet wordt (bijvoorbeeld een bom ontploft in de metro, een buitenlandse overheid controleert de

immédiatement démarrer, et en particulier, dans l'optique d'identifier les auteurs d'une part et de démontrer le cas échéant les liens entre plusieurs auteurs d'autre part, il sera nécessaire d'utiliser les données d'identification, de localisation et de trafic antérieures à ce fait et conservées initialement pour les besoins des services de renseignement.

À l'identique, si un Quick Freeze est opéré sur des personnes qui représentent une menace pour la sécurité nationale et qu'il appert en outre que ces personnes commettent des faits de criminalité grave (car jacking) en lien ou pas avec leur projet initial, pour les besoins de l'enquête judiciaire qui va immédiatement démarrer, il sera nécessaire d'utiliser les données d'identification, de localisation et de trafic antérieures à ce fait et conservées initialement pour les besoins des services de renseignement.

Le Comité permanent R fait remarquer à juste titre (point 25) qu'il existe une différence entre la version néerlandophone et francophone en ce qui concerne les sanctions en cas de non-respect de l'obligation de conservation. Le texte a été adapté de manière à ce que tout refus de coopérer soit puni d'une amende allant de 26 euros à 20 000 euros. Toutefois, contrairement à l'article 39*quinquies*, § 3, alinéa 2 du CIC, la LRS ne prévoit pas de peine d'emprisonnement, et ce, afin de rester cohérent avec les autres dispositions pénales de la LRS.

Art. 29 (modifications à l'article 18/7)

La formulation de l'article 18/7 est alignée sur la formulation des autres méthodes de renseignement.

Par ailleurs, il est ajouté à l'article 18/7 que les services de renseignement peuvent également demander les factures relatives à un abonnement spécifique.

Afin de se conformer à l'avis du Comité permanent R (point 33), les auteurs du projet apportent une précision supplémentaire sur l'importance des données de facturation: s'il n'y a plus de conservation généralisée des données (cf. annulation des dispositions LCE), les données de facturation seront d'autant plus importantes. En effet, elles permettent de savoir à quels services et moyens de communication une personne s'est abonnée, quelle adresse et quel numéro de compte ont été fournis, etc. Une facture peut révéler, par exemple, que l'abonnement n'est pas payé par l'abonné mais par un tiers ou une société. Cela peut révéler de nouveaux liens entre des individus et des entreprises. Si la facture de téléphone d'un lobbyiste auprès d'une institution internationale

sociale media), is het ten behoeve van het strafonderzoek – dat onmiddellijk wordt ingesteld in het bijzonder voor de identificatie van de daders enerzijds en om desgevallend banden tussen meerdere daders aan te tonen, anderzijds – noodzakelijk gebruik te maken van de identificatie-, lokalisatie- en verkeersgegevens die dateren van voor de feiten en die initieel bewaard werden ten behoeve van de inlichtingendiensten.

Idem in het geval een "*quick freeze*" wordt uitgevoerd op personen die een bedreiging vormen voor de nationale veiligheid en van wie blijkt dat zij ernstige criminele feiten (car jacking) al dan niet gelieerd aan hun oorspronkelijk plan. Ten behoeve van het strafonderzoek dat onmiddellijk van start gaat, is het noodzakelijk om gebruik te maken van de identificatie-, lokalisatie- en verkeersgegevens die dateren van voor de feiten en die initieel bewaard werden voor de inlichtingendiensten.

Het Vast Comité I merkt terecht op (punt 25), dat er een verschil is tussen de Nederlandstalige versie en de Franstalige versie als het gaat over de straffen wegens niet-naleving van de bewaarplicht. De tekst werd in die zin aangepast dat weigering tot medewerking gestraft wordt met een geldboete van zesentwintig euro tot twintigduizend euro. In tegenstelling tot artikel 39*quinquies*, § 3, tweede lid Sv, bepaalt de WIV echter geen gevangenisstraf, dit om coherent te blijven met de andere strafbepalingen in de WIV.

Art. 29 (wijzigingen aan artikel 18/7)

De bewoording van artikel 18/7 wordt in lijn gebracht met de formulering van de andere inlichtingenmethoden.

In artikel 18/7 wordt eveneens ingevoegd dat de inlichtingendiensten ook de facturen met betrekking tot een welbepaald abonnement kunnen opgevraagd worden.

Om tegemoet te komen aan het advies van het Vast Comité I (punt 33), geven de redacteurs van het ontwerp verdere verduidelijking bij het belang van facturatiegegevens: als er geen algemene dataretentie meer is (zie vernietiging van de bepalingen van de WEC), zijn de facturatiegegevens des te belangrijker. Dit geeft immers zicht op de communicatiediensten en –middelen waarop men geabonneerd is, welk adres en rekeningnummer opgegeven is, … Uit een factuur kan bijvoorbeeld blijken dat het abonnement niet betaald wordt door de geabonneerde, maar door een andere persoon of door een bedrijf. Dit kan nieuwe linken tussen personen en bedrijven aan het licht brengen. Indien de telefoonrekening van lobbyist bij een internationale

est en fait payée par une ambassade étrangère, cela peut indiquer que ses activités sont contrôlées par une puissance étrangère ayant un agenda caché. Une facture contient également des données relatives au trafic de données qui ont un impact sur la facture. La facturation de services d'itinérance (roaming), par exemple, fournit des informations sur un séjour à l'étranger.

L'article 18/7, tel qu'inséré par la loi du 4 février 2010, prévoyait la possibilité de requérir la communication des factures relatives à des abonnements identifiés. Cette partie de la disposition avait été supprimée par la loi modificative du 5 février 2016 (art. 224) laquelle prévoyait cependant la possibilité de demander des informations sur le mode de paiement. L'article 26 du projet vise à réintroduire la partie supprimée de la disposition.

Art. 30 (modifications à l'article 18/8)

Dans son arrêt du 22 avril 2021, la Cour constitutionnelle a décidé d'annuler les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.

Elle justifie l'annulation de l'ensemble de ces dispositions par le fait qu'elles sont indissociablement liées à l'obligation de conservation générale et indifférenciée des données relatives aux communications électroniques par les opérateurs (voir points B.18 et B.20), principe considéré comme disproportionnel par la Cour de Justice de l'Union européenne dans ses arrêts du 6 octobre 2020.

L'article 14 de cette loi du 29 mai 2016 modifiait l'article 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cet article 18/8 porte sur l'accès aux données de communications électroniques par les services de renseignement et de sécurité et non sur la conservation de ces données. Seul le paragraphe 2 de cet article fait référence à l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.

Dès lors, seule l'annulation de ce paragraphe se justifie eu égard aux arrêts précités.

Les autres modifications visées à l'article 14 doivent donc être réintégrées.

L'article 18/8 ayant encore été modifié après la loi du 29 mai 2016, il est difficile de restituer la version en vigueur suite à l'annulation effectuée par la Cour. Les

instelling effectief betaald wordt door een buitenlandse ambassade, kan dit erop wijzen dat diens activiteiten gestuurd worden door een buitenlandse mogendheid met een verborgen agenda. Een factuur bevat ook verkeersgegevens die een invloed hebben op de factuur. Facturatie voor roamingdiensten, bijvoorbeeld, geeft informatie over een verblijf in het buitenland.

In artikel 18/7, zoals ingevoegd door de wet van 4 februari 2010, stond de bevoegdheid ingeschreven om de mededeling te vorderen van de facturen met betrekking tot de geïdentificeerde abonnementen. Dit deel van de bepaling werd geschrapt door de wetswijziging van 5 februari 2016 (art. 224). Er is toen wel de mogelijkheid ingevoerd om gegevens over de betalingswijze op te vragen. Artikel 26 van het ontwerp beoogt de herinvoering van dit geschrapt deel van de bepaling.

Art. 30 (wijzigingen aan artikel 18/8)

Bij arrest van 22 april 2021 heeft het Grondwettelijk Hof beslist om de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie te vernietigen.

Het Hof verantwoordt de vernietiging van het geheel van deze bepalingen door het feit dat deze onlosmakelijk verbonden zijn met de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie door de operatoren (zie punten B.18 en B.20), hetgeen door het Hof van Justitie van de Europese Unie als disproportioneel werd bevonden in haar arresten van 6 oktober 2020.

Artikel 14 van deze wet van 29 mei 2016 wijzigde artikel 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Dit artikel 18/8 betreft de toegang tot de gegevens met betrekking tot elektronische communicatie door de inlichtingen- en veiligheidsdiensten en niet de bewaring van deze gegevens. Enkel in paragraaf 2 van dit artikel werd gerefereerd naar artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Bijgevolg dringt zich enkel de vernietiging van deze paragraaf op in het licht van voormelde arresten.

De overige wijzigingen doorgevoerd door artikel 14 dienen bijgevolg opnieuw geïntegreerd te worden.

Gezien artikel 18/8 na de wet van 29 mei 2016 nogmaals werd gewijzigd, is het moeilijk om de versie van kracht ten gevolge van de vernietiging door het Hof te

auteurs du projet ont donc décidé, par sécurité juridique, de remplacer entièrement l'article 18/8.

Néanmoins, il convient de préciser qu'aucune modification n'est apportée à l'accès par les services de renseignement et de sécurité aux données de communications électroniques, ni à ses modalités.

La seule modification de l'article 18/8 consiste en la suppression du paragraphe 2 annulé par la Cour constitutionnelle.

L'accès aux données par les services de renseignement et de sécurité visé à l'article 18/8 porte bien entendu sur toutes les données conservées par les opérateurs, peu importe pour quelle finalité.

En effet, comme le précise la Cour de Justice de l'Union européenne dans son arrêt du 6 octobre 2020, en ses points 166 et 167, un accès à des données conservées pour un objectif de lutte contre la criminalité ou pour les besoins propres des opérateurs (facturation, marketing, sécurité des réseaux, …) est *a fortiori* justifié par l'objectif de sauvegarde de la sécurité nationale.

En réponse à un commentaire du Comité permanent R (points 16-18), les auteurs du projet souhaitent souligner qu'il n'y a plus de raison de moduler l'accès aux données, puisque l'accès dépendra de la durée de conservation effective et modulée. En outre, l'accès devra toujours être motivé de sorte que la Commission et le Comité permanent R puissent vérifier la proportionnalité, la subsidiarité et la légalité de l'historique demandé. Cette obligation de motivation a en effet été réintroduite, à la demande du Comité, à l'article 18/3, 2, 12°.

Art. 31 (modification à l'article 18/14)

Suite à une recommandation du Comité permanent R (point 35) et afin d'améliorer la lisibilité de la LRS, une modification purement technique est apportée à l'article 18/14. Une modification similaire sera apportée à l'article 18/15 à l'occasion de la révision complète de cet article.

Art. 32 (modification à l'article 18/17)

Suite à une recommandation du Comité permanent R (point 35) et pour améliorer la lisibilité de la LRS, une modification purement technique est apportée à l'article 18/17.

herstellen. De auteurs van het ontwerp hebben bijgevolg ervoor geopteerd om het volledige artikel 18/8 te vervangen omwille van redenen van rechtszekerheid.

Het is echter aangewezen om te preciseren dat geen enkele wijziging werd aangebracht aan de toegang tot de gegevens met betrekking tot de elektronische communicatie door de inlichtingen- en veiligheidsdiensten, noch aan de modaliteiten ervan.

De enige wijziging betreft de opheffing van paragraaf 2, die logischerwijze werd vernietigd door het Grondwettelijk Hof.

De toegang tot de gegevens door de inlichtingen- en veiligheidsdiensten bedoeld in artikel 18/8, heeft betrekking op alle gegevens bewaard door de operatoren, ongeacht de doelstelling.

Zoals het Hof van Justitie van de Europese Unie in zijn arrest van 6 oktober 2020 in de punten 166 en 167 heeft verklaard, is de toegang tot de gegevens die zijn bewaard met het oog op de bestrijding van criminaliteit of voor de eigen behoeften van de operatoren (facturatie, marketing, netwerkbeveiliging, enz.) *a fortiori* gerechtvaardigd ter vrijwaring van de nationale veiligheid.

In reactie op een opmerking van het Vast Comité I (punten 16-18) wensen de indieners van het ontwerp erop te wijzen dat er geen reden meer is om de toegang tot de gegevens te moduleren omdat de toegang zal afhangen van de effectieve, gemoduleerde, bewaartermijn. De toegang zal trouwens steeds gemotiveerd moeten worden zodat de Commissie en het vast Comité I de proportionaliteit, subsidiariteit en wettelijkheid van de opgevraagde historiek kunnen controleren. Deze motivatieplicht is trouwens, op vraag van het Comité, terug ingevoerd in artikel 18/3, 2, 12°.

Art. 31 (wijziging aan artikel 18/14)

Als gevolg van een aanbeveling van het Vast Comité I (punt 35) en ter bevordering van de leesbaarheid van de WIV, wordt een louter technische aangebracht aan artikel 18/14. Een gelijkaardige wijziging aan artikel 18/15 zal worden doorgevoerd ter gelegenheid van de volledige herziening van dat artikel.

Art. 32 (wijziging aan artikel 18/17)

Als gevolg van een aanbeveling van het Vast Comité I (punt 35) en ter bevordering van de leesbaarheid van de WIV, wordt een louter technische wijziging aangebracht aan artikel 18/17.

CHAPITRE 8

Modifications a la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 33 (modification à l'article 84)

Conformément aux articles 82, 2°, et 84 actuels de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, l'auditeur de la FSMA peut, moyennant l'autorisation préalable d'un juge d'instruction, requérir la communication des données de trafic et de localisation de communications électroniques et demander les détails de paiement des services de communications électroniques. Le présent projet vise à modifier l'article 84 de cette loi en instaurant, à certaines conditions, la possibilité pour l'auditeur de la FSMA d'ordonner, sans l'autorisation préalable d'un juge d'instruction, aux opérateurs d'un réseau de communications électroniques et à toute personne qui met à disposition ou offre, sur le territoire belge, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques (appelés ci-après "les opérateurs"), de conserver ces données temporairement (et de procéder ainsi à ce que l'on appellera ci-dessous un "*quick freeze*").

Il s'agit d'un "*quick freeze*" tel qu'autorisé à certaines conditions par l'arrêt Quadrature de la Cour de Justice de l'Union européenne rendu le 6 octobre 2020, mais avec une portée très limitée: il porte uniquement sur des données existantes qui, au moment où est émis l'ordre, sont encore conservées mais risquent d'être supprimées ou rendues anonymes le temps d'obtenir l'autorisation du juge d'instruction pour requérir ces données. Dans la mesure où l'auditeur de la FSMA ne peut requérir ces données que moyennant l'autorisation préalable du juge d'instruction, il s'écoule en effet toujours un laps de temps entre le moment où l'auditeur souhaite requérir les données et la demande proprement dite des données avec l'autorisation du juge d'instruction. Pour éviter que les données ne soient entre-temps plus disponibles, l'auditeur de la FSMA peut adresser aux opérateurs un ordre de *quick freeze* leur enjoignant de conserver ces données plus longtemps que durant les délais maximaux fixés par la loi du 13 juin 2005 relative aux communications électroniques (laquelle prévoit, plus précisément dans ses nouveaux articles 122, § 4/2, et 123, § 1er, 5°, une dérogation concernant les données qui sont nécessaires pour répondre à une obligation

HOOFDSTUK 8

Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 33 (wijziging aan artikel 84)

Overeenkomstig de bestaande artikelen 82, 2° en 84 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, kan de auditeur van de FSMA, mits voorafgaande toestemming van een onderzoeksrechter, de mededeling vorderen van verkeers- en locatiegegevens van elektronische communicatie en van betalingsdetails van elektronische communicatiediensten. In artikel 84 van deze wet wordt thans onder bepaalde voorwaarden de mogelijkheid ingevoerd voor de auditeur van de FSMA om, zonder de voorafgaande toestemming van een onderzoeksrechter, aan de operatoren van een elektronisch communicatienetwerk en iedereen die binnen het Belgisch grondgebied een dienst beschikbaar stelt of aanbiedt die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden (hierna "de operatoren" genoemd), te bevelen deze gegevens tijdelijk te bewaren (hierna "*quick freeze*" genoemd).

Het betreft een "*quick freeze*" zoals onder bepaalde voorwaarden toegelaten door het arrest Quadrature van het Europees Hof van Justitie van 6 oktober 2020, maar met een zeer beperkte draagwijdte: het betreft enkel bestaande gegevens, die op het moment van dit bevel nog bewaard worden, maar riskeren te worden verwijderd of anoniem gemaakt in afwachting van de toestemming van de onderzoeksrechter om deze gegevens op te vragen. Omdat de auditeur van de FSMA deze gegevens enkel kan opvragen met voorafgaande toestemming van de onderzoeksrechter, verstrijkt er immers steeds een periode tussen het moment waarop de auditeur de gegevens wenst op te vragen en de eigenlijke opvraging van de gegevens met toestemming van de onderzoeksrechter. Om te vermijden dat de gegevens intussen niet meer beschikbaar zijn, kan de auditeur van de FSMA met een bevel tot *quick freeze* aan de operatoren opleggen om deze gegevens langer te bewaren dan de maximale termijnen voorzien in de wet van 13 juni 2005 betreffende de elektronische communicatie (die hierop, met name in het nieuwe artikel 122, § 4/2 en artikel 123, § 1, 5°, een afwijking bepalen voor de gegevens die noodzakelijk zijn om gevolg te geven

légale dans le chef des opérateurs, telle qu'un *quick freeze* ordonné par l'auditeur de la FSMA).

Cette possibilité de *quick freeze* n'est en outre prévue que pour les violations de l'interdiction d'abus de marché (articles 14 ou 15 du Règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché)), qui constituent de la criminalité grave. Leur impact sur l'intégrité des marchés financiers et sur la confiance des investisseurs est en effet important. Il s'agit, au sein du secteur financier, de l'une des infractions les plus graves, comme en témoignent notamment le fait que ces violations peuvent donner lieu à des amendes maximales d'un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement et à la plupart des autres législations financières (voir notamment l'article 36, § 2, de la loi du 2 août 2002), ainsi que le fait que les mêmes faits (sous réserve de la présence d'une intention) sont également passibles de sanctions pénales (voir les articles 39 et 40 de la loi du 2 août 2002). Dans le cadre des enquêtes généralement longues et complexes qui concernent les abus de marché, les données de communications électroniques jouent souvent un rôle important dans l'administration de la preuve, par exemple pour constater que des personnes ont, à un moment donné, été en contact l'une avec l'autre et qu'il existe une relation entre deux ou plusieurs personnes.

Pour répondre à l'observation formulée par le Conseil d'État, selon laquelle il convient de limiter le pouvoir de *quick freeze* à des faits dont le caractère de gravité est établi ou peut être présumé par l'auditeur, il est précisé que ce pouvoir n'est applicable qu'en cas d'indices sérieux d'une violation de l'interdiction d'abus de marché, c'est-à-dire d'une infraction qui doit toujours être considérée comme grave. En complément des éléments déjà fournis à l'alinéa précédent et au regard de l'observation du Conseil d'État selon laquelle, bien que les montants maximaux prévus soient élevés, les sanctions en question sont de nature administrative et non pénale, il y a lieu de relever qu'il peut être déduit de la conclusion formulée par l'avocat général dans l'arrêt Ministerio Fiscal de la Cour de justice (C-207/16) que la notion de criminalité grave dans la jurisprudence de la Cour de justice de l'Union européenne n'est pas limitée aux faits passibles d'une sanction pénale (et en particulier d'une peine d'emprisonnement). En effet, l'avocat général indique notamment ce qui suit: "(…) Ainsi, le fait qu'un État membre prévoie une peine d'emprisonnement peu élevée, voire une peine alternative à l'emprisonnement, ne préjuge pas pour autant de la gravité intrinsèque du type d'infraction concerné" (n° 98) et "(…) la sanction encourue ne saurait être considérée comme pouvant

aan een wettelijke verplichting in hoofde van de operatoren, waaronder ook een *quick freeze* op bevel van de auditeur van de FSMA begrepen wordt).

Bovendien wordt deze mogelijkheid tot *quick freeze* enkel voorzien voor inbreuken op het verbod op marktmisbruik (artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik)), wat zware criminaliteit uitmaakt. De impact daarvan op de integriteit van de financiële markten en het vertrouwen van de beleggers is immers groot. Binnen de financiële sector gaat het om één van de meest ernstige inbreuken, wat o.m. blijkt uit het feit dat er voor deze inbreuken aanzienlijk hogere minimale maximumboetes voorzien zijn dan voor de inbreuken op andere bepalingen van de verordening en op de meeste andere financiële wetgeving (zie met name artikel 36, § 2, van de wet van 2 augustus 2002), alsook uit het feit dat er op dezelfde feiten (mits de aanwezigheid van opzet) ook strafrechtelijke sancties staan (artikelen 39 en 40 van de wet van 2 augustus 2002). In het kader van de doorgaans complexe en tijdsintensieve onderzoeken inzake marktmisbruik spelen elektronische communicatiegegevens dikwijls een belangrijke rol in de bewijsvoering, bijvoorbeeld om vast te stellen dat personen op een bepaald moment met elkaar in contact zijn geweest en er tussen twee of meer personen een relatie bestaat.

In antwoord op de opmerking van de Raad van State dat de bevoegdheid tot *quick freeze* dient te worden beperkt tot feiten waarvan de ernst door de auditeur is vastgesteld of wordt vermoed, wordt erop gewezen dat deze bevoegdheid enkel geldt in geval van ernstige aanwijzingen van een inbreuk op het verbod van marktmisbruik, i.e. een inbreuk die steeds als zwaar te beschouwen is. Aanvullend op de in de vorige alinea reeds vermelde elementen en in het licht van de opmerking van de Raad van State dat het, hoewel de voorziene maxima hoog zijn, administratieve en geen strafsancties betreft, wordt erop gewezen dat uit de conclusie van de advocaat-generaal bij het arrest Ministerio Fiscal van het Hof van Justitie (C-207/16) kan worden afgeleid dat het begrip van zware criminaliteit in de rechtspraak van het Europees Hof van Justitie niet beperkt is tot feiten waarop een strafsanctie (en met name een gevangenisstraf) staat. De advocaat-generaal gaf immers onder meer het volgende aan: "(…) Zo zegt het feit dat een lidstaat op een bepaald strafbaar feit een korte gevangenisstraf of zelfs een alternatieve straf stelt, niets over de intrinsieke ernst van het type strafbaar feit."(nr. 98) en "(…) dat de voorgeschreven straf noch vanuit de kwalitatieve invalshoek van het soort straf, noch vanuit de kwantitatieve invalshoek van de strafmaat de enige maatstaf kan zijn om de bijzondere

refléter à elle seule, que ce soit sous l'angle qualitatif du type de peine et/ou sous l'angle quantitatif du niveau de peine, la particulière gravité d'une infraction pénale" (n° 104). Des faits passibles d'amendes administratives très élevées peuvent donc également être qualifiés de criminalité grave. Tel est le cas pour les infractions aux articles 14 et 15 du règlement relatif aux abus de marché, qui sont passibles d'amendes administratives maximales de 5 millions d'euros pour les personnes physiques et de 15 millions d'euros, ou si le montant obtenu par application de ce pourcentage est plus élevé, de 15 % du chiffre d'affaires annuel total pour les personnes morales (voir l'article 36, § 2, alinéa 2, 2°, de la loi du 2 août 2002). Il est en outre souligné que les amendes administratives pouvant être imposées pour abus de marché sont des sanctions administratives à caractère pénal au sens de la jurisprudence de la Cour européenne des droits de l'homme. Dans ce cadre, il est important que les interdictions administratives dont la violation est alléguée, visent à sauvegarder l'intérêt général de la société, normalement protégé par le droit pénal, et que la sanction, en raison du montant maximal qu'elle peut théoriquement atteindre, vise, par son caractère dissuasif, à prévenir de tels actes et à éviter la récidive et, par son caractère punitif, à sanctionner une irrégularité (voir, en ce sens, notamment les considérants 94 et suivants de l'arrêt Grande Stevens de la CEDH, n° 18640/10, rendu le 4 mars 2014, et les références y citées). Les mêmes faits sont en outre également passibles de sanctions pénales pouvant aller jusqu'à quatre ans d'emprisonnement en cas de manipulation de marché et de délit d'initié et jusqu'à deux ans d'emprisonnement en cas de divulgation d'informations privilégiées (voir les articles 39 et 40 de la loi du 2 août 2002). Il s'agit là de sanctions considérablement plus lourdes que l'emprisonnement maximal d'une durée d'un an retenu comme seuil minimal à l'article 39*quinquies*, en projet, du Code d'instruction criminel, auquel le Conseil d'État se réfère (et par ailleurs aussi à l'article 88*bis* dudit Code). Il est donc incontestable que de tels faits d'abus de marché sont considérés comme graves. L'auditeur de la FSMA réclame par ailleurs les données de communication électroniques en phase d'instruction (préliminaire), à un moment où il n'est en général pas encore clair si les faits feront l'objet de poursuites administratives ou pénales, et il demande ainsi ces données également aux fins du contrôle du respect des articles 39 et 40 de la loi du 2 août 2002 (voir aussi l'article 82, 2°, juncto l'article 35, § 1er, 1°, de la loi du 2 août 2002). Enfin, il se fait aussi que la réglementation européenne, et en particulier l'article 23, paragraphe 2, h), du règlement relatif aux abus de marché, impose que, dans la mesure où le droit national autorise que les enregistrements existants de données relatives au trafic détenus par un opérateur soient réclamés (ce qui est le cas en Belgique), les autorités administratives compétentes telles que la

ernst van een strafbaar feit te beoordelen" (nr. 104). Ook feiten waarop erg hoge administratieve geldboetes staan, kunnen dus kwalificeren als zware criminaliteit. Dit is het geval voor inbreuken op de artikelen 14 en 15 van de Verordening marktmisbruik, waarop maximale administratieve geldboetes staan van 5 miljoen euro voor natuurlijke personen en van 15 miljoen euro of, indien dit hoger is, 15 procent van de totale jaaromzet voor rechtspersonen (zie artikel 36, § 2, tweede lid, 2°, van de wet van 2 augustus 2002). Bovendien wordt benadrukt dat deze voor marktmisbruik voorziene administratieve geldboetes administratieve sancties met een strafkarakter zijn in de zin van de rechtspraak van het Europees Hof voor de rechten van de mens. Daarbij is het van belang dat de administratieve verbodsbepalingen waarvan een schending wordt verweten tot doel hebben het algemeen belang van de samenleving te vrijwaren, dat normaal beschermd wordt door het strafrecht, en de sanctie, omwille van het maximum dat zij theoretisch kan bereiken, door haar ontradend karakter, tot doel heeft dergelijke handelingen te voorkomen en recidive te vermijden, en, door haar punitief karakter, een onregelmatigheid te sanctioneren (zie in die zin onder meer overwegingen 94 en volgende van het arrest Grande Stevens van het EHRM van 4 maart 2014, nr. 18640/10, en de daar geciteerde referenties). Daarnaast zijn voor dezelfde feiten ook strafrechtelijke sancties voorzien die kunnen oplopen tot vier jaar gevangenisstraf voor marktmanipulatie en handel met voorwetenschap en tot twee jaar gevangenisstraf voor mededeling van voorwetenschap (zie artikelen 39 en 40 van de wet van 2 augustus 2002). Dit is aanzienlijk hoger dan de maximum gevangenisstraf van één jaar die als minimum drempel werd weerhouden in artikel 39*quinquies* van het Wetboek van Strafvordering in ontwerp, waarnaar de Raad van State verwijst (en overigens ook in artikel 88*bis* van hetzelfde wetboek). Het staat bijgevolg buiten kijf dat dergelijke feiten van marktmisbruik als zwaar beschouwd worden. De auditeur van de FSMA vraagt overigens de elektronische communicatiegegevens op in de fase van het (voor)onderzoek, op een moment dat meestal nog niet duidelijk is of de feiten administratief dan wel strafrechtelijk zullen worden vervolgd, en vraagt deze gegevens aldus ook op voor doeleinden van het toezicht op de naleving van de artikelen 39 en 40 van de wet van 2 augustus 2002 (zie ook artikel 82, 2°, juncto artikel 35, § 1, 1°, van de wet van 2 augustus 2002). Tenslotte is het ook zo dat Europese regelgeving, en met name artikel 23, lid 2, h), van de Verordening marktmisbruik, vereist dat indien de nationale wetgeving toestaat dat bestaande verkeersgegevensoverzichten waarover een operator beschikt, worden opgevraagd (wat in België het geval is), ook de bevoegde administratieve autoriteiten zoals de FSMA deze gegevens moeten kunnen opvragen wanneer er een redelijk vermoeden bestaat van en wanneer dergelijke overzichten relevant kunnen zijn voor het onderzoek naar

FSMA doivent également pouvoir requérir ces données lorsqu'il existe des motifs raisonnables de suspecter une violation de l'interdiction de délit d'initié ou de celle de manipulation de marché, et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à ladite violation.

Les garanties matérielles et procédurales nécessaires sont à cet égard prévues:

— le *quick freeze* n'est possible qu'à des fins bien déterminées, à savoir en vue d'éviter, lors de la détection, l'examen et la poursuite d'abus de marché (tant par la FSMA que dans le cadre d'une demande de coopération émanant d'autorités compétentes d'autres États membres de l'EEE ou de pays tiers qui sont dotées de pouvoirs comparables à ceux de la FSMA), que des données de trafic et de localisation nécessaires à la manifestation de la vérité ne soient supprimées ou rendues anonymes, dans l'attente de l'obtention de l'autorisation d'un juge d'instruction pour requérir ces données;

— seul l'auditeur (ou, en son absence, l'auditeur adjoint) de la FSMA peut ordonner le *quick freeze*;

— l'auditeur (ou, en son absence, l'auditeur adjoint) indique dans son ordre de *quick freeze* les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver son ordre, des principes de proportionnalité et de subsidiarité. Il doit, dans ce cadre, mentionner notamment la ou les personnes qui font l'objet de l'ordre de conservation, les catégories de données de trafic et de localisation qui doivent être conservées et la période du passé sur laquelle porte l'ordre. Il doit en outre préciser les motifs pour lesquels ces données peuvent contribuer à la mise au jour d'abus de marché et les raisons pour lesquelles elles risquent d'être supprimées ou rendues anonymes par les opérateurs de télécommunications, par exemple par suite du respect des délais de conservation limités prévus par la loi du 13 juin 2005 relative aux communications électroniques;

— il s'agit d'une conservation d'une durée limitée, à savoir jusqu'à ce que l'auditeur ait reçu d'un juge d'instruction l'autorisation de requérir ces données;

— les opérateurs doivent veiller à ce que l'intégrité des données soit garantie et à ce que les données soient conservées de manière sécurisée;

— toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours,

een inbreuk op het verbod op handel met voorwetenschap of marktmanipulatie.

Ter zake worden de nodige materiële en procedurele waarborgen voorzien:

— de *quick freeze* is enkel mogelijk voor welbepaalde doeleinden, met name om bij het opsporen, onderzoeken en vervolgen van marktmisbruik (zowel door de FSMA als in het kader van een verzoek tot samenwerking van bevoegde autoriteiten van andere lidstaten van de EER of van derde staten met bevoegdheden die vergelijkbaar zijn met die van de FSMA) te vermijden dat verkeers- en locatiegegevens die noodzakelijk zijn om de waarheid aan de dag te brengen, worden verwijderd of anoniem gemaakt, in afwachting van het bekomen van de toestemming van een onderzoeksrechter om deze gegevens op te vragen;

— enkel de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) van de FSMA kan de *quick freeze* bevelen;

— de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) doet in zijn bevel tot *quick freeze* opgave van de feitelijke omstandigheden die de maatregel rechtvaardigen en hij houdt rekening met het evenredigheids- en subsidiariteitsbeginsel bij de motivering van zijn bevel. Daarbij dient hij met name de persoon of personen waarop de bewaring betrekking heeft, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden en de periode in het verleden waarover het bevel zich uitstrekt, te vermelden. Bovendien moet hij motiveren waarom deze gegevens kunnen bijdragen tot het aan het licht brengen van marktmisbruik en waarom ze riskeren te worden verwijderd of anoniem te worden gemaakt door de telecomoperatoren, zo bijvoorbeeld als gevolg van de beperkte bewaartermijnen bepaald in de wet van 13 juni 2005 betreffende de elektronische communicatie;

— het gaat om een bewaring voor een beperkte tijd, met name totdat de auditeur de toestemming van een onderzoeksrechter heeft bekomen voor de opvraging van deze gegevens;

— de operatoren moeten ervoor zorgen dat de integriteit van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden;

— iedere persoon die uit hoofde van zijn functie kennis krijgt van de maatregel of daaraan zijn medewerking

est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal;

— bien que l'auditeur ne soit pas tenu, pour ordonner le *quick freeze*, d'obtenir préalablement l'autorisation d'un juge d'instruction (contrairement à ce qui est le cas pour la demande de communication des données), un contrôle juridictionnel effectif sera toutefois bel et bien opéré (a posteriori): le juge d'instruction amené à statuer sur la demande d'autorisation préalable qui lui est adressée par l'auditeur en vue de requérir les données, se prononcera également sur le *quick freeze*. S'il estime que le *quick freeze* n'était pas légitime ou pas justifié ou s'il refuse, pour une autre raison, de donner l'autorisation de requérir les données de trafic et de localisation qui font l'objet du *quick freeze*, ce *quick freeze* prendra fin et l'auditeur (ou, en son absence, l'auditeur adjoint) de la FSMA en avisera l'opérateur concerné. À la suggestion du Conseil d'État, il a été ajouté dans le projet de loi que cette demande à un juge d'instruction d'une autorisation pour requérir la communication des données doit intervenir sans délai, ceci afin de garantir un contrôle juridictionnel rapide. Notons par ailleurs que, dans le cadre d'une éventuelle procédure ultérieure, il sera également question d'un contrôle juridictionnel opéré a posteriori: dans le cas de poursuites pénales, par la chambre de mise en accusation et le juge du fond qui se prononce sur la régularité de la procédure et des actes d'investigation; dans le cas d'une procédure de sanction administrative, par la Cour des marchés qui statue sur le recours formé contre les décisions de sanction de la FSMA et qui se prononce éventuellement aussi sur la régularité de la procédure et des actes d'investigation.

verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek;

— hoewel de auditeur voor de *quick freeze* niet voorafgaand de toestemming van een onderzoeksrechter moet bekomen (in tegenstelling tot voor de vordering tot mededeling van de gegevens), vindt er (a posteriori) wel een effectieve rechterlijke controle plaats: de onderzoeksrechter die oordeelt over het verzoek van de auditeur tot voorafgaande toestemming om de gegevens op te vragen, zal ook oordelen over de *quick freeze*. Indien hij oordeelt dat de *quick freeze* niet wettig of niet gerechtvaardigd was of indien hij om een andere reden de toestemming weigert om de verkeers- en locatiegegevens die het voorwerp uitmaken van de *quick freeze* op te vragen, komt de *quick freeze* ten einde en brengt de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) van de FSMA de betrokken operator hiervan op de hoogte. Ingevolge een suggestie van de Raad van State, werd in het wetsontwerp toegevoegd dat dit verzoek aan een onderzoeksrechter tot toestemming voor de opvraging van de gegevens, onverwijld dient te gebeuren. Aldus wordt een snelle rechterlijke controle verzekerd. Daarnaast is het zo dat er in het kader van een eventuele latere procedure ook een a posteriori rechterlijke controle zal plaatsvinden: in geval van strafvervolging, door de kamer van inbeschuldigingstelling en de rechter ten gronde die de regelmatigheid van de procedure en de onderzoeksdaden beoordeelt, in geval van een administratieve sanctieprocedure, door het Marktenhof dat oordeelt over het beroep tegen de sanctiebeslissingen van de FSMA en dat desgevallend ook de regelmatigheid van de procedure en de onderzoeksdaden beoordeelt.

CHAPITRE 9

HOOFDSTUK 9

Modification a la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS")

Wijziging aan de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet")

Art. 34 (remplacement de l'article 62)

L'article 34 prévoit une nouvelle formulation de l'article 62 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS"). Les paragraphes 1er, 3 et 4 reprennent le contenu actuel des alinéas 1 à 4 de l'article 62. Le nouveau paragraphe 2 habilite quant à lui le CCB, en tant que CSIRT national, à demander des données relatives à l'utilisateur

Art. 34 (vervanging van artikel 62)

Artikel 34 bevat een nieuwe formulering van artikel 62 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet"). De paragrafen 1, 3 en 4 nemen de huidige inhoud van lid 1 tot 4 van artikel 62 over. De nieuwe paragraaf 2 machtigt het CCB, als nationaal CSIRT, om gegevens op te vragen over de gebruiker of

ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, x 91°de la loi du 13 juin 2005 relative aux communications électroniques auprès des opérateurs de communications électroniques, lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches légales énumérées à l'article 60, a) à e) de la loi NIS.

Les tâches du CSIRT national reprises à l'article 60, a) à e), de la loi NIS visent la diffusion d'informations sur les risques et incidents en matière de sécurité des réseaux et systèmes d'information, l'intervention en cas d'incident, l'analyse dynamique des risques et incidents, ainsi que la détection, l'observation et l'analyse des problèmes de sécurité informatique.

Il s'agit pour le CSIRT national de protéger notamment les autorités publiques ou les opérateurs de services essentiels au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Ce sont des entités publiques ou privées qui exercent une activité en Belgique liée à la fourniture d'un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques.

Ces opérateurs de services essentiels remplissent un rôle important dans des secteurs clés, tels que l'énergie, l'eau potable, la santé ou encore les transports maritimes, ferroviaires et routiers. Les incidents pour lesquels le CSIRT national assure des missions de suivi, d'intervention mais aussi de détection et de prévention, peuvent, par exemple, avoir pour conséquence de rendre inopérante la distribution d'électricité ou de rendre indisponibles des services de transport. En ce qu'ils affectent des acteurs essentiels de secteurs clés ou des pouvoirs publics, ces incidents constituent des menaces graves pour la sécurité publique.

Le CSIRT national joue également un rôle de prévention, de recherche et de détection en matière d'infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave.

Le CSIRT national (Centre pour la Cybersécurité Belgique, ci-après le "CCB") doit être en mesure, le cas échéant, d'obtenir des différents opérateurs, des données de communications électroniques afin d'accomplir ses missions légales. Les finalités poursuivies par ces différentes tâches sont énumérées à l'alinéa 2. Il s'agit notamment de la prévention de menaces graves contre la sécurité publique, de l'examen de défaillances de la

abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens als bedoeld in artikel 2, x 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie bij elektronische-communicatieoperatoren, indien dat strikt noodzakelijk is voor de uitvoering van zijn wettelijke taken opgesomd in artikel 60, a) tot e), van de NIS-wet.

De taken van het nationale CSIRT vermeld in artikel 60, a) tot e), van de NIS-wet betreffen het verspreiden van informatie over risico's en incidenten rond de beveiliging van netwerk- en informatiesystemen, het reageren op incidenten, de dynamische risico- en incidentanalyse, alsook het opsporen, observeren en analyseren van computerbeveiligingsproblemen.

Het nationale CSIRT dient met name overheden of aanbieders van essentiële diensten als bedoeld in de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid te beschermen. Dit zijn publieke of private entiteiten die een activiteit uitoefenen in België met betrekking tot de verlening van een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten.

Die aanbieders van essentiële diensten spelen een belangrijke rol in sleutelsectoren zoals energie, drinkwater, gezondheidszorg of nog, vervoer over water, spoorvervoer en vervoer over de weg. Incidenten waarvoor het nationale CSIRT opdrachten vervult op het vlak van monitoring en reactie maar ook van opsporing en preventie, kunnen er bijvoorbeeld toe leiden dat de elektriciteitsdistributie buiten werking wordt gesteld of vervoersdiensten niet meer beschikbaar zijn. Aangezien deze incidenten essentiële spelers in sleutelsectoren of overheden treffen, vormen zij een ernstige bedreiging voor de openbare veiligheid.

Het nationale CSIRT speelt ook een rol op het vlak van het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten.

Het nationale CSIRT (Centrum voor Cybersecurity België, hierna het "CCB") moet in voorkomend geval immers in staat zijn om van de verschillende operatoren elektronische-communicatiegegevens te verkrijgen teneinde zijn wettelijke opdrachten te vervullen. De doeleinden van deze verschillende taken worden opgesomd in het tweede lid. Het betreft met name het voorkomen van ernstige bedreigingen voor de openbare

sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information, de la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques (en ce compris des faits qui relèvent de la criminalité grave).

Les dispositions actuelles de la loi NIS n'autorisent pas de manière suffisamment explicite le CSIRT national à demander aux opérateurs de communications électroniques des données de communications électroniques qu'ils conservent, ce qui pose des problèmes pratiques.

Le paragraphe 2 vise à doter explicitement le CSIRT national de ce pouvoir et d'encadrer de telles demandes.

Le troisième alinéa prévoit que le CSIRT national peut obtenir des données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, moyennant l'autorisation d'un supérieur hiérarchique compétent.

Il s'agit ici pour le CSIRT national de fournir à l'opérateur un identifiant spécifique (par exemple, une adresse IP) afin de connaître la personne physique ou morale utilisateur de cet identifiant. Une adresse IP est générée sans être rattachée à une communication déterminée et sert principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique ou morale propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'internet est effectuée.

Une telle demande de données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ne permet donc pas de tirer des conclusions précises sur la vie privée d'une éventuelle personne physique (le traçage du parcours de navigation d'un internaute, établir son profil détaillé ou déterminer ses différentes localisations).

Dans le respect des finalités, de tâches légales et des mesures de contrôle précités, le CSIRT national pourra ainsi identifier auprès d'un opérateur de communications électroniques l'utilisateur d'un identifiant spécifique, sans commettre une ingérence grave dans les droits fondamentaux des éventuelles personnes physiques concernées.

Lorsque la demande du CSIRT national dépasse le cadre d'une donnée relative à l'utilisateur ou à l'abonné et peut constituer une ingérence grave dans la vie privée

veiligheid, het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen, het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd (met inbegrip van zware criminele feiten).

De huidige bepalingen van de NIS-wet machtigen het nationale CSIRT onvoldoende duidelijk om elektronische-communicatiegegevens op te vragen bij elektronische-communicatieoperatoren die deze gegevens bewaren, wat praktische problemen oplevert.

Paragraaf 2 heeft tot doel deze bevoegdheid uitdrukkelijk toe te kennen aan het nationale CSIRT en een kader te creëren voor de verzoeken om toegang.

Het derde lid bepaalt dat het nationale CSIRT gegevens kan verkrijgen over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, mits een bevoegde hiërarchische meerdere hiervoor toestemming verleent.

Het nationale CSIRT bezorgt de operator daarbij een specifieke identificatiecode (bijvoorbeeld een IP-adres) om de natuurlijke of rechtspersoon te kennen die deze identificatiecode gebruikt. Een IP-adres wordt los van een bepaalde communicatie gegenereerd en dient voornamelijk om via aanbieders van elektronische-communicatiediensten de natuurlijke of rechtspersoon te identificeren die eigenaar is van de eindapparatuur waarmee via het internet wordt gecommuniceerd.

Een dergelijk verzoek om gegevens over de gebruiker of abonnee als bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector laat dus niet toe precieze conclusies te trekken over de persoonlijke levenssfeer van een eventuele natuurlijke persoon (de navigatieroute van een internetgebruiker traceren, een gedetailleerd profiel van hem opstellen of zijn verschillende locaties bepalen).

Met inachtneming van de voornoemde doeleinden, wettelijke taken en controlemaatregelen kan het nationale CSIRT dus de gebruiker van een specifieke identificatiecode bij een elektronische-communicatieoperator identificeren, zonder dat er sprake is van een ernstige inmenging in de fundamentele rechten van de eventuele betrokken natuurlijke personen.

Als het verzoek van het nationale CSIRT verder gaat dan een gegeven over de gebruiker of abonnee en een ernstige inmenging in de persoonlijke levenssfeer

de personnes physiques, celle-ci doit alors être soumise aux conditions plus strictes énoncées au quatrième alinéa.

Le quatrième alinéa permet au CSIRT national d'obtenir, après autorisation préalable de l'Autorité de protection des données créé par la loi du 3 décembre 2017, des métadonnées de communications électroniques au sens de l'article 2, 91° de la loi du 13 juin 2005 relative aux communications électroniques autres que des données relatives à l'utilisateur ou à l'abonné.

Le cinquième alinéa précise qu'en cas de situation urgente dûment justifiée, le CSIRT national peut se passer de l'Autorité de protection des données créé par la loi du 3 décembre 2017 pour obtenir des métadonnées de communications électroniques.

Comme l'a souligné l'Autorité de protection des données dans son avis, l'existence d'une urgence particulière, qui est dûment justifiée, peut, en effet, justifier de se passer d'un contrôle préalable tel défini par la jurisprudence de la Cour de Justice de l'Union européenne.

En pratique, ce mécanisme permet au CSIRT national d'intervenir rapidement notamment en cas de situation de crise nationale en matière de cybersécurité.

Dans ce cas, la demande d'obtenir les données doit alors être communiquée sans délai à l'Autorité de protection des données créé par la loi du 3 décembre 2017.

De plus, le CCB demeure soumis aux contrôles juridictionnels de droit commun de l'administration, à savoir soit le contrôle des juridictions judiciaires, soit le contrôle de la section du contentieux administratif du Conseil d'État. Il est également soumis au contrôle de l'Autorité de protection des données.

Le sixième alinéa dispose que le directeur du CSIRT national désigne expressément les personnes habilitées à traiter ces données de communications électroniques. Cette disposition a pour objectif de limiter l'accès aux données concernées seulement à une catégorie restreinte de personnes chargées d'accomplir certaines tâches pour le compte du CSIRT national.

Enfin, le dernier alinéa impose au CSIRT de prévenir, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement des ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées. Cette disposition entend mettre

van natuurlijke personen kan vormen, moet dit worden onderworpen aan de striktere voorwaarden vermeld in het vierde lid.

Het vierde lid laat het nationale CSIRT toe om, na voorafgaande machtiging van de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017, elektronische-communicatiemetagegevens te verkrijgen als bedoeld in artikel 2, 91° , van de wet van 13 juni 2005 betreffende de elektronische communicatie die geen gegevens over de gebruiker of abonnee zijn.

Het vijfde lid verduidelijkt dat het nationale CSIRT zich in dringende en naar behoren gemotiveerde gevallen elektronische-communicatiemetagegevens kan verkrijgen zonder raadpleging van de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017.

Zoals de Gegevensbeschermingsautoriteit heeft opgemerkt in haar advies, kan het bestaan van een naar behoren gemotiveerde dringende situatie immers rechtvaardigen dat er geen voorafgaand toezicht zoals bepaald door de rechtspraak van het Hof van Justitie van de Europese Unie plaatsvindt.

Dankzij dit mechanisme kan het nationale CSIRT in de praktijk vlug optreden, met name in een nationale crisissituatie op het vlak van cyberbeveiliging.

In dat geval moet het verzoek tot het verkrijgen van de gegevens onverwijld worden meegedeeld aan de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017.

Bovendien blijft het CCB onderworpen aan de gemeenrechtelijke rechterlijke controle op het bestuur, namelijk de toetsing door gewone rechtscolleges of de toetsing door de afdeling bestuursrechtspraak van de Raad van State. Het is eveneens onderworpen aan het toezicht van de Gegevensbeschermingsautoriteit.

Het zesde lid bepaalt dat de directeur van het nationale CSIRT uitdrukkelijk de personen aanwijst die gemachtigd zijn om deze elektronische-communicatiegegevens te verwerken. Doel van deze bepaling is ervoor te zorgen dat enkel een beperkte categorie van personen die bepaalde taken uitvoeren voor rekening van het nationale CSIRT, toegang krijgt tot de betrokken gegevens.

Tot slot bepaalt het laatste lid dat het CSIRT de betrokken natuurlijke personen voor zover mogelijk op de hoogte moet brengen van de toegang tot hun elektronische-communicatiegegevens, als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd. Deze bepaling beoogt

en œuvre le principe de transparence et d'information vis-à-vis des personnes concernées, pour autant que cela ne préjudicie pas aux actions en cours.

Art. 35 (modification à l'article 65)

Cet article insère au sein du paragraphe 2 de l'article 65 de la loi NIS les termes "des données de communications électroniques," parmi les données pouvant être traitées par le CSIRT national, afin notamment de satisfaire au prescrit de l'article 23, § 2, (b) du RGPD.

CHAPITRE 10

Modification de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits

Art. 36 (modification à l'article 11)

Cet article instaure une possibilité d'identification sur la base d'une adresse IP ou d'un numéro de téléphone, suite aux nouvelles dispositions introduites aux articles 127, § 1er, et 127/1, § 1er, de la loi de la loi du 13 juin 2005 relative aux communications électroniques (ci-après loi Télécom). Le commerce en ligne explose. Par conséquent, de plus en plus de particuliers et d'entreprises vendent des biens et des services en ligne. Ceci a pour conséquence que l'Inspection Produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement doit elle aussi se concentrer de plus en plus sur le contrôle de ce commerce en ligne. Afin de pouvoir exercer correctement son rôle d'autorité de surveillance du marché, elle doit disposer des instruments juridiques appropriés.

Le caractère hautement anonyme qu'offre internet pour les vendeurs forme à cet égard un important défi à relever. Souvent, l'adresse IP et le numéro de téléphone sont les seules données que le service d'inspection peut obtenir grâce à la coopération de la plateforme en ligne où l'infraction a été commise. Il est donc très important que le service d'inspection puisse identifier au moyen de ces données ceux qui commettent des infractions à la mise sur le marché de produits, en demandant la mise à disposition de documents et de données d'identification à l'opérateur d'un réseau de communications électroniques et au fournisseur d'un service de communications électroniques. Il s'agit des données d'identité mentionnées à l'article 127, § 1er, de la loi Télécom: ex. nom, prénom, date de naissance de l'abonné et/ou une copie de sa pièce d'identité (ex. passeport).

uitvoering te geven aan de beginselen van transparantie en voorlichting van de betrokkenen, voor zover dit geen afbreuk doet aan lopende acties.

Art. 35 (wijziging aan artikel 65)

Dit artikel voegt in paragraaf 2 van artikel 65 van de NIS-wet de woorden "elektronische-communicatiegegevens," toe aan de gegevens die door het nationale CSIRT kunnen worden verwerkt, om met name te voldoen aan artikel 23, lid 2, (b), van de AVG.

HOOFDSTUK 10

Wijziging van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere produkten

Art. 36 (wijziging aan artikel 11)

Dit artikel voert de mogelijkheid in om een identiteit te achterhalen op grond van het IP-adres of telefoonnummer, in navolging van de nieuwe bepalingen in artikelen 127, § 1, en 127/1, § 1, van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna Telecomwet). Online handel groeit explosief. Er zijn dan ook steeds meer personen en ondernemingen die goederen en diensten online verkopen. Dit heeft als gevolg dat ook de Inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu zich meer en meer moet toespitst op het controleren van deze online handel. Om haar rol als markttoezichtautoriteit op een degelijke manier te kunnen uitvoeren, moet zij over de juiste juridische instrumenten beschikken.

De grote anonimiteit die het internet biedt aan verkopers, vormt hierbij een belangrijke uitdaging. Vaak zijn het IP-adres of het telefoonnummer de enige gegevens die de inspectiedienst kan bekomen door medewerking van de online marktplaats waarop de inbreuk werd begaan. Daarom is het van groot belang dat de inspectiedienst diegenen, die inbreuken begaan bij het op de markt brengen van producten, kan identificeren aan de hand van deze gegevens, door identificatiegegevens te vorderen van de operator van een elektronisch communicatienetwerk en verstrekker van een elektronische communicatiedienst. Het gaat over de identiteitsgegevens vermeld in artikel 127, § 1, van de Telecomwet: bijv. naam, voornaam, geboortedatum en/of een kopie van zijn identiteitsstuk (bijv. paspoort).

L'autorisation accordée offre des garanties suffisantes pour assurer le respect de la vie privée des personnes: seul le numéro de téléphone ou l'adresse IP à la source d'une communication électronique sera utilisé, et pour autant que cette communication soit publique: Il peut s'agir par exemple de l'adresse IP sous laquelle un compte de vente a été créé ou une annonce de vente a été placée, ou du numéro de téléphone renseigné dans une offre en ligne. De plus, à la suite de cette autorisation, des mesures organisationnelles et techniques seront mises en œuvre au sein du SPF Santé après avoir effectué une analyse d'impact sur la protection des données (AIPD) afin d'identifier et de réduire les risques pour la vie privée liés à ce traitement des données.

Chaque demande d'identification doit être approuvée au préalable, par le chef du service d'inspection concerné du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement.

CHAPITRE 11

Dispositions transitoires

Art. 37

L'alinéa 1er de cet article prévoit l'entrée en vigueur de l'article 126/1, § 3, premier alinéa, 3° à 5° de la loi du 13 juin 2005 relative aux communications électroniques. L'entrée en vigueur de ces dispositions sera déterminée par un arrêté royal délibéré en Conseil des ministres, et au plus tard le 1er janvier 2027.

L'alinéa 2 du présent article prévoit que, soit le 1er janvier 2026, soit à la date fixée par le Roi avant cette date, les autorités compétentes pour l'une des matières visées par ces dispositions transmettent les informations nécessaires à la détermination concrète des zones géographiques au service désigné par le Roi.

Vu qu'il s'agit de la première application de cet article, le délai d'un an permettra au service désigné par le Roi de disposer du temps nécessaire pour réaliser la première carte.

Art. 38

Cet article prévoit une période transitoire entre l'entrée en vigueur de la loi et la publication de l'arrêté ministériel visé à l'article 126/1, § 3, alinéa 1er, 1° de la loi du 13 juin 2005 relative aux communications électroniques. Cet arrêté ministériel établit la liste des

De machtiging biedt voldoende waarborgen voor het respect van het privéleven van personen: er wordt enkel het IP-adres of telefoonnummer gebruikt dat aan de bron ligt van de elektronische communicatie en voor zover deze openbaar van aard is: het gaat bijvoorbeeld over het IP adres waaronder een verkoopaccount werd aangemaakt of een verkoopadvertentie werd geplaatst of over het telefoonnummer vermeld in een online aanbieding. Bovendien worden binnen de FOD Volksgezondheid naar aanleiding van deze bevoegdheid organisatorische en technische maatregelen doorgevoerd als gevolg van een Data Protection Impact Assessment (DPIA) om privacy-risico's van deze gegevensverwerking in kaart te brengen en ze te verkleinen.

De identificatieverzoek dient voorafgaand door het hoofd van de betreffende inspectiedienst van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden.

HOOFDSTUK 11

Overgangsbepalingen

Art. 37

Dit artikel bepaalt de inwerkingtreding van artikel 126/1, § 3, eerste lid, 3° tot 5° van de wet van 13 juni 2005 betreffende de elektronische communicatie. De inwerkingtreding van deze bepalingen zal bepaald worden bij een in Ministerraad overlegd besluit, en ten laatste op 1 januari 2027.

Het tweede lid van het onderhavige artikel bepaalt dat ofwel op 1 januari 2026, ofwel op de datum vastgesteld door de Koning vóór die datum, de autoriteiten die bevoegd zijn voor een van de materies die door deze bepalingen worden beoogd, de informatie die nodig is voor de concrete bepaling van de geografische gebieden verzenden naar de door de Koning aangewezen dienst.

Aangezien het gaat om de eerste toepassing van het artikel zal de termijn van een jaar de door de Koning aangewezen dienst de nodige tijd geven om de eerste kaart tot stand te brengen.

Art. 38

Dit artikel voorziet in een overgangsperiode tussen de inwerkingtreding van de wet en de publicatie van het ministerieel besluit bedoeld in artikel 126/1, § 3, eerste lid, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie. Dit ministerieel besluit

arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que leur durée de conservation. En effet, entre l'entrée en vigueur de la loi et la publication du cet arrêté ministériel, il y aurait une période d'incertitude concernant la durée de conservation des données visée à l'article 126/1 § 2 sur la base des critères visés à l'article 126/1 § 3, alinéa 1er, 1° de la même loi. Cet article prévoit donc que les ministres de la Justice et de l'Intérieur déterminent la durée de conservation qui s'appliquera jusqu'à la publication de cet arrêté ministériel.

Le ministre de la Justice,

Vincent VAN QUICKENBORNE

stelt de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn. Tussen de inwerkingtreding van de wet en de publicatie van dit ministerieel besluit zou immers een periode van onzekerheid zijn betreffende de bewaartermijn van de gegevens bedoeld in artikel 126/1, § 2 op basis van de criteria bedoeld in artikel 126/1, § 3, eerste lid, 1° van dezelfde wet. Daarom voorziet dit artikel dat de ministers van Justitie en van Binnenlandse Zaken de bewaartermijn bepalen die zal gelden tot de publicatie van dit ministerieel besluit.

De minister van Justitie,

Vincent VAN QUICKENBORNE

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités

Chapitre 1er - Disposition générale

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Chapitre 2 - Modifications à la loi du 13 juin 2005 relative aux communications électroniques

Art. 2. À l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, au lieu du 74°, annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un 74° rédigé comme suit:

"74° "Appels infructueux": toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau.".

Art. 3. Dans l'article 9 de la loi du 13 juin 2005 relative aux communications électroniques, le paragraphe 7 est abrogé.

Art. 4. Dans l'article 122 de la même loi, les modifications suivantes sont apportées:

1° Dans le paragraphe 1er:

Le mot "finals" est remplacé par le mot "finaux";

L'alinéa 2 est supprimé;

2° Dans le paragraphe 2:

l'alinéa 1er est remplacé par ce qui suit:

"§ 2. Par dérogation au § 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs peuvent conserver et traiter les données de trafic nécessaires à cette fin."

dans l'alinéa 2, les mots "de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" sont remplacés par les mots "du RGPD et de la loi du 30 juillet 2018";

3° Dans le paragraphe 3:

dans l'alinéa 1er, 2°, les mots "la manifestation de volonté libre, spécifique et basée sur des informations par laquelle

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten

Hoofdstuk 1 - Algemene bepaling

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Hoofdstuk 2 - Wijzigingen aan de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 2. In artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, in de plaats van de bepaling onder 74°, vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een als volgt luidende bepaling onder 74° ingevoegd:

"74° "Oproeppoging zonder resultaat": een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord.".

Art. 3. In artikel 9 van de wet van 13 juni 2005 betreffende de elektronische communicatie wordt paragraaf 7 opgeheven.

Art. 4. In artikel 122 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° In paragraaf 1:

Wordt in de Franstalige versie het woord "finals" vervangen door het woord "finaux";

Wordt het tweede lid geschrapt;

2° In paragraaf 2:

wordt het eerste lid vervangen als volgt:";

"§ 2. In afwijking van § 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken".

worden in het tweede lid de woorden "van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "van de AVG en van de wet van 30 juli 2018";

3° In paragraaf 3:

worden in het eerste lid, 2° de woorden "de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene

l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées" sont remplacés par les mots "le consentement au sens de l'article 4 du RGPD";

dans l'alinéa 1er, 3°, les mots "utilisateurs finals la possibilité de retirer le consentement donné de manière simple" sont remplacés par les mots "utilisateurs finaux la possibilité de retirer le consentement donné facilement et à tout moment.";

dans l'alinéa 2, les mots "de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" sont remplacés par les mots "du RGPD et de la loi du 30 juillet 2018";

4° Le paragraphe 4 est remplacé comme suit:

"§ 4. Pour l'application du présent paragraphe, une fraude est un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite, commis par le biais de l'utilisation d'un service de communications électroniques.

Pour l'application du présent paragraphe, une utilisation malveillante du réseau est une utilisation du réseau afin d'importuner son correspondant ou de provoquer des dommages.

Par dérogation au § 1er, sans prendre connaissance du contenu des communications et dans le seul but de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine, les opérateurs:

1° conservent les données de localisation et les autres données de trafic nécessaires à cette fin, le temps nécessaire à cette fin et au minimum quatre mois;

2° traitent les données de trafic nécessaires à cette fin, en ce compris, lorsque c'est nécessaire, les données visées au paragraphe 2.

Lorsqu'un opérateur a détecté une fraude potentielle ou avérée ou une utilisation malveillante potentielle ou avérée du réseau, il prend les mesures appropriées, compte tenu des possibilités techniques les plus récentes, pour éviter que l'utilisateur final ne subisse un préjudice ou ne soit importuné.

Afin d'établir une utilisation malveillante d'un réseau de communications électroniques et de retrouver son auteur, les opérateurs conservent pendant 12 mois les données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles.

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et des Autorité de protection des données compétentes:

1° les données de trafic visées aux alinéas 3 et 5;

of zijn wettelijke vertegenwoordiger aanvaardt dat verkeersgegevens die op hem betrekking hebben worden verwerkt" vervangen door de woorden "de toestemming in de zin van artikel 4 van de AVG";

worden in het eerste lid, 3° de woorden "op eenvoudige wijze" vervangen door de woorden "makkelijk en te allen tijde";

worden in het tweede lid de woorden "van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "van de AVG en van de wet van 30 juli 2018";

4° Paragraaf 4 wordt vervangen als volgt:

"§ 4. Voor de toepassing van deze paragraaf bestaat fraude in een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of het contract en om zichzelf of iemand anders een ongeoorloofd voordeel te doen, via het gebruik van een elektronische-communicatiedienst.

Voor de toepassing van deze paragraaf bestaat kwaadwillig gebruik van het netwerk in een gebruik van het netwerk teneinde zijn contactpersoon te ontrieven of schade te berokkenen.

In afwijking van § 1, zonder kennis te nemen van de inhoud van de communicatie en met als enig doel een vermoed geval van fraude of van kwaadwillig gebruik van een elektronische-communicatienetwerk op te sporen en te analyseren, inclusief de herkomst ervan:

1° bewaren de operatoren de locatiegegevens en andere verkeersgegevens die daartoe nodig zijn, gedurende de tijd die ervoor nodig is en minstens vier maanden;

2° verwerken de operatoren de noodzakelijke gegevens daartoe, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.

Wanneer een operator een mogelijk of bewezen geval van fraude of een mogelijk of bewezen geval van kwaadwillig gebruik van het netwerk heeft opgespoord, neemt hij de gepaste maatregelen, rekening houdend met de meest recente technische mogelijkheden, om te vermijden dat de eindgebruiker schade ondervindt of wordt ontriefd.

Om kwaadwillig gebruik van een elektronisch communicatienetwerk vast te stellen en de dader ervan te vinden, bewaren de operatoren gedurende 12 maanden de verkeersgegevens in verband met de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de bevoegde gegevensbeschermingsautoriteiten, bepalen:

1° de verkeersgegevens bedoeld in het derde en vijfde lid;

2° les actions que l'opérateur doit ou peut entreprendre lorsqu'il détecte une fraude présumée ou avérée ou une utilisation malveillante présumée ou avérée du réseau.

Les données visées aux alinéas 3 et 5 sont communiquées aux autorités compétentes en cas d'infraction présumé."

5° Un paragraphe 4/1 est inséré, rédigé comme suit:

"§ 4/1. Par dérogation au § 1er, les opérateurs conservent et traitent les données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

Ils les conservent pour une durée de douze mois. Ils peuvent les conserver pour une durée plus longue, qui est limitée au strict nécessaire."

6° Un paragraphe 4/2 est inséré, rédigé comme suit:

"§ 4/2. Par dérogation au § 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation légale dans leur chef, pour la durée requise à cette fin."

7° Le paragraphe 5 est remplacé comme suit:

"§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services à données de trafic ou de localisation et par les membres de sa Cellule de coordination. "

8° Dans le paragraphe 6, les mots "L'Institut" sont remplacé par les mots "L'Institut, le Service de médiation pour les télécommunications,".

9° Il est inséré un paragraphe 7, rédigé comme suit:

"§ 7. Cet article ne porte pas préjudice à l'article 127/1."

Art. 5. À l'article 123 de la même loi, les modifications suivantes sont apportées

1° L'alinéa 1er est remplacé comme suit:

"§ 1er. Sans préjudice de l'application du RGPD et de la loi du 30 juillet 2018, les opérateurs de réseaux mobiles ne peuvent conserver et traiter de données de localisation autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final que dans les cas suivants:

2° de acties die de operator moet of mag ondernemen wanneer hij een vermoed of bewezen geval van fraude of van kwaadwillig gebruik van het netwerk heeft opgespoord.

De gegevens bedoeld in het derde en vijfde lid worden meegedeeld aan de bevoegde autoriteiten in geval van vermoed misdrijf."

5° Een paragraaf 4/1 wordt ingevoerd, luidend:

"§ 4/1. In afwijking van § 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om de veiligheid en correcte werking van hun netwerken en diensten voor elektronische communicatie te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

Zij bewaren deze voor een duur van twaalf maanden. Zij kunnen ze voor een langere periode bewaren, die beperkt is tot het strikt noodzakelijke."

6° Een paragraaf 4/2 wordt ingevoerd, luidende:

"§ 4/2. In afwijking van § 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een wettelijke verplichting die op hen rust, voor de daartoe benodigde duur."

7° Paragraaf 5 wordt vervangen als volgt:

"§ 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten met verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel. "

8° In paragraaf 6 worden de woorden "het Instituut" vervangen door de woorden "het Instituut, de Ombudsdienst voor telecommunicatie,".

9° Er wordt een paragraaf 7 ingevoegd, luidende:

"§ 7. Dit artikel doet geen afbreuk aan artikel 127/1."

Art. 5. In artikel 123 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de eerste paragraaf wordt vervangen als volgt:

"§ 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen:

1° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées le temps nécessaire à cette fin;

2° lorsque cela est nécessaire pour déceler des fraudes ou l'utilisation malveillante du réseau, les données étant conservées le temps nécessaire à cette fin ou;

3° lorsque les données ont été rendues anonymes, ou;

4° lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation, ou;

5° lorsque le traitement est nécessaire pour répondre à une obligation légale dans le chef de l'opérateur."

2° Dans le paragraphe 2:

Dans le 1°, e), les mots "définitivement ou temporairement"sont abrogés;

Dans le 2°, alinéa 2, les mots "la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données de localisation se rapportant à lui soient traitées" sont remplacés par les mots "le consentement au sens de l'article 4 du RGPD".

3° Le paragraphe 4, alinéa 1er est remplacé par ce qui suit:

"§ 4. Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit le service à données de trafic ou de localisation, ou par la Cellule de coordination de l'opérateur visée à l'article 127/3.";

4° Il est inséré un paragraphe 6, rédigé comme suit:

"§ 6. Cet article ne porte pas préjudice à l'article 127/1.".

Art. 6. L'article 125, § 2, de la même loi est abrogé.

Art. 7. Dans l'article 126 de la même loi, les modifications suivantes sont apportées:

1° Le paragraphe 1er est remplacé comme suit:

"§ 1. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données de souscription de l'abonné ainsi que les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, pour autant qu'ils traitent ou génèrent ces données dans le cadre de la fourniture des réseaux ou services de communications concernés.

1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is;

2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is; of;

3° wanneer de gegevens anoniem gemaakt zijn, of;

4° wanneer de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens, of;

5° wanneer de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting in hoofde van de operator."

2° In paragraaf 2:

Worden in het 1°, e), de woorden "definitief of tijdelijk" opgeheven;

Worden in het 2°, tweede lid, de woorden "de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat locatiegegevens die op hem betrekking hebben worden verwerkt" vervangen door de woorden "de toestemming in de zin van artikel 4 van de AVG".

3° Paragraaf 4, eerste lid, wordt vervangen als volgt:

"§ 4. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst met verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator waarvan sprake in artikel 127/3.";

4° Er wordt een paragraaf 6 ingevoegd, luidende:

"§ 6. Dit artikel doet geen afbreuk aan artikel 127/1.".

Art. 6. Artikel 125, § 2, van dezelfde wet wordt opgeheven.

Art. 7. In artikel 126 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° Het paragraaf 1 wordt vervangen als volgt:

"§ 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken leveren, de abonnementsgegevens van de abonnee alsook de technische gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, op voorwaarde dat ze deze gegevens in het kader van de verstrekking van de communicatienetwerken of -diensten in kwestie verwerken of genereren.

Le présent article ne porte pas sur le contenu des communications.

Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1.

Les données visées au présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Par dérogation à l'alinéa 3, les adresses IP dynamiques, autres que celle qui a été utilisée pour souscrire au service, sont conservées jusqu'à douze mois après la fin de la session."

2° Le paragraphe 2 est remplacé comme suit:

"§ 2. Le Roi fixe après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver ainsi que les exigences auxquelles ces données doivent répondre."

Art. 8. Dans la même loi, un article 126/1 est inséré comme suit:

"126/1. § 1er. Sans préjudice du RGDP et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées au paragraphe 2, pour les zones géographiques visées au paragraphe 3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans le présent article.

Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communication concernés.

Ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.

§ 2. Les données visées au paragraphe 1er sont les suivantes:

1° les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau;

2° les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination;

3° les données des appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés:

Dit artikel heeft geen betrekking op de inhoud van de communicatie.

Deze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1.

De in dit artikel beoogde gegevens worden bewaard vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is.

In afwijking van het derde lid worden de andere dynamische IP-adressen dan diegene die is gebruikt om in te tekenen op de dienst, tot twaalf maanden na het einde van de sessie bewaard."

2° De tweede paragraaf wordt vervangen als volgt:

"§ 2. De Koning bepaalt, na advies van de bevoegde Gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens alsook de vereisten waaraan deze gegevens moeten beantwoorden."

Art. 8. In dezelfde wet, wordt een artikel 126/1 ingevoegd, luidende:

"126/1. § 1. Onverminderd de AVG en de wet van 30 juli 2018, dienen de operatoren die aan de eindgebruikers elektronische communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische communicatienetwerken aanbieden, de in paragraaf 2 bedoelde gegevens voor de geografische zones bedoeld in paragraaf 3, te bewaren, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in huidig artikel.

Elke operator bewaart de door hem gegenereerde of verwerkte gegevens in het kader van de verstrekking van de betrokken communicatiediensten en -netwerken.

Deze gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

§ 2. De gegevens bedoeld in paragraaf 1 zijn:

1° de gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt;

2° de communicatiegegevens, met uitzondering van de inhoud, en met inbegrip van hun herkomst en hun bestemming;

3° de gegevens van oproeppogingen zonder resultaat, voor zover die gegevens in het kader van de aanbieding van de bedoelde communicatiediensten:

i° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs; ou

ii° en ce qui concerne les données de l'internet, journalisées par ces opérateurs.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre et du ministre de la Justice, du ministre de l'Intérieur, du ministre de la défense, et du ministre, après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver et peut fixer les exigences auxquelles ces données doivent répondre.

§ 3. Les zones géographiques dans lesquelles sont conservées les données visées au paragraphe 2 sont les suivantes:

1° la zone géographique composée des:

arrondissements judiciaires dans lesquels au moins 3 infractions visées à l'article 90*ter* du Code d'instruction criminelle par 1000 habitants par an ont été constatées durant l'année sur une moyenne des troisannées calendriers précédentes celle en cours;

zones de police, dans lesquelles, au moins 3infractions visées à l'article 90*ter* du Code d'instruction criminelle par 1000 habitants par an ont été constatées sur une moyenne des trois années calendriers précédentes celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier précédente celle en cours, moins de 3 infractions visées à l'article 90*ter* du Code d'instruction criminelle par 1000 habitants par an sur une moyenne de trois années précédente celle en cours ont été constatées.

Dans l'hypothèse visée au 1er tiret, le délai de conservation des données visées au paragraphe 2 est de:

a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90*ter* du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois dernières années calendriers précédentes celle en cours;

b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90*ter* du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours;

c) 12 mois, s'il y a 7 ou plus de 7 d'infractions visées à l'article 90*ter* du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours.

Dans l'hypothèse visée au deuxième tiret, le délai de conservation des données visées au paragraaf 2 est de:

a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90*ter* du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois dernières années calendriers précédentes celle en cours;

i° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren; of

ii° wat de internetgegevens betreft, door deze operatoren worden gelogd.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens en kan de vereisten waaraan deze gegevens moeten beantwoorden bepalen.

§ 3. De geografische zones waarbinnen de gegevens bedoeld in paragraaf 2 bewaard worden, zijn de volgende:

1° de geografische zones bestaande uit:

de gerechtelijke arrondissementen waar minstens 3 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drievoorbije kalenderjaren;

de politiezones waar minstens 3strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan 3 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de 3 voorbije kalenderjaren.

In het geval bedoeld in het eerste streepje bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2:

a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per jaar per 1000 inwonders vastgesteld zijn in de drie voorbije kalenderjaren;

c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de 3 voorbije kalenderjaren.

In het geval bedoeld in het tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf2:

a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90*ter* du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours;

c) 12 mois, s'il y a 7 ou plus de 7 infractions visées à l'article 90*ter* du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers précédentes celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non 5.

Les statistiques utilisées proviennent de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police.

La direction visée à l'article 44/11 de la loi sur la fonction de police transmet chaque année, à la date déterminée par le Roi, ces statistiques à l'Organe de contrôle de l'information policière qui, dans les [quinze] jours après leur réception, vérifie leur exactitude et en informe le service désigné par le Roi.

2° Toutes les zones dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones.

3° Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave, à savoir:

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2., 3°, 4° et 5° de la Code de la Navigation;

b) les gares au sens de l'article 2, 5° de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du Titre III de la Constitution;

f) les bâtiments affectés à la police locale et à la police fédérale;

b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren.

c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet 5 bereikt.

De gebruikte statistieken zijn afkomstig van de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet op het politieambt.

De directie, zoals bedoeld in artikel 44/11 van de wet op het politieambt, zendt jaarlijks op de door de Koning vastgestelde datum deze statistieken toe aan het Controleorgaan op de politionele informatie dat, binnen de [vijftien] dagen na ontvangst, de juistheid ervan controleert en de door de Koning aangewezen dienst ervan in kennis stelt.

2° Alle zones waar het algemene dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2° van de wet van 10 juli 2006 betreffende de dreigingsanalyse, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de dreigingsanalyse, en zolang niveau 3 blijft bestaan.

3° De gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2., 3°, 4° en 5° van het Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5° van de Wet van 27 april 2018 houdende de spoorwegpolitie;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad, alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden;

e) de gebouwen bestemd voor de instellingen bedoeld in Titel III, hoofdstukken 5 tot 7 van de Grondwet;

f) de gebouwen bestemd voor de lokale en de federale politie;

g) les bâtiments affectés à l'administration des douanes et accises;

h) les communes dans lesquelles se trouvent des domaines militaires;

i) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;

j) les maisons de transition visées dans la loi du 17 mai 2006 relative au statut juridique externe des personnes condamnées à une peine privative de liberté et aux droits reconnus à la victime dans le cadre des modalités d'exécution de la peine;

k) les armuriers et les stands de tir au sens de l'article 2, points 1 et 19 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

l) les établissements visés à l'article 3.1.a) de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

m) les établissements SEVESO visés dans l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

n) les communes dans lesquelles il y a une ou plusieurs infrastructures critiques visées dans la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques;

o) le réseau utilisé par la S.A. Astrid et ses infrastructures ainsi que le réseau et les infrastructures du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

p) les réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de service essentiels désignés sur base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

q) le cas échéant, les autres zones fixées par arrêté royal.

4° Les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:

g) de gebouwen bestemd voor de administratie van douane en accijnzen;

h) de gemeenten waar zich militaire domeinen bevinden;

i) de gevangenissen in de zin van artikel 2, 15°, van de Basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gesteld, bedoeld in artikel 606 van het Wetboek van Strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de interning;

j) de transitiehuizen als bedoeld in de wet van 17 mei 2006 betreffende de externe rechtspositie van de veroordeelden tot een vrijheidsstraf en de aan het slachtoffer toegekende rechten in het raam van de strafuitvoeringsmodaliteiten;

k) de wapenkamers en schietstanden zoals bedoeld in artikel 2, punten 1 en 19 van de Wet van 8 juni 2006 houdende de economische en individuele activiteiten met wapens;

l) de faciliteiten bedoeld in artikel 3.1.a) van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

m) de SEVESO-inrichtingen zoals bedoeld in het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

n) de gemeenten waar zich kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren;

o) het door de N.V. Astrid gebruikte netwerk en haar infrastructuren, evenals het netwerk en het beveiligde en versleutelde communicatie- en informatiesysteem bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

p) de informatienetwerken en –systemen die de verlening van essentiële diensten van operatoren van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid;

q) in voorkomend geval, de andere zones vastgesteld bij Koninklijk besluit.

4° De zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, met name:

a) en matière d'ordre public, les zones neutres et les cabinets ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la sécurité sur proposition du ministre de la Justice et de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenant;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:

i) les assemblées législatives au sens de l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) les sièges des conseils provinciaux;

iv) le palais royal;

v) les domaines royaux;

vi) les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du Titre III de la Constitution;

vii) les communes dans lesquelles se trouvent des domaines militaires;

viii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu' à la Sûreté de l'État;

e) pour ce qui concerne l'intégrité du territoire national les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:

i) les hôpitaux au sens de l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soin;

ii) la Banque nationale de Belgique;

g) le cas échéant, les autres zones fixées par arrêté royal.

5° Les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national, à savoir:

a) voor de openbare orde, de neutrale zones en de ministeriële kabinetten;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden die zijn opgenomen in een lijst die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst wordt opgesteld op voorstel van de minister van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ii) de gemeentehuizen;

iii) de zetels van de provincieraden;

iv) het koninklijk paleis;

v) de koninklijke domeinen;

vi) de gebouwen toegewezen aan de instellingen bedoeld in Titel III, hoofdstukken 5 tot 7 van de Grondwet;

vii) de gemeenten waar zich militaire domeinen bevinden;

viii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;

e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:

i) de ziekenhuizen zoals bedoeld in artikel 2 van de Gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;

g) in voorkomend geval, de andere zones vastgesteld bij koninklijk besluit.

5° De zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, met name:

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union Européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) les bureaux des institutions de l'Espace économique européen;

e) les bureaux des Nations unies;

f) le cas échéant, les autres zones fixées par arrêté royal.

Chaque autorité compétente dans l'une des matières visées aux points 1° à 5° transmet chaque année à la date déterminée par le Roi et au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.

Ces autorités informent sans délai ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée au paragraphe 1er dans cette zone.

Chaque année et chaque fois qu'il est informé d'une modification, le service désigné par le Roi met à jour la liste des zones géographiques soumises à l'obligation de conservation et transmet cette liste aux opérateurs.

À l'exception de la liste des lieux visés à l'alinéa 1er, point 4°, b), mise à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière la liste actualisée des zones où une conservation de données est obligatoire.

La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1er, point 1°.

§ 4. Les opérateurs conservent les données pour toutes les communications effectuées à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone.

Lorsqu'un utilisateur final entre dans une zone visée au paragraphe 3 ou sort de cette zone, les seules données conservées sont celles traitées ou générées lorsqu'il se trouve dans cette zone.

Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée au paragraphe 3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent à cet effet la localisation satellitaire d'un équipement terminal.

a) de ambassades en diplomatieke vertegenwoordigingen;

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuren bestemd voor de NAVO;

d) de kantoren van de instellingen van de Europese Economische Ruimte;

e) de kantoren van de Verenigde Naties;

f) in voorkomend geval, de andere zones vastgesteld bij Koninklijk besluit.

Elke autoriteit die bevoegd is voor een van de in de punten 1 tot en met 5 bedoelde aangelegenheden deelt jaarlijks op de door de Koning vastgestelde datum aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de operationele tenuitvoerlegging van dit lid.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld in paragraaf 1 in deze zone zo spoedig mogelijk kan worden beëindigd.

Elk jaar en telkens wanneer hij van een wijziging in kennis wordt gesteld, werkt de door de Koning aangewezen dienst de lijst van de onder de geografische gebieden waar de gegevens moeten bewaard worden bij en zendt hij deze lijst door aan de operatoren.

Met uitzondering van de in het eerste lid, punt 4°, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten ter beschikking van het vast Comité I wordt gesteld, stelt de Koning aangewezen dienst de bijgewerkte lijst van zones waar de bewaring van gegevens verplicht is, ter beschikking van het Controleorgaan van de politionele informatie.

De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°.

§ 4. De operatoren bewaren de gegevens voor alle communicaties die vanuit of naar een geografisch gebied als bedoeld in paragraaf 3 worden gevoerd.

Wanneer een eindgebruiker een in paragraaf 3 bedoelde zone binnengaat of deze zone verlaat, worden alleen de gegevens bewaard die zijn verwerkt of gegenereerd wanneer hij zich in deze zone bevond.

Om te bepalen of eindapparatuur zich in een geografisch gebied als bedoeld in paragraaf 3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens die beschikbaar zijn. Zij maken hiervoor gebruik van de satellietlocatie van eindapparatuur.

Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.

§ 5. Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la défense, et du ministre, et après avis des Autorités de protection des données compétentes et de l'Institut, les éléments suivants:

— les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées au paragraphe 3;

— la liste des différentes autorités compétentes dans les matières visées au paragraphe 3, alinéa 1er, points 2° à 5°;

— les modalités de communication des informations par les autorités compétentes vers le service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er;

— s'il y échet, les zones géographiques additionnelles visées au paragraphe 3, alinéa 1er, points 3°, q), 4°, g) et 5° f).

L'arrêté royal visé à l'alinéa 1er, 4ème tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1er en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal.

§ 6. Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et de la Sécurité, et de l'Institut et des autorités de protection des données compétentes, un rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 5, afin de vérifier si des dispositions doivent être adaptées.

Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 5 répondent toujours aux critères visés au paragraphe 3, alinéa 1er, points 3° à 5° et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.

Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.

Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.

§ 5. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister, na raadpleging van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, het volgende bepalen:

— de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones;

— de lijst van de verschillende autoriteiten die bevoegd zijn voor de in paragraaf 3, eerste lid, punten 2° tot en met 5° bedoelde aangelegenheden;

— de procedures voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de procedures voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen;

— in voorkomend geval, de bijkomende geografische zones bedoeld in paragraaf 3, eerste lid, punten 3°, q), 4° g) en 5°,f).

Elke drie jaar dient het koninklijk besluit bedoeld in het eerste lid, 4e streepje te worden hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 voor wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt."

§ 6. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité voor Inlichtingen en Veiligheid, en van het Instituut en de bevoegde gegevensbeschermingsautoriteiten, jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 5 bedoelde Koninklijk Besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 5, bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in paragraaf 3, eerste lid, punten 3° tot 5° of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit

Ce rapport est envoyé à l'Organe de contrôle de l'information policière.

Pour la première application du présent article:

— les opérateurs concernés le mettent en œuvre dans les trois mois après l'entrée en vigueur de l'arrêté royal visé au paragraphe 2, alinéa 2;

— les autorités compétentes visées au paragraphe 3, alinéa 2 transmettent les informations nécessaires au service désigné par le Roi le mois qui suit l'entrée en vigueur de la loi.".

Art. 9. Dans la même loi, l'article 127 est remplacé par ce qui suit:

"Art. 127. § 1er. Les opérateurs identifient leurs abonnés ou collectent et conservent les données nécessaires pour que les autorités qui sont habilitées à obtenir cette identité puissent les identifier.

Ces données et documents sont conservés pour les autorités et les finalités visées à l'article 127/1.

Les données et documents collectés en vertu du présent article sont conservés à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

§ 2. Lorsque l'abonné présente un document d'identification comprenant le numéro de registre national, l'opérateur, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.

Afin d'identifier l'abonné, l'opérateur ou le canal de vente de services de communications électroniques peut réaliser, de manière automatique, une comparaison entre les paramètres biométriques sur la photo de la pièce d'identité de l'abonné et ceux de son visage.

Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur ou à l'entreprise fournissant un service d'identification.

Si une introduction directe dans les systèmes informatiques de l'opérateur ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.

L'opérateur conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Dit evaluatierapport wordt gestuurd naar het controleorgaan op de politionele informatie.

Bij de eerste toepassing van huidig artikel:

— leggen de betrokken operatoren dit artikel ten uitvoer binnen drie maanden na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 2, tweede lid;

— delen de paragraaf 3, tweede lid bedoelde bevoegde autoriteiten de nodige gegevens mee aan de door de Koning aangewezen dienst op de maand volgend op de inwerkingtreding van de wet.".

Art. 9. In dezelfde wet, wordt het artikel 127 vervangen als volgt:

"Art. 127. § 1. De operatoren identificeren hun abonnees of verzamelen en bewaren de nodige gegevens opdat de autoriteiten die gemachtigd zijn om deze identiteit te verkrijgen, hen kunnen identificeren.

Deze gegevens en documenten worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1.

De gegevens en documenten vergaard krachtens dit artikel, worden bewaard vanaf de datum van activering van de dienst tot twaalf maanden na de datum vanaf wanneer communicatie voor het laatst mogelijk is aan de hand van de gebruikte dienst.

§ 2. Wanneer de abonnee een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.

Teneinde de abonnee te identificeren, kan de operator of het verkoopkanaal van elektronische-communicatiediensten automatisch een vergelijking uitvoeren tussen de biometrische gegevens op de foto van het identiteitsstuk van de abonnee en deze van zijn gezicht.

Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator of naar de onderneming die een identificatiedienst verstrekt.

Indien een rechtstreekse invoer in de computersystemen van de operator of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.

De operator bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.

§ 3. Le Roi peut, après avis des Autorités de protection des données compétentes et de l'Institut, déterminer les modalités d'identification de l'utilisateur final, et entre autres:

1° déterminer si l'opérateur doit lui-même identifier ses abonnés ou s'il peut seulement rendre cette identification possible;

2° déterminer les méthodes d'identification que les opérateurs peuvent utiliser, y compris soumettre une méthode d'identification proposée par un opérateur à une autorisation préalable du ministre et du ministre de la Justice;

3° déterminer les données et documents d'identification à collecter et à conserver par l'opérateur;

4° imposer des obligations aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification et aux utilisateurs finaux, en vue de l'identification de ces derniers.

Sauf preuve contraire, l'abonné est présumé utiliser lui-même le service de communications électroniques.

§ 4. Si un opérateur ne respecte pas les mesures qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

Les opérateurs déconnectent les abonnés qui ne respectent pas les mesures qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces abonnés ne sont en aucune manière indemnisés pour la déconnexion."

Art. 10. Dans la même loi, un article 127/1 est inséré comme suit:

"Art 127/1, § 1er. Seules les autorités suivantes peuvent obtenir, via la Cellule de coordination visée à l'article 127/3 des opérateurs des données conservées en vertu des articles 122, 123, 126, 126/1, et 127 pour les finalités ci-dessous et dans les conditions prévues par les dispositions qui les y habilitent:

1° les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne;

2° les services de renseignement et de sécurité afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

3° les autorités chargées d'apporter de l'aide aux personnes, en ce compris le service de médiation pour les

§ 3. De Koning kan, na advies van de bevoegde gegevensbeschermingsautoriteiten en het Instituut, de nadere bepalingen voor identificatie van de eindgebruiker vastleggen, en onder andere:

1° bepalen of de operator zelf zijn abonnees moet identificeren of louter deze identificatie mogelijk moet kunnen maken;

2° de methodes voor identificatie bepalen die de operatoren kunnen gebruiken, inclusief een door een operator voorgestelde identificatiemethode onderwerpen aan een voorafgaande machtiging van de minister en van de minister van Justitie;

3° de door de operator te verzamelen en bewaren identificatiegegevens en -documenten bepalen;

4° verplichtingen opleggen aan de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken en de eindgebruikers, met het oog op de identificatie van deze laatsten.

Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

§ 4. Indien een operator niet voldoet aan de hem door dit artikel of door de Koning opgelegde maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.

De operatoren sluiten de abonnees die niet voldoen aan de hen door dit artikel of door de Koning opgelegde maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die abonnees worden op geen enkele wijze vergoed voor de afsluiting."

Art. 10. In dezelfde wet, wordt een artikel 127/1 ingevoegd, luidende:

"Art. 127/1. § 1. Enkel de volgende autoriteiten mogen, via de in artikel 127/3 bedoelde Coördinatiecel, van de operatoren gegevens ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127 om de doeleinden hieronder en volgens de vastgelegde voorwaarden die hen daartoe machtigen:

1° de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronische-communicatienetwerk, zoals de inbreuken die online worden gepleegd;

2° de inlichtingen- en veiligheidsdiensten teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;

3° de autoriteiten belast met het verlenen van hulp aan personen, inclusief de Ombudsdienst voor telecommunicatie

télécommunications pour ce qui concerne l'utilisation malveillante du réseau, les services d'urgence et la Cellule des personnes disparues de la Police Fédérale;

4° l'Institut dans le cadre de la mise en œuvre et le contrôle de la présente loi;

5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service.

§ 2. L'Institut publie sur son site Internet des informations générales concernant l'accès des autorités visées au paragraphe premier aux données conservées en vertu des articles 122, 123, 126, 126/1 et 127.

Art. 11. Dans la même loi, un article 127/2 est inséré comme suit:

"Art. 127/2, § 1er. Le ministre et le ministre de la Justice font en sorte que des statistiques sur l'accès des autorités aux données conservées en vertu des articles 122, 123, 126, 126/1 et 127 soient transmises annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment:

1° les cas dans lesquels des données ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l'information confidentielle.

Les données qui concernent l'application de l'alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine sur avis de l'Institut, les statistiques que les opérateurs transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 2. Les opérateurs font en sorte que les données qu'ils conservent pour leurs propres besoins et celles qu'ils conservent pour les autorités soient accessibles de manière illimitée à partir de la Belgique.

Ils veillent également à garantir la qualité de ces données et, pour ce qui concerne les données conservées pour les autorités, à ce qu'elles soient de la même qualité que les données sur le réseau.

wat betreft het kwaadwillig gebruik van het netwerk, de hulpdiensten en de Cel Vermiste Personen van de federale politie;

4° het Instituut in het kader van de uitvoering en de controle van deze wet;

5° de autoriteiten bevoegd voor het onderzoek van een veiligheidsprobleem op het netwerk of van de dienst.

§ 2. Het Instituut publiceert op zijn website algemene informatie betreffende de toegang tot gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127 voor de in de eerste paragraaf bedoelde autoriteiten.

Art. 11. In dezelfde wet, wordt een artikel 127/2 ingevoegd, luidende:

"Art. 127/2 § 1. De minister en de minister van Justitie zorgen ervoor dat jaarlijks statistieken met betrekking tot de toegang van de autoriteiten tot de gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127 worden bezorgd aan de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name:

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken om gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens of vertrouwelijke informatie omvatten.

De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens gevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt op advies van het Instituut, de statistieken die de operatoren jaarlijks bezorgen aan het Instituut en deze die het Instituut bezorgt aan de minister en aan de minister van Justitie.

§ 2. De operatoren zorgen ervoor dat de gegevens die ze bewaren voor hun eigen behoeften en deze die ze bewaren voor de autoriteiten onbeperkt toegankelijk zijn vanuit België.

Ze garanderen eveneens de kwaliteit van deze gegevens en, in het geval van de gegevens bewaard voor de autoriteiten, zorgen ervoor dat ze dezelfde kwaliteit hebben als de gegevens in het netwerk.

Les opérateurs sont en mesure d'établir des liens entre les données conservées pour les autorités.

§ 3. Pour ce qui concerne les données conservées pour les autorités, les opérateurs:

1° garantissent que les données conservées sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

2° conservent les données sur le territoire de l'Union européenne;

3° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

4° ne peuvent utiliser les données conservées pour d'autres finalités que la fourniture de ces données aux autorités, sauf lorsqu'ils obtiennent le consentement des abonnés concernés conformément à l'article 4 du RGDP et sans préjudice d'autres dispositions légales.

Pour ce qui concerne les données conservées pour leurs propres besoins ou pour les autorités, les opérateurs:

1° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données ou rendent ces données anonymes;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, conformément à l'article 105/1;

3° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 127/3, § 1er, de manière manuelle ou de manière automatisée;

4° assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité.

La traçabilité visée à l'alinéa 1er, 4°, s'effectue à l'aide d'un journal.

L'opérateur prend les mesures nécessaires pour que chaque accès aux données qu'il conserve pour les autorités et chaque accès d'un membre de la Cellule de coordination visée à l'article 127/3 à d'autres données génère de manière automatisée un enregistrement dans le journal.

Ce journal comprend également les informations et documents suivants:

De operatoren zijn in staat verbanden te leggen tussen de gegevens bewaard voor de autoriteiten.

§ 3. Wat betreft de gegevens bewaard voor de autoriteiten, dienen de operatoren:

1° te garanderen dat de bewaarde gegevens onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;

2° de gegevens op het grondgebied van de Europese Unie te bewaren;

3° te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

4° mogen de bewaarde gegevens niet gebruiken voor andere doeleinden dan de verstrekking van deze gegevens aan de autoriteiten, tenzij wanneer ze de toestemming krijgen van de betrokken abonnees, conform artikel 4 van de AVG en onverminderd andere wettelijke bepalingen.

Wat betreft de gegevens bewaard voor hun eigen behoeften of voor de autoriteiten, dienen de operatoren:

1° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt van elke drager worden verwijderd of dat deze gegevens worden geanonimiseerd;

2° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, conform artikel 105/1;

3° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 127/3, § 1, op manuele of op automatische wijze;

4° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit.

De in het eerste lid, 4°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek.

De operator neemt de nodige maatregelen opdat elke toegang tot de gegevens die hij bewaart voor de autoriteiten en elke toegang van een lid van de Coördinatiecel bedoeld in artikel 127/3 tot andere gegevens, automatisch wordt geregistreerd in het logboek.

Dit logboek bevat eveneens de volgende informatie en documenten:

1° l'identité de la personne ayant accédé aux données;

2° l'identité de l'autorité demanderesse, l'objet, la date et l'heure de la demande et la demande;

3° pour ce qui concerne la réponse de l'opérateur à la demande de l'autorité: l'identité de son destinataire, la date et l'heure de son envoi ainsi que le moyen de communication utilisé pour l'envoyer.

Le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte.

Les données de ce journal sont conservées pendant une période de dix ans. A l'échéance de la période de conservation, les données du journal sont détruites.

L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal et, en particulier, pour empêcher toute manipulation non autorisée de ce dernier.

Le Roi peut préciser, après avis des Autorités de protection des données compétentes et de l'Institut, les exigences à respecter par les opérateurs concernant le journal.

Dans le cadre du contrôle de l'opérateur, l'Institut et les autorités de protection des données compétentes peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.

§ 4. Si l'Institut dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2 ou 3, il peut l'obliger à se soumettre à un contrôle de sécurité effectué par un organisme qualifié indépendant, proposé par l'opérateur à l'Institut pour accord.

Cet organisme ne prend pas connaissance des demandes des autorités envers les opérateurs, en compris le journal visé au paragraphe 3, alinéa 3.

Le rapport et les résultats de ce contrôle de sécurité sont communiqués à l'Institut. Le coût du contrôle est à la charge de l'opérateur.".

Art. 12. Dans la même loi, un article 127/3 est inséré comme suit:

"Art. 127/3. § 1er. Auprès de chaque opérateur est constituée une Cellule de coordination, chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques.

Ces autorités adressent leurs demandes à cette cellule.

Le cas échéant, plusieurs opérateurs peuvent créer une Cellule de coordination commune. En pareil cas, cette Cellule

1° de identiteit van de persoon die toegang heeft gehad tot de gegevens;

2° de identiteit van de vragende autoriteit, het voorwerp, de datum en het tijdstip van het verzoek en het verzoek;

3° wat betreft het antwoord van de operator op het verzoek van de autoriteit: de identiteit van zijn geadresseerde, de datum en het tijdstip van de verzending ervan alsook het communicatiemiddel dat werd gebruikt voor de verzending.

Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan.

De gegevens van dit logboek worden bewaard gedurende een periode van tien jaar. Nadat deze bewaringstermijn is verstreken, worden de logboekgegevens vernietigd.

De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen en, in het bijzonder, om elke niet-toegestane handeling in verband met dat logboek te voorkomen.

De Koning kan, na advies van de Gegevensbeschermingsautoriteite en van het Instituut, de eisen bepalen die de operatoren in acht moeten nemen wat betreft het logboek.

In het kader van de controle van de operator mogen het Instituut en de bevoegde gegevensbeschermingsautoriteiten mogen dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.

§ 4. Indien het Instituut over aanwijzingen beschikt die zouden kunnen duiden op een inbreuk van een operator op paragraaf 2 of 3, dan kan het de operator verplichten om zich te onderwerpen aan een veiligheidscontrole door een gekwalificeerde onafhankelijke instantie die de operator ter goedkeuring voorlegt aan het Instituut.

Die instantie neemt geen kennis van de verzoeken van de autoriteiten jegens de operatoren, inclusief het logboek bedoeld in paragraaf 3, derde lid.

Het rapport en de resultaten van deze veiligheidscontrole worden bezorgd aan het Instituut. De kosten van de controle worden door de operator gedragen.".

Art. 12. In dezelfde wet, wordt een artikel 127/3 ingevoegd, luidende:

"Art. 127/3. § 1. Bij elke operator wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.

Deze autoriteiten richten hun verzoeken tot deze cel.

In voorkomend geval kunnen verscheidene operatoren een gemeenschappelijke Coördinatiecel oprichten. In dergelijk

de coordination doit prévoir le même service pour chaque opérateur.

Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l'alinéa 1er. Ils peuvent cependant, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur.

Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.

Chaque opérateur veille à la confidentialité des données traitées par la Cellule de coordination.

§ 2. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs. Il met à la disposition de l'Institut, sur demande, des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Chaque opérateur est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur base des articles 122, 123, 126, 126/1 et 127.

§ 3. Le Roi peut déterminer, après avis des autorités de protection des données compétentes et de l'Institut:

1° les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité;

2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en ce compris lui imposer, le cas échéant, de faire l'objet d'un avis de sécurité positif;

3° si un avis de sécurité positif est imposé, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un officier de sécurité comme prévu à l'article 22*quinquies*, § 6, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ainsi que les règles qui s'appliquent en l'absence d'un tel officier;

4° les règles permettant que les autorités belges qui ont besoin de connaître les coordonnées de la Cellule de coordination et de ses membres en soient informés;

5° les autres règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles, y compris, le cas échéant et par autorité concernée:

a) le mode de transfert, la forme et le contenu des demandes et des réponses;

geval moet deze Coördinatiecel voorzien in dezelfde dienst voor elke operator.

Enkel de leden van de Coördinatiecel mogen antwoorden op de verzoeken van de autoriteiten met betrekking tot de gegevens bedoeld in het eerste lid. Ze mogen echter, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator.

De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.

Elke operator waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel.

§ 2. Elke operator stelt een interne procedure op om te antwoorden op de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens betreffende de eindgebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en zijn antwoord.

Elke operator wordt beschouwd als verantwoordelijk voor de verwerking in de zin van de AVG, voor de gegevens behandeld op basis van de artikelen 122, 123, 126, 126/1 en 127.

§ 3. De Koning kan na advies van de bevoegde gegevensbeschermingsautoriteiten, en van het Instituut het volgende bepalen:

1° de vereisten waaraan de Coördinatiecel moeten beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid;

2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inclusief hem in voorkomend geval verplichten om het voorwerp uit te maken van een positief veiligheidsadvies;

3° indien een positief veiligheidsadvies wordt opgelegd, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een veiligheidsofficier aan te stellen zoals bepaald in artikel 22*quinquies*, § 6, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

4° de regels die het mogelijk maken dat de Belgische autoriteiten die de contactgegevens van de Coördinatiecel en van de leden ervan moeten kennen, daarvan op de hoogte worden gebracht;

5° de overige regels die de samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen regelen, met inbegrip van, in voorkomend geval en per betrokken overheid:

a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;

b) le degré d'urgence de traitement des demandes;

c) le délai de réponse;

d) la disponibilité requise du service;

e) les modalités de test de la collaboration;

f) les tarifs de rétribution de cette collaboration.

Si nécessaire, le Roi peut prévoir des règles différentes selon différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et le lieu où ils opèrent leurs activités.".

Art. 13. Dans la même loi, l'article 127/4 est inséré comme suit:

"Art. 127/4 Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les conditions dans lesquelles les fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public enregistrent et conservent les données permettant l'identification des personnes concernées de l'équipement terminal ou du service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, en vue de la poursuite et la répression d'infractions pénales, et en vue de la répression d'appels malveillants vers les services d'urgence, en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les mesures techniques et administratives imposées aux fournisseurs visées à l'alinéa 1er, en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par les articles 46*bis*, 88*bis*, 90*ter* à 90*decies*, 464/13, 464/25 et 464/26 du Code d'instruction criminelle, ainsi qu'aux conditions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs visés à l'alinéa 1er font en sorte que les données mentionnées à l'alinéa 1er soient accessibles de manière illimitée depuis la Belgique."

b) het dringendheidsniveau voor de behandeling van de verzoeken;

c) de reactietermijn voor de antwoorden;

d) de vereiste beschikbaarheid van de dienst;

e) de modaliteiten voor het testen van de samenwerking;

f) de tarieven van de vergoeding van die samenwerking.

Indien nodig kan de Koning verschillende regels bepalen volgens verschillende categorieën van operatoren, met name volgens het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en de plaats waar zij hun activiteiten uitvoeren.".

Art. 13. In dezelfde wet, wordt het artikel 127/4 ingevoegd, luidende:

"Art. 127/4. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de voorwaarden vast waaronder de aanbieders van private elektronische-communicatienetwerken en elektronische-communicatiediensten die niet openbaar beschikbaar zijn de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische-communicatiedienst, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten en met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, voor het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de technische en administratieve maatregelen vast die aan de aanbieders beoogd in het eerste lid worden opgelegd om de betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke mogelijk te maken onder de voorwaarden bepaald door de artikelen 46*bis*, 88*bis*, 90*ter* tot 90*decies*, 464/13, 464/25 en 464/26 van het Wetboek van strafvordering, evenals de voorwaarden bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De aanbieders beoogd in het eerste lid zorgen ervoor dat de in het eerste lid van deze paragraaf vermelde gegevens onbeperkt toegankelijk zijn vanuit België."

Art. 14. Dans la même loi, un article 127/5 est inséré comme suit:

"Art. 127/5. § 1er. Sauf pour les systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements, qui font l'objet de règles particulières au paragraphe 2, il est interdit de fournir ou d'utiliser un service ou un équipement qui empêche la réalisation des opérations suivantes:

1° les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant;

2° l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

3° les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les dispositions du présent paragraphe dérogent à l'article 105/4.

Le paragraphe 1er, alinéa 1er, 1°, est applicable aux systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

Les systèmes d'encryptage visés à l'alinéa 1er, ne peuvent pas empêcher la conservation par l'opérateur des données d'identification, de trafic ou de localisation pour les autorités, comme prévu dans la présente loi, le Code d'instruction criminelle ou la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Lorsqu'un opérateur a mis en place un système d'encryptage visé à l'alinéa 1er, il rend possible les opérations visées au paragraphe 1er, alinéa 1er, 2° et 3°, dans les [24 heures] à partir de la transmission d'une requête.

Il rend possible la réalisation de ces opérations uniquement pour les communications visées dans la requête et qui sont postérieures à celle-ci.

Toute clause contractuelle faisant obstacle au respect des obligations visées dans le présent paragraphe est interdite et nulle.

Art. 15. À l'article 145 de la même loi, les modifications suivantes sont apportées:

1° dans le paragraphe 1er, les mots "127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, et 127" sont remplacés

Art. 14. In dezelfde wet, wordt een artikel 127/5 ingevoegd, luidende:

"Art. 127/5. § 1. Behalve voor de versleutelingssystemen die gebruikt kunnen worden om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te waarborgen, welke onder specifieke regels vallen in paragraaf 2, is het verboden om een dienst of een toestel aan te bieden of te gebruiken waardoor de uitvoering van de volgende handelingen wordt verhinderd:

1° noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of de verstrekking van de identificatiegegevens van de oproeper;

2° de identificatie van de eindgebruiker, het opsporen en lokaliseren van niet voor het publiek toegankelijke communicatie onder de voorwaarden bepaald door het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

3° het afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie onder de voorwaarden bepaald door het Wetboek van strafvordering en door de wet van 30 november 1998. houdende regeling van de inlichtingen- en veiligheidsdiensten.

§ 2. De bepalingen van deze paragraaf wijken af van artikel 105/4.

Paragraaf 1, eerste lid, 1°, is van toepassing op de versleutelingssystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te waarborgen.

De in het eerste lid bedoelde versleutelingssystemen mogen niet verhinderen dat de operator voor de autoriteiten identificatie-, verkeers- of locatiegegevens bewaart, zoals bepaald in deze wet, het Wetboek van strafvordering of de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Wanneer een operator een versleutelingssysteem als bedoeld in het eerste lid heeft ingesteld, maakt hij de in paragraaf 1, eerste lid, 2° en 3° bedoelde handelingen mogelijk binnen [24 uur] na de verzending van het verzoekschrift.

Hij maakt de uitvoering van deze handelingen enkel mogelijk voor de communicatie waarop het verzoekschrift slaat alsook voor de communicatie die daarna volgt.

Elke contractuele clausule die de inachtneming van de in deze paragraaf beoogde verplichtingen belemmert, is verboden en nietig.

Art. 15. In artikel 145 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, worden de woorden "127 en de ter uitvoering van de artikelen 32, 39, § 3, 47, en 127 genomen

par les mots “126 à 127/5 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, 126, 126/1, 127 et 127/2 à 127/4.”

2° au lieu du paragraphe 3*ter*, annulé par l’arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un paragraphe 3*ter* rédigé comme suit:

“§ 3*ter*. Est puni d’une amende de 50 euros à 50 000 euros et d’une peine d’emprisonnement de six mois à trois ans ou d’une de ces peines seulement:

1° toute personne qui, à l’occasion de l’exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu’elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données conservées par l’opérateur pour les autorités;

2° celui qui, sachant que les données ont été obtenues par la commission de l’infraction visée au 1°, les détient, les révèle à une autre personne, les divulgue ou en fait un usage quelconque.”.

Chapitre 3 - Modifications à la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

Art. 16. À l’article 14, § 2, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, un 2°/1 est introduit entre le 2° et le 3°, rédigé comme suit:

“2°/1 peut demander aux opérateurs les données d’identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l’accomplissement de l’une de ses missions;”.

Chapitre 4 - Modifications du Code d’instruction criminelle

Art. 17. Dans le Code d’instruction criminelle, un article 39*quinquies* est inséré comme suit:

“Art. 39*quinquies*. § 1. Lors de la recherche de crimes et délits, le procureur du Roi peut, s’il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d’un an ou à une peine plus lourde, ordonner, par une décision écrite et motivée, à un ou plusieurs acteurs visés à l’alinéa 2, de conserver les données visées à l’article 88*bis*, § 1, alinéa 1er, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu’il juge nécessaires.

L’ordre visé à l’alinéa 1er peut être donné, directement ou par l’intermédiaire du service de police désigné par le Roi, à:

l’opérateur d’un réseau de communications électroniques; et

besluiten overtreedt.” vervangen door de woorden “126 tot en met 127/5 en de ter uitvoering van de artikelen 32, 39, § 3, 47, 126, 126/1, 127 en 127/2 tot en met 127/4 genomen besluiten overtreedt.”

2° in de plaats van paragraaf 3*ter*, vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een als volgt luidende paragraaf 3*ter* ingevoegd:

“§ 3*ter*. Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de door de operator voor de autoriteiten bewaarde gegevens op enige manier overneemt, bij zich houdt of er enig gebruik van maakt;;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.”.

Hoofdstuk 3 - Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 16. In artikel 14, § 2, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector wordt een 2°/1 ingevoegd tussen de 2° en de 3°, luidend als volgt:

“2°/1 kan het Instituut van de operatoren de identificatie-, verkeers- of locatiegegevens vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten;”.

Hoofdstuk 4 - Wijzigingen aan het Wetboek van strafvordering

Art. 17. In het Wetboek van strafvordering wordt een artikel 39*quinquies* ingevoerd, luidende:

“Art. 39*quinquies*. § 1. Bij het opsporen van de misdaden en de wanbedrijven kan de procureur des Konings, wanneer er ernstige aanwijzingen zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, bij een met redenen omklede en schriftelijke beslissing aan een of meerdere van de actoren bedoeld in het tweede lid bevelen de noodzakelijke gegevens bedoeld in artikel 88*bis*, § 1, eerste lid, die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Het bevel bedoeld in het eerste lid kan, rechtstreeks of via de door de Koning aangewezen politiedienst, gegeven worden aan:

de operator van een elektronisch communicatienetwerk; en

toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La décision écrite et motivée mentionne:

le nom du procureur du Roi qui ordonne la conservation;

l'infraction qui fait l'objet de l'ordre;

les circonstances de fait de la cause qui justifient la conservation;

l'indication précise d'un ou de plusieurs des éléments suivants: la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;

le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;

la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;

la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. L'ordre doit être confirmé dans les plus brefs délais dans la forme prévue à l'alinéa 3.

§ 2. Les acteurs visés au § 1er, alinéa 2 veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, est punie d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

§ 4. L'accès aux données conservées conformément à cet article n'est possible qu'en application de l'article 88*bis*.

Art. 18. Dans l'article 88*bis* du même Code, inséré par la loi du 11 février 1991 et modifié en dernier lieu par la loi du 5 mai 2019, les modifications suivantes sont apportées:

iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

De met redenen omklede en schriftelijke beslissing vermeldt:

de naam van de procureur des Konings die de bewaring beveelt;

het strafbare feit waarop het bevel betrekking heeft;

de feitelijke omstandigheden van de zaak die de bewaring van de gegevens rechtvaardigen;

de precieze aanduiding van één of meerdere van de volgende elementen: de persoon of de personen, de communicatiemiddelen of de plaatsen waarop de bewaring betrekking heeft;

in voorkomend geval, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden;

de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevel, onverminderd een hernieuwing;

de duur van bewaring van deze gegevens, die niet langer mag zijn dan zes maanden. Deze termijn kan schriftelijk worden verlengd.

In spoedeisende gevallen kan het bevel tot bewaring mondeling worden gegeven. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde lid.

§ 2. De actoren bedoeld in § 1, tweede lid zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van zesentwintig tot twintigduizend euro of met één van die straffen alleen.

§ 4. De toegang tot de overeenkomstig dit artikel bewaarde gegevens kan slechts met toepassing van artikel 88*bis*.

Art. 18. In artikel 88*bis*, ingevoegd bij de wet van 11 februari 1991 en laatstelijk gewijzigd bij de wet van 5 mei 2019, worden de volgende wijzigingen aangebracht:

1° dans le paragraphe 1er, alinéa 5, les mots “conformément au paragraphe 2” sont supprimés;

2° paragraphe 3, inséré par la loi du 29 mai 2016, modifié par la loi du 5 mai 2019 et annulé par l’arrêt n° 57/2021 du 22 avril 2021 de la Cour Constitutionnelle, est rétabli dans la rédaction suivante:

“La mesure ne peut porter sur les moyens de communication électronique d’un avocat ou d’un médecin que si celui-ci est lui-même soupçonné d’avoir commis une infraction visée au paragraphe 1er ou d’y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d’avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l’ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d’instruction des éléments qu’il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l’article 458 du Code pénal.”

Chapitre 5 - Modifications de la loi du 5 août 1992 sur la fonction de police

Art. 19. À l’article 42 de la loi du 5 août 1992 sur la fonction de police, modifié par la loi du 12 novembre 2017, les modifications suivantes sont apportées:

1° Le mot “§ 1er” est inséré au début de l’article;

2° L’article est complété par un paragraphe 2 rédigé comme suit:

“§ 2. Un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale peut, dans le cadre de sa mission d’assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu’il existe des présomptions ou indices sérieux que l’intégrité physique de la personne disparue se trouve en danger imminent, requérir d’obtenir les données relatives aux communications électroniques concernant la personne disparue.

Seules les données visant à identifier l’utilisateur ou l’abonné et les moyens de communication et relatives à l’accès et la connexion de l’équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, concernant la personne disparue et conservées au cours des 48 heures précédant la demande d’obtention des données, sont communiquées.

La réquisition est adressée par l’officier de police judiciaire visé à paragraphe 2, alinéa 1, à:

1° In paragraaf 1, vijfde lid, worden de woorden “overeenkomstig paragraaf 2” geschrapt;

2° paragraaf 3, ingevoegd bij de wet van 29 mei 2016, gewijzigd bij de wet van 5 mei 2019 en vernietigd door arrest nr. 57/2021 van 22 april 2021 van het Grondwettelijk Hof, wordt hersteld als volgt:

“De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Dezelfde personen zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.”

Hoofdstuk 5 - Wijzigingen van de wet van 5 augustus 1992 op het politieambt

Art. 19. In artikel 42 van wet van 5 augustus 1992 op het politieambt, gewijzigd bij de wet van 12 november 2017, worden de volgende wijzigingen aangebracht:

1° Het woord “§ 1” wordt ingevoegd aan het begin van het artikel;

2° Het artikel wordt aangevuld met een paragraaf 2 ingevoegd, luidende:

“§ 2. Een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kan, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood en de opsporing van personen van wie de verdwijning onrustwekkend is, en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon opvorderen.

Enkel de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen en met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, betreffende de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan de opvordering, worden meegedeeld.

De vordering wordt via de officier van gerechtelijke politie bedoeld in paragraaf 2, eerste lid 1, gericht aan:

l'opérateur d'un réseau de communications électroniques; ou

toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques."

Chapitre 6 - Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 20. À l'article 3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les modifications suivantes sont apportées:

1° le 10° est complété par les mots ", quelle que soit la nature du destinataire ou du récepteur;";

2° il est inséré un 10/1 , rédigé comme suit:

"10/1° "opérateur": personne ou entreprise qui, sur le territoire belge, fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public".

Art. 21. À l'article 7 de la même loi, les mots ", chargée de la sécurité nationale," sont insérés entre les mots "La Sûreté de l'État" et "a pour mission".

Art. 22. Dans l'article 11 de la même loi, les mots ", chargé de la sécurité nationale," sont insérés entre les mots "Renseignement et de la Sécurité" et "a pour mission".

Art. 23. À l'article 16/2, § 1, les modifications suivantes sont apportées:

1° À l'alinéa 1er, les mots "de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques" sont abrogés;

2° À l'alinéa 3, les mots "de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques" sont abrogés;

3° À l'alinéa 4, les mots "ou du fournisseur du service" sont abrogés.

Art. 24. Dans la même loi, un article 16/2/1 est inséré, rédigé comme suit:

"Art. 16/2/1. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur pour procéder à la conservation des:

1° données de trafic et de localisation de moyens de communications électroniques conservées au moment de la réquisition et qui font l'objet de celle-ci;

de operator van een elektronisch communicatienetwerk; of

iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen."

Hoofdstuk 6 - Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Art. 20. In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, worden de volgende wijzigingen aangebracht:

1° de bepaling onder 10° wordt aangevuld met de woorden ", ongeacht de aard van de bestemmeling of de ontvanger;";

2° onder 10°/1° wordt een bepaling ingevoegd, luidende:

"10/1° "operator": persoon of onderneming die op het Belgische grondgebied een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische communicatiedienst aanbiedt".

Art. 21. In artikel 7 van dezelfde wet, worden de woorden ", belast met de nationale veiligheid," ingevoegd tussen de woorden "Veiligheid van de Staat" en "heeft als opdracht".

Art. 22. In artikel 11 van dezelfde wet, worden de woorden ", belast met de nationale veiligheid," ingevoegd tussen de woorden "Inlichting en Veiligheid" en "heeft als opdracht".

Art. 23. In artikel 16/2, § 1, worden de volgende wijzigingen aangebracht:

1° In het eerste lid worden de woorden "van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst" opgeheven;

2° In het derde lid worden de woorden "van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst" opgeheven;

3° In het vierde lid worden de woorden "of van de dienstenverstrekker" opgeheven.

Art. 24. In dezelfde wet wordt een artikel 16/2/1 ingevoerd, luidende:

"Art. 16/2/1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator voor het bewaren van:

1° de verkeers- en lokalisatiegegevens van de elektronische communicatiemiddelen die op het ogenblik van de vordering worden bewaard en die het voorwerp uitmaken van de vordering;

2° données de trafic et de localisation qu'il génère et traite et qui font l'objet de la réquisition.

La décision est effectuée par écrit par le dirigeant de service ou son délégué et est motivée.

En cas d'urgence, le dirigeant du service ou son délégué peut requérir cette conservation verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite.

La réquisition écrite mentionne:

1° les personnes, les groupes de personnes, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation font l'objet de la conservation;

2° la durée de conservation des données qui ne peut excéder six mois sans préjudice de la possibilité de prolongation en suivant la même procédure.

Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.

Le Comité permanent R reçoit chaque mois du service de renseignement et de sécurité concerné une liste des réquisitions de conservation. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la méthode.

Toute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à vingt mille euros.

Les données conservées par les opérateurs sur base du présent article sont détruites 12 mois après le début de leur conservation.

Le Roi peut déterminer, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs."

Art. 25. À l'article 18/2, § 2, de la même loi, les mots "à 18/17" sont remplacés par les mots "à 18/17/1".

Art. 26. À l'article 18/3, § 2, de la même loi, le 12° est abrogé.

Art. 27. À l'article 18/7 de la même loi, les modifications suivantes sont apportées:

1° Au paragraphe 1, les mots "Dans l'intérêt de l'exercice des missions, le dirigeant du service peut, par une décision écrite" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions";

2° de verkeers- en lokalisatiegegevens die hij genereert en verwerkt en die het voorwerp uitmaken van de vordering.

De beslissing gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde en wordt met redenen omkleed.

In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze bewaring mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.

De schriftelijke vordering vermeldt:

1° de personen, groepen personen, geografische gebieden, communicatiemiddelen en/of gebruikswijzen waarvoor de verkeers- en lokalisatiegegevens moeten worden bewaard;

2° de periode gedurende welke de gegevens worden bewaard, die niet langer mag zijn dan zes maanden, onverminderd de mogelijkheid van verlenging volgens dezelfde procedure.

De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring.

Het Vast Comité I ontvangt elke maand van de betrokken inlichtingen- en veiligheidsdienst een lijst van vorderingen tot bewaring. Indien er een onwettigheid vastgesteld wordt, beëindigt het Vast Comité I de methode.

Eenieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.

Gegevens die door operatoren op grond van dit artikel worden bewaard, worden 12 maanden na het begin van hun bewaring vernietigd.

De Koning kan, op voorstel van de minister van Justitie, de minister van Defensie en de minister bevoegd voor de elektronische communicatie, nadere regels voor de samenwerking met de operatoren bepalen."

Art. 25. In artikel 18/2, § 2, van dezelfde wet worden de woorden "tot 18/17" vervangen door de woorden "tot 18/17/1".

Art. 26. In artikel 18/3, § 2, van dezelfde wet wordt de bepaling onder 12° opgeheven.

Art. 27. In artikel 18/7 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° In paragraaf 1 worden de woorden "In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing,"vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,";

2° Au paragraphe 1, 2°, les mots “d’un réseau de communications électroniques ou d’un fournisseur d’un service de communications électroniques” sont abrogés;

3° Au paragraphe 1, 2°, les mots “la communication des factures afférentes aux abonnements identifiés,” sont insérés entre les mots “afin de l’obtenir” et les mots “les données relatives à la méthode de paiement”;

4° Au paragraphe 3, alinéa 1, les mots “d’un réseau de communications électroniques ou d’un fournisseur d’un service de communications électroniques” sont abrogés;

5° Au paragraphe 3, alinéa 2, les mots “le dirigeant du service” sont remplacés par les mots “le service concerné”.

Art. 28. L’article 18/8 de la même loi est remplacé comme suit:

“Art. 18/8. § 1er. Les services de renseignement et de sécurité peuvent, dans l’intérêt de l’exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l’opérateur, procéder ou faire procéder:

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l’origine ou de la destination de communications électroniques.

Dans les cas visés à l’alinéa 1er et pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l’origine ou la destination de la communication électronique est localisée, le jour, l’heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.

La nature de la décision est communiquée à l’opérateur.

§ 2. Tout opérateur qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions.

Toute personne visée à l’alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d’une amende de vingt-six euros à vingt mille euros. “

Art. 29. À l’article 18/10, § 4, alinéa 4, de la même loi, les mots “et 18/17” sont remplacés par les mots “, 18/17 et 18/17/1”.

2° In paragraaf 1 worden in de bepaling onder 2° de woorden “van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst” opgeheven;

3° In paragraaf 1 worden in de bepaling onder 2° de woorden “de mededeling van de facturen met betrekking tot de geïdentificeerde abonnementen,” ingevoegd tussen de woorden “tot het bekomen van” en de woorden “de gegevens betreffende de betalingswijze”;

4° In paragraaf 3, eerste lid worden de woorden “van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst” opgeheven;

5° In paragraaf 3, tweede lid, worden de woorden “het diensthoofd” vervangen door de woorden “de betrokken dienst”.

Art. 28. Het artikel 18/8 van dezelfde wet wordt vervangen als volgt:

“Art. 18/8. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator te vorderen, overgaan of doen overgaan tot:

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.

In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.

De aard van de beslissing wordt meegedeeld aan de operator.

§ 2. Iedere operator die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie.

Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro. “

Art. 29. In artikel 18/10, § 4, vierde lid, van dezelfde wet worden de woorden “en 18/17” vervangen door de woorden “, 18/17 en 18/17/1”.

Art. 30. À l'article 18/17, § 3, alinéa 1er de la même loi, les mots "du réseau ou le fournisseur d'un service de communications électroniques"sont abrogés.

Art. 31. Dans la même loi, il est inséré un article 18/17/1, rédigé comme suit:

"Art. 18/17/1. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux.

La réquisition est effectuée par écrit par le dirigeant du service et mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné visée à l'article 18/10 § 3, alinéa 3, selon le cas.

L'autorisation du dirigeant du service est transmise au ministre compétent.

Le service de renseignement et de sécurité concerné peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques pour transmettre la réquisition à tous les opérateurs concernés.

Le dirigeant du service peut requérir, par une décision écrite, des personnes dont il présume qu'elles ont une expertise technique utile de prêter leur concours à la mise en œuvre de cette méthode. Cette réquisition mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.

Toute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à vingt mille euros.

La méthode est autorisée pour une durée ne pouvant excéder 6 mois sans préjudice de la procédure visée à l'article 18/10, § 5.

Le service de renseignement et de sécurité concerné fait rapport à la commission tous les deux mois sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

Le Roi peut déterminer, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs.".

Art. 30. In artikel 18/17, § 3, eerste lid, van dezelfde wet, worden de woorden "van het netwerk of de verstrekker van een elektronische communicatiedienst" opgeheven.

Art. 31. In dezelfde wet wordt een artikel 18/17/1 ingevoerd, luidende:

"Art. 18/17/1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid, de medewerking vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt.

De vordering wordt schriftelijk gedaan door het diensthoofd en vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister bedoeld in artikel 18/10, § 3, derde lid.

De machtiging van het diensthoofd wordt overgemaakt aan de bevoegde minister.

De betrokken inlichtingen- en veiligheidsdienst kan de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, om de vordering aan alle betrokken operatoren over te maken.

Het diensthoofd kan bij schriftelijke beslissing vorderen dat personen van wie hij veronderstelt dat zij over de nodige technische deskundigheid beschikken, medewerking verlenen bij de tenuitvoerlegging van deze methode. De vordering vermeldt, naargelang het geval, de aard van de instemming van de commissie, de aard van de instemming van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.

Eenieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

De methode wordt toegestaan voor een periode die niet langer mag zijn dan 6 maanden onverminderd de procedure bedoeld in artikel 18/10, § 5.

De betrokken inlichtingen- en veiligheidsdienst brengt om de twee maanden bij de Commissie verslag uit over de evolutie van de dreiging. In dit verslag worden de elementen belicht die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen.

De Koning kan, op voorstel van de minister van Justitie, de minister van Defensie en de minister bevoegd voor de elektronische communicatie, nadere regels voor de samenwerking met de operatoren bepalen.".

Chapitre 7 - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 32. À l'article 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, rétabli par la loi du 2 mai 2007 et modifié par les lois des 25 avril 2014 et 31 juillet 2017, il est inséré un paragraphe 1er*bis*/1 rédigé comme suit:

"§ 1er*bis*/1. Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1er, alinéa 2, de conserver les données visées au paragraphe 1er, alinéa 1er, qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.

Les paragraphes 1er, alinéas 4 et 5, et 3 s'appliquent par analogie à l'ordre visé à l'alinéa 1er.

Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

L'auditeur ou, en son absence, l'auditeur adjoint fait part au juge d'instruction de l'ordre visé à l'alinéa 1er au moment où il lui adresse sa demande d'autorisation préalable pour requérir la communication des données visées au paragraphe 1er, alinéa 1er. Si le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre ou s'il estime que l'ordre n'était pas légitime ou pas justifié, cet ordre s'éteint.".

Chapitre 8 - Modification de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits

Art. 33. L'article 11, § 1er, de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits, remplacé par la loi du 10 avril 2014, est complété par un alinéa rédigé comme suit:

"Ils peuvent identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique.

À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification à:

1° l'opérateur d'un réseau de communications électroniques; et

2° toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui

Hoofdstuk 7 - Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 32. In artikel 84 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, hersteld bij de wet van 2 mei 2007 en gewijzigd bij de wetten van 25 april 2014 en 31 juli 2017, wordt een paragraaf 1*bis*/1 ingevoegd, luidende:

"§ 1*bis*/1. Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de in paragraaf 1, tweede lid, bedoelde actoren bevelen om de gegevens bedoeld in paragraaf 1, eerste lid, die riskeren te worden verwijderd of anoniem gemaakt, te bewaren totdat hij de toestemming van een onderzoeksrechter heeft bekomen om de mededeling van deze gegevens te vorderen.

Paragrafen 1, vierde en vijfde lid, en 3 zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.

De in paragraaf 1, tweede lid, bedoelde actoren zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, bezorgt het in het eerste lid bedoelde bevel aan de onderzoeksrechter gelijktijdig met zijn verzoek tot voorafgaande toestemming om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel betrekking heeft of oordeelt dat het bevel niet wettig of niet gerechtvaardigd was, vervalt het bevel.".

Hoofdstuk 8 - Wijziging van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten

Art. 33. Artikel 11, § 1, van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedings-middelen en andere producten, vervangen bij de wet van 10 april 2014, wordt aangevuld met een lid, luidende:

"Zij mogen natuurlijke en rechtspersonen identificeren aan de hand van het telefoonnummer van de betrokkene of het IP-adres dat aan de bron van de elektronische communicatie ligt.

Hiertoe mogen zij met gemotiveerd verzoek de verstrekking van de identificatiedocumenten en gegevens vorderen van:

1° de operator van een elektronisch communicatienetwerk; en

2° iedereen die binnen het Belgisch grondgebied, op welke wijze ook een dienst beschikbaar stelt of aanbiedt, die

consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Sans préjudice d'une éventuelle délégation, chaque demande d'identification doit être approuvée au préalable, par écrit, par le chef du service Inspection produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement."

Chapitre 9 - Modification de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS")

Art. 34. L'article 62 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est remplacé comme suit:

"Art. 62. § 1. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 60 et 61. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.

§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, le CSIRT national peut obtenir des opérateurs, au sens de l'article 2, 11° de la loi du 13 juin 2005 relative aux communications électroniques, des données d'identification, de trafic et de localisation conservées par ceux-ci.

Pour ce faire, le CSIRT national respecte les règles et les procédures prévues par la loi du 13 juin 2005 relative aux communications électroniques.

Les fonctionnaires dirigeants du CSIRT national désignent expressément les personnes habilitées à solliciter ces informations auprès des opérateurs visés à l'alinéa 1er et à les traiter.

§ 3. Pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

§ 4. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

Onverminderd een eventuele delegatie, dient elk identificatieverzoek voorafgaand, door het diensthoofd van de Inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden."

Hoofdstuk 9 - Wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk-en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet")

Art. 34. Artikel 62 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt vervangen als volgt:

"Art. 62. § 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, a) tot e) van deze wet, kan het nationale CSIRT van de operatoren, als bedoeld in artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, identificatie- en verkeers- en locatiegegevens die door hen worden bewaard, verkrijgen.

Daartoe houdt het nationale CSIRT zich aan de regels en procedures bedoeld in de wet van 13 juni 2005 betreffende de elektronische communicatie.

De leidende ambtenaren van het nationale CSIRT wijzen uitdrukkelijk de personen aan die gemachtigd zijn om deze informatie op te vragen bij de operatoren bedoeld in het eerste lid en om ze te verwerken.

§ 3. Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

§ 4. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.".

Art. 35. Dans l'article 65, § 2, de la même loi, les mots "des données de communications électroniques," sont insérés entre les mots "des données ou des identifiants de connexion," et "des données de géolocalisation".

Chapitre 10 - Entrée en vigueur

[Art. 36. La loi entre en vigueur le jour où l'annulation de la loi du 29 mai 2016 par l'arrêt n° 57/2021 de la Cour constitutionnelle prend effet.]

De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit."

Art. 35. In artikel 65, § 2, van dezelfde wet worden de woorden "elektronische communicatiegegevens," ingevoegd tussen de woorden "verbindingsgegevens of -identificatoren," en de woorden "locatie-gegevens".

Hoofdstuk 10 - Inwerkingtreding

[Art. 36. De wet treedt in werking op de dag waarop de vernietiging van de wet van 29 mei 2016 door het arrest nr. 57/2021 van het Grondwettelijk Hof gevolgen ressorteert.]

Formulaire AIR - v2 – oct. 2014

Analyse d'impact de la réglementation

RiA-AiR

:: Remplissez de préférence le formulaire en ligne ria-air.fed.be
:: Contactez le Helpdesk si nécessaire ria-air@premier.fed.be
:: Consultez le manuel, les FAQ, etc. www.simplification.be

Fiche signalétique

Auteur .a.

Membre du Gouvernement compétent	Ministre de la Justice
Contact cellule stratégique (nom, email, tél.)	Samuelle Godin - Samuelle@teamjustitie.be
Administration compétente	FOD Justitie
Contact administration (nom, email, tél.)	Frederik Decruyenaere – frederik.decruyenaere@just.fgov.be – 02/542 67 87

Projet .b.

Titre du projet de réglementation	Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités	
Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.	Dans l'arrêt n° 57/2001 du 22 avril 2021, la Cour constitutionnelle a annulé les articles 2,b), 3 à 11 et 14 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques », en ce qu'ils reposent sur une obligation de conservation généralisée et indifférenciée des données. Le projet de loi vise essentiellement à réparer la législation applicable en la matière, en tenant compte des objections de la Cour constitutionnelle et de la jurisprudence de la Cour de justice de l'Union européenne, et en particulier de l'arrêt « La Quadrature du Net » (aff. jtes. C-511/18, C-512/18 et C-520/18 du 6 octobre 2020). Ainsi, ce projet de loi a pour leitmotiv la recherche constante du juste équilibre entre le respect de la protection des données à caractère, et plus largement à la vie privée des citoyens, et la sauvegarde de la sécurité nationale et la protection de la sécurité publique.	
Analyses d'impact déjà réalisées	☒ Oui ☐ Non	Si oui, veuillez joindre une copie ou indiquer la référence du document : _ _

Consultations sur le projet de réglementation .c.

Consultations obligatoires, facultatives ou informelles :	Inspection des finances - Ministre du budget - Autorités de protection des données –Consultation publique- Comité de consertation - Comité interministériel des télécommunications, de la radiodiffusion et de la télévision - Conseil d'État.

Sources utilisées pour effectuer l'analyse d'impact .d.

Statistiques, documents de référence, organisations et personnes de référence : _ _

Date de finalisation de l'analyse d'impact .e.

_

Formulaire AIR - v2 – oct. 2014

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

>

Un projet de réglementation aura généralement des impacts sur un nombre limité de thèmes.

Une liste non-exhaustive de mots-clés est présentée pour faciliter l'appréciation de chaque thème.

S'il y a des **impacts positifs et / ou négatifs, expliquez-les** (sur base des mots-clés si nécessaire) et indiquez les mesures prises pour alléger / compenser les éventuels impacts négatifs.

Pour les thèmes 3, 10, 11 et 21, des questions plus approfondies sont posées.

Consultez le manuel ou contactez le helpdesk ria-air@premier.fed.be pour toute question.

Lutte contre la pauvreté .1.

Revenu minimum conforme à la dignité humaine, accès à des services de qualité, surendettement, risque de pauvreté ou d'exclusion sociale (y compris chez les mineurs), illettrisme, fracture numérique.

☐ Impact positif ☐ Impact négatif ↓ Expliquez.

_ _

☒ Pas d'impact

Égalité des chances et cohésion sociale .2.

Non-discrimination, égalité de traitement, accès aux biens et services, accès à l'information, à l'éducation et à la formation, écart de revenu, effectivité des droits civils, politiques et sociaux (en particulier pour les populations fragilisées, les enfants, les personnes âgées, les personnes handicapées et les minorités).

☐ Impact positif ☐ Impact négatif ↓ Expliquez.

_ _

☒ Pas d'impact

Égalité entre les femmes et les hommes .3.

Accès des femmes et des hommes aux ressources : revenus, travail, responsabilités, santé/soins/bien-être, sécurité, éducation/savoir/formation, mobilité, temps, loisirs, etc.

Exercice des droits fondamentaux par les femmes et les hommes : droits civils, sociaux et politiques.

1. Quelles personnes sont directement et indirectement concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

   Si aucune personne n'est concernée, expliquez pourquoi.

   Les chapitres en question ne portent pas et n'ont pas d'impact sur l'égalité entre les femmes et les hommes

↓ Si des personnes sont concernées, répondez à la question 2.

2. Identifiez les éventuelles différences entre la situation respective des femmes et des hommes dans la matière relative au projet de réglementation.

_ _

↓ S'il existe des différences, répondez aux questions 3 et 4.

3. Certaines de ces différences limitent-elles l'accès aux ressources ou l'exercice des droits fondamentaux des femmes ou des hommes (différences problématiques) ? [O/N] > expliquez

_ _

4. Compte tenu des réponses aux questions précédentes, identifiez les impacts positifs et négatifs du projet sur l'égalité des femmes et les hommes ?

_ _

↓ S'il y a des impacts négatifs, répondez à la question 5.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

_ _

Formulaire AIR - v2 – oct. 2014

Santé .4.

Accès aux soins de santé de qualité, efficacité de l'offre de soins, espérance de vie en bonne santé, traitements des maladies chroniques (maladies cardiovasculaires, cancers, diabètes et maladies respiratoires chroniques), déterminants de la santé (niveau socio-économique, alimentation, pollution), qualité de la vie.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Emploi .5.

Accès au marché de l'emploi, emplois de qualité, chômage, travail au noir, conditions de travail et de licenciement, carrière, temps de travail, bien-être au travail, accidents de travail, maladies professionnelles, équilibre vie privée - vie professionnelle, rémunération convenable, possibilités de formation professionnelle, relations collectives de travail.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Modes de consommation et production .6.

Stabilité/prévisibilité des prix, information et protection du consommateur, utilisation efficace des ressources, évaluation et intégration des externalités (environnementales et sociales) tout au long du cycle de vie des produits et services, modes de gestion des organisations.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Développement économique .7.

Création d'entreprises, production de biens et de services, productivité du travail et des ressources/matières premières, facteurs de compétitivité, accès au marché et à la profession, transparence du marché, accès aux marchés publics, relations commerciales et financières internationales, balance des importations/exportations, économie souterraine, sécurité d'approvisionnement des ressources énergétiques, minérales et organiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Investissements .8.

Investissements en capital physique (machines, véhicules, infrastructures), technologique, intellectuel (logiciel, recherche et développement) et humain, niveau d'investissement net en pourcentage du PIB.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Recherche et développement .9.

Opportunités de recherche et développement, innovation par l'introduction et la diffusion de nouveaux modes de production, de nouvelles pratiques d'entreprises ou de nouveaux produits et services, dépenses de recherche et de développement.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

PME .10.

Impact sur le développement des PME.

1. Quelles entreprises sont directement et indirectement concernées par le projet ?
   Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (< 50 travailleurs) dont le % de micro-entreprise (< 10 travailleurs).
   Si aucune entreprise n'est concernée, expliquez pourquoi.

   Les opérateurs fournissant des services de communications électroniques sont concernés.

↓ Si des PME sont concernées, répondez à la question 2.

2. Identifiez les impacts positifs et négatifs du projet sur les PME.
   N.B. les impacts sur les charges administratives doivent être détaillés au thème 11

   Il n'y a pas d'impact spécifique sur les PME.

↓ S'il y a un impact négatif, répondez aux questions 3 à 5.

3. Ces impacts sont-ils proportionnellement plus lourds sur les PME que sur les grandes entreprises ? [O/N] > expliquez

   – –

4. Ces impacts sont-ils proportionnels à l'objectif poursuivi ? [O/N] > expliquez

   – –

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

   – –

Charges administratives .11.

Réduction des formalités et des obligations administratives liées directement ou indirectement à l'exécution, au respect et/ou au maintien d'un droit, d'une interdiction ou d'une obligation.

↓ Si des citoyens (cf. thème 3) et/ou des entreprises (cf. thème 10) sont concernés, répondez aux questions suivantes.

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation.
   S'il n'y a aucune formalité ou obligation, expliquez pourquoi.

   a. Réglementation actuelle

   ↓ S'il y a des formalités et des obligations dans la réglementation actuelle*, répondez aux questions 2a à 4a.

   b. Réglementation en projet**

   ↓ S'il y a des formalités et des obligations dans la réglementation en projet**, répondez aux questions 2b à 4b.

2. Quels documents et informations chaque groupe concerné doit-il fournir ?

   a. /

   b. Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication.

3. Comment s'effectue la récolte des informations et des documents, par groupe concerné ?

   a. /

   b. Ces données peuvent être demandées par certaines autorités compétentes.

4. Quelles est la périodicité des formalités et des obligations, par groupe concerné ?

   a. /

   b. Cela dépend des demandes des autorités compétentes.

5. Quelles mesures sont prises pour alléger / compenser les éventuels impacts négatifs ?

   – –

Énergie .12.

Mix énergétique (bas carbone, renouvelable, fossile), utilisation de la biomasse (bois, biocarburants), efficacité énergétique, consommation d'énergie de l'industrie, des services, des transports et des ménages, sécurité d'approvisionnement, accès aux biens et services énergétiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Mobilité .13.

Volume de transport (nombre de kilomètres parcourus et nombre de véhicules), offre de transports collectifs, offre routière, ferroviaire, maritime et fluviale pour les transports de marchandises, répartitions des modes de transport (modal shift), sécurité, densité du trafic.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Alimentation .14.

Accès à une alimentation sûre (contrôle de qualité), alimentation saine et à haute valeur nutritionnelle, gaspillages, commerce équitable.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Changements climatiques .15.

Émissions de gaz à effet de serre, capacité d'adaptation aux effets des changements climatiques, résilience, transition énergétique, sources d'énergies renouvelables, utilisation rationnelle de l'énergie, efficacité énergétique, performance énergétique des bâtiments, piégeage du carbone.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Ressources naturelles .16.

Gestion efficiente des ressources, recyclage, réutilisation, qualité et consommation de l'eau (eaux de surface et souterraines, mers et océans), qualité et utilisation du sol (pollution, teneur en matières organiques, érosion, assèchement, inondations, densification, fragmentation), déforestation.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Air intérieur et extérieur .17.

Qualité de l'air (y compris l'air intérieur), émissions de polluants (agents chimiques ou biologiques : méthane, hydrocarbures, solvants, SOx, NOx, NH3), particules fines.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Biodiversité .18.

Niveaux de la diversité biologique, état des écosystèmes (restauration, conservation, valorisation, zones protégées) , altération et fragmentation des habitats, biotechnologies, brevets d'invention sur la matière biologique, utilisation des ressources génétiques, services rendus par les écosystèmes (purification de l'eau et de l'air, …), espèces domestiquées ou cultivées, espèces exotiques envahissantes, espèces menacées.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Nuisances .19.

Nuisances sonores, visuelles ou olfactives, vibrations, rayonnements ionisants, non ionisants et électromagnétiques, nuisances lumineuses.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Autorités publiques .20.

Fonctionnement démocratique des organes de concertation et consultation, services publics aux usagers, plaintes, recours, contestations, mesures d'exécution, investissements publics.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Cohérence des politiques en faveur du développement .21.

Prise en considération des impacts involontaires des mesures politiques belges sur les intérêts des pays en développement.

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants :

- o sécurité alimentaire
- o santé et accès aux médicaments
- o travail décent
- o commerce local et international
- o revenus et mobilisations de ressources domestiques (taxation)
- o mobilité des personnes
- o environnement et changements climatiques (mécanismes de développement propre)
- o paix et sécurité

Expliquez si aucun pays en développement n'est concerné.

L'avant-projet de loi ne concerne pas les pays en développement. L'avant-projet concerne la Belgique.

↓ S'il y a des impacts positifs et/ou négatifs, répondez à la question 2.

2. Précisez les impacts par groupement régional ou économique (lister éventuellement les pays). Cf. manuel

_ _

↓ S'il y a des impacts négatifs, répondez à la question 3.

3. Quelles mesures sont prises pour les alléger / compenser les impacts négatifs ?

_ _

RIA formulier - v2 - oct. 2014

Regelgevingsimpactanalyse

RiA-AiR

:: Vul het formulier bij voorkeur online in ria-air.fed.be
:: Contacteer de helpdesk indien nodig ria-air@premier.fed.be
:: Raadpleeg de handleiding, de FAQ, enz. www.vereenvoudiging.be

Beschrijvende fiche

Auteur .a.

Bevoegd regeringslid	Minister van Justitie_
Contactpersoon beleidscel (Naam, E-mail, Tel. Nr.)	**Samuelle Godin - Samuelle@teamjustitie.be**
Overheidsdienst	FOD Justitie
Contactpersoon overheidsdienst (Naam, E-mail, Tel. Nr.)	Frederik Decruyenaere – frederik.decruyenaere@just.fgov.be – 02/542 67 87

Ontwerp .b.

Titel van het ontwerp van regelgeving	Voorontwerp van wet betreffende de invoering van maatregelen met het oog op het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie _ _
Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.	Via arrest nr. 57/2001 van 22 april 2021 heeft het Grondwettelijk Hof de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie nietig verklaard daar ze berusten op een verplichting tot een algemene en ongedifferentieerde bewaring van de gegevens. Het wetsontwerp beoogt hoofdzakelijk om de ter zake geldende wetgeving te herstellen, rekening houdende met de bezwaren van het Grondwettelijk Hof en de rechtspraak van het Europees Hof van Justitie, en in het bijzonder het arrest-"La Quadrature du Net" (gevoegde zaken C-511/18, C-512/18 en C-520/18 van 6 oktober 2020). Aldus bestaat het leitmotiv van dit wetsontwerp in het voortdurend streven naar het juiste evenwicht tussen de inachtneming van de persoonsgebonden gegevens, en bij uitbreiding de persoonlijke levenssfeer van de burgers, en het vrijwaren van de nationale veiligheid en de bescherming van de openbare veiligheid.
Impactanalyses reeds uitgevoerd	☒ Ja ☐ Nee — Indien ja, gelieve een kopie bij te voegen of de referentie van het document te vermelden: _ _

Raadpleging over het ontwerp van regelgeving .c.

Verplichte, facultatieve of informele raadplegingen:	Inspectie Financiën – Minister Begroting - Gegevensbeschermingsautoriteiten– openbare raadpleging- Overlegcomité - Interministerieel Comité voor Telecommunicatie en Radio-omroep en Televisie – Raad van State.

Bronnen gebruikt om de impactanalyse uit te voeren .d.

Statistieken, referentiedocumenten, organisaties en contactpersonen:	_ _

Datum van beëindiging van de impactanalyse .e.

_

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

>

Een ontwerp van regelgeving zal meestal slechts impact hebben op enkele thema's.

Een niet-exhaustieve lijst van trefwoorden is gegeven om de inschatting van elk thema te vergemakkelijken.

Indien er een **positieve en/of negatieve impact** is, leg deze uit (gebruik indien nodig trefwoorden) en vermeld welke maatregelen worden genomen om de eventuele negatieve effecten te verlichten/te compenseren.

Voor de thema's 3, 10, 11 en 21, worden meer gedetailleerde vragen gesteld.

Raadpleeg de handleiding of contacteer de helpdesk ria-air@premier.fed.be indien u vragen heeft.

Kansarmoedebestrijding .1.

Menswaardig minimuminkomen, toegang tot kwaliteitsvolle diensten, schuldenoverlast, risico op armoede of sociale uitsluiting (ook bij minderjarigen), ongeletterdheid, digitale kloof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Gelijke Kansen en sociale cohesie .2.

Non-discriminatie, gelijke behandeling, toegang tot goederen en diensten, toegang tot informatie, tot onderwijs en tot opleiding, loonkloof, effectiviteit van burgerlijke, politieke en sociale rechten (in het bijzonder voor kwetsbare bevolkingsgroepen, kinderen, ouderen, personen met een handicap en minderheden).

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Gelijkheid van vrouwen en mannen .3.

Toegang van vrouwen en mannen tot bestaansmiddelen: inkomen, werk, verantwoordelijkheden, gezondheid/zorg/welzijn, veiligheid, opleiding/kennis/vorming, mobiliteit, tijd, vrije tijd, etc.

Uitoefening door vrouwen en mannen van hun fundamentele rechten: burgerlijke, sociale en politieke rechten.

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

   Indien geen enkele persoon betrokken is, leg uit waarom.

   De betrokken hoofdstukken hebben geen betrekking of impact op de gelijkheid van mannen en vrouwen.

↓ Indien er personen betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de eventuele verschillen in de respectieve situatie van vrouwen en mannen binnen de materie waarop het ontwerp van regelgeving betrekking heeft.

↓ Indien er verschillen zijn, beantwoord dan vragen 3 en 4.

3. Beperken bepaalde van deze verschillen de toegang tot bestaansmiddelen of de uitoefening van fundamentele rechten van vrouwen of mannen (problematische verschillen)? [J/N] > Leg uit

   _ _

4. Identificeer de positieve en negatieve impact van het ontwerp op de gelijkheid van vrouwen en mannen, rekening houdend met de voorgaande antwoorden?

   _ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 5.

5. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

   _ _

Gezondheid .4.

Toegang tot kwaliteitsvolle gezondheidszorg, efficiëntie van het zorgaanbod, levensverwachting in goede gezondheid, behandelingen van chronische ziekten (bloedvatenziekten, kankers, diabetes en chronische ademhalingsziekten), gezondheidsdeterminanten (sociaaleconomisch niveau, voeding, verontreiniging), levenskwaliteit.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Werkgelegenheid .5.

Toegang tot de arbeidsmarkt, kwaliteitsvolle banen, werkloosheid, zwartwerk, arbeids- en ontslagomstandigheden, loopbaan, arbeidstijd, welzijn op het werk, arbeidsongevallen, beroepsziekten, evenwicht privé- en beroepsleven, gepaste verloning, mogelijkheid tot beroepsopleiding, collectieve arbeidsverhoudingen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Consumptie- en productiepatronen .6.

Prijsstabiliteit of -voorzienbaarheid, inlichting en bescherming van de consumenten, doeltreffend gebruik van hulpbronnen, evaluatie en integratie van (sociale- en milieu-) externaliteiten gedurende de hele levenscyclus van de producten en diensten, beheerpatronen van organisaties.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Economische ontwikkeling .7.

Oprichting van bedrijven, productie van goederen en diensten, arbeidsproductiviteit en productiviteit van hulpbronnen/grondstoffen, competitiviteitsfactoren, toegang tot de markt en tot het beroep, markttransparantie, toegang tot overheidsopdrachten, internationale handels- en financiële relaties, balans import/export, ondergrondse economie, bevoorradingszekerheid van zowel energiebronnen als minerale en organische hulpbronnen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Investeringen .8.

Investeringen in fysiek (machines, voertuigen, infrastructuren), technologisch, intellectueel (software, onderzoek en ontwikkeling) en menselijk kapitaal, nettoinvesteringscijfer in procent van het bbp.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Onderzoek en ontwikkeling .9.

Mogelijkheden betreffende onderzoek en ontwikkeling, innovatie door de invoering en de verspreiding van nieuwe productiemethodes, nieuwe ondernemingspraktijken of nieuwe producten en diensten, onderzoeks- en ontwikkelingsuitgaven.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Kmo's .10.

Impact op de ontwikkeling van de kmo's.

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?
   Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (< 50 werknemers), waaronder het % micro-ondernemingen (< 10 werknemers).
   Indien geen enkele onderneming betrokken is, leg uit waarom.
   De operatoren die elektronische communicatiediensten aanbieden zijn betrokken.

↓ Indien er kmo's betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.
   N.B. De impact op de administratieve lasten moet bij thema 11 gedetailleerd worden.
   Er is geen specifieke impact op kmo's.

↓ Indien er een negatieve impact is, beantwoord dan vragen 3 tot 5.

3. Is deze impact verhoudingsgewijs zwaarder voor de kmo's dan voor de grote ondernemingen? [J/N] > Leg uit
   _ _
4. Staat deze impact in verhouding tot het beoogde doel? [J/N] > Leg uit
   _ _
5. Welke maatregelen worden genomen om deze negatieve impact te verlichten / te compenseren?
   _ _

Administratieve lasten .11.

Verlaging van de formaliteiten en administratieve verplichtingen die direct of indirect verbonden zijn met de uitvoering, de naleving en/of de instandhouding van een recht, een verbod of een verplichting.

↓ Indien burgers (zie thema 3) en/of ondernemingen (zie thema 10) betrokken zijn, beantwoord dan volgende vragen.

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving.
   Indien er geen enkele formaliteiten of verplichtingen zijn, leg uit waarom.

a. _ _huidige regelgeving*

↓ Indien er formaliteiten en/of verplichtingen zijn in de huidige* regelgeving, beantwoord dan vragen 2a tot 4a.

b. _ _ontwerp van regelgeving

↓ Indien er formaliteiten en/of verplichtingen zijn in het ontwerp van regelgeving**, beantwoord dan vragen 2b tot 4b.

2. Welke documenten en informatie moet elke betrokken doelgroep verschaffen?
   a. /
   b. Gegevens m.b.t. elektronische communicatie..
3. Hoe worden deze documenten en informatie, per betrokken doelgroep, ingezameld?
   a. /
   b. Zij kunnen opgevraagd worden door bevoegde autoriteiten.
4. Welke is de periodiciteit van de formaliteiten en verplichtingen, per betrokken doelgroep?
   a. _ _*
   b. Afhankelijk van opvraging door bevoegde autoriteiten.
5. Welke maatregelen worden genomen om de eventuele negatieve impact te verlichten / te compenseren?
   _ _

Energie .12.

Energiemix (koolstofarm, hernieuwbaar, fossiel), gebruik van biomassa (hout, biobrandstoffen), energie-efficiëntie, energieverbruik van de industrie, de dienstensector, de transportsector en de huishoudens, bevoorradingszekerheid, toegang tot energiediensten en -goederen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Mobiliteit .13.

Transportvolume (aantal afgelegde kilometers en aantal voertuigen), aanbod van gemeenschappelijk personenvervoer, aanbod van wegen, sporen en zee- en binnenvaart voor goederenvervoer, verdeling van de vervoerswijzen (modal shift), veiligheid, verkeersdichtheid.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Voeding .14.

Toegang tot veilige voeding (kwaliteitscontrole), gezonde en voedzame voeding, verspilling, eerlijke handel.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Klimaatverandering .15.

Uitstoot van broeikasgassen, aanpassingsvermogen aan de gevolgen van de klimaatverandering, veerkracht, energie overgang, hernieuwbare energiebronnen, rationeel energiegebruik, energie-efficiëntie, energieprestaties van gebouwen, winnen van koolstof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Natuurlijke hulpbronnen .16.

Efficiënt beheer van de hulpbronnen, recyclage, hergebruik, waterkwaliteit en -consumptie (oppervlakte- en grondwater, zeeën en oceanen), bodemkwaliteit en -gebruik (verontreiniging, organisch stofgehalte, erosie, drooglegging, overstromingen, verdichting, fragmentatie), ontbossing.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Buiten- en binnenlucht .17.

Luchtkwaliteit (met inbegrip van de binnenlucht), uitstoot van verontreinigende stoffen (chemische of biologische agentia: methaan, koolwaterstoffen, oplosmiddelen, SOX, NOX, NH3), fijn stof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Biodiversiteit .18.

Graad van biodiversiteit, stand van de ecosystemen (herstelling, behoud, valorisatie, beschermde zones), verandering en fragmentatie van de habitatten, biotechnologieën, uitvindingsoctrooien in het domein van de biologie, gebruik van genetische hulpbronnen, diensten die de ecosystemen leveren (water- en luchtzuivering, enz.), gedomesticeerde of gecultiveerde soorten, invasieve uitheemse soorten, bedreigde soorten.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Hinder .19.

Geluids-, geur- of visuele hinder, trillingen, ioniserende, niet-ioniserende en elektromagnetische stralingen, lichtoverlast.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Overheid .20.

Democratische werking van de organen voor overleg en beraadslaging, dienstverlening aan gebruikers, klachten, beroep, protestbewegingen, wijze van uitvoering, overheidsinvesteringen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Beleidscoherentie ten gunste van ontwikkeling .21.

Inachtneming van de onbedoelde neveneffecten van de Belgische beleidsmaatregelen op de belangen van de ontwikkelingslanden.

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van:

- o voedselveiligheid
- o gezondheid en toegang tot geneesmiddelen
- o waardig werk
- o lokale en internationale handel
- o inkomens en mobilisering van lokale middelen (taxatie)
- o mobiliteit van personen
- o leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling)
- o vrede en veiligheid

Indien er geen enkelen ontwikkelingsland betrokken is, leg uit waarom.

Dit ontwerp heeft geen betrekking op ontwikkelingslanden. Het voorontwerp heeft betrekking op België.

↓ Indien er een positieve en/of negatieve impact is, beantwoord dan vraag 2.

2. Verduidelijk de impact per regionale groepen of economische categorieën (eventueel landen oplijsten). Zie bijlage

_ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 3.

3. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

_ _

AVIS DU CONSEIL D'ÉTAT N° 69.381/4 DU 28 JUIN 2021

Le 10 mai 2021, le Conseil d'État, section de législation, a été invité par le Vice-Premier ministre et ministre de la Justice et de la Mer du Nord à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités'.

L'avant-projet a été examiné par la quatrième chambre le 28 juin 2021. La chambre était composée de Martine Baguet, président de chambre, Luc Cambier et Bernard Blero, conseillers d'État, Sébastien Van Drooghenbroeck et Marianne Dony, assesseurs, et Anne-Catherine Van Geersdaele, greffier.

Le rapport a été présenté par Anne Vagman, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine Baguet.

L'avis, dont le texte suit, a été donné le 28 juin 2021.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[1‡], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

Formalités préalables

L'avant-projet de loi soumis pour avis a été délibéré en Conseil des ministres du 7 mai 2021, où il a été décidé que le texte en projet adopté fera l'objet d'une consultation publique et sera adressé pour avis aux Autorités de protection des données et au Conseil d'État. Les résultats de ces différentes consultations seront alors discutés au sein du Groupe de travail de coordination de la politique concerné et l'avant-projet, le cas échéant adapté, sera ensuite soumis au Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision, et au Comité de concertation[2].

1 ‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

2 Ceci ressort également de la lettre de demande d'avis.

ADVIES VAN DE RAAD VAN STATE NR. 69.381/4 VAN 28 JUNI 2021

Op 10 mei 2021 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'betreffende het verzamelen en het bewaren van de identificatie-, verkeers-en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten'.

Het voorontwerp is door de vierde kamer onderzocht op 28 juni 2021. De kamer was samengesteld uit Martine Baguet, kamervoorzitter, Luc Cambier en Bernard Blero, staatsraden, Sébastien Van Drooghenbroeck en Marianne Dony, assessoren, en Anne-Catherine Van Geersdaele, griffier.

Het verslag is uitgebracht door Anne Vagman, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine Baguet.

Het advies, waarvan de tekst hierna volgt, is gegeven op 28 juni 2021.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[1‡] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

Voorafgaande vormvereisten

Over dit voorontwerp van wet dat ter fine van advies voorgelegd is, is overleg gepleegd op de Ministerraad van 7 mei 2021, waarop besloten is dat over de ontworpen tekst een openbare raadpleging gehouden moet worden en dat die tekst om advies voorgelegd moet worden aan de Gegevensbeschermingsautoriteiten en aan de Raad van State. De resultaten van al die raadplegingen zullen vervolgens binnen de betrokken Werkgroep Beleidscoördinatie besproken worden, waarna de eventueel aangepaste tekst van het voorontwerp voorgelegd zal worden aan het Interministerieel Comité voor Telecommunicatie en Radio-Omroep en Televisie en aan het Overlegcomité.[2]

1 ‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

2 Dit blijkt ook uit de brief met de adviesaanvraag.

À la suite de cette concertation, le Groupe de travail se réunira à nouveau et si “des problèmes se posent encore au sein du Groupe de travail, en ce qui concerne les adaptations éventuelles nécessaire”, le texte en projet sera à nouveau soumis au Conseil des ministres. Si par contre, aucun problème de ne se pose au sein du Groupe de travail, l’avant-projet sera soumis à la signature du Roi, en vue de son dépôt à la chambre des représentants.

La section de législation relève en outre que l’avis de l’Organe de contrôle de l’information policière a été donné le 21 mai 2021; la consultation publique s’est, pour sa part, clôturée le 4 juin 2021; enfin, l’avis du Comité Permanent R a été donné le 14 juin 2021. Ces documents ont été transmis à la section de législation postérieurement à l’introduction de la demande d’avis et sont également postérieurs, à fortiori, à la délibération du Conseil des ministres du 7 mai 2021.

Il résulte de ce qui précède que le texte soumis pour avis est encore susceptible de subir des modifications autres que celles qui pourraient découler de l’avis de la section de législation: ainsi il pourrait faire l’objet de modifications à la suite de la consultation publique, des avis des autorités de protection des données, de l’Organe de contrôle de l’information policière et du Comité permanent R et à l’issue de la concertation organisée au sein du Comité interministériel et du Comité de concertation.

Or, et même si la section de législation est tenue de se prononcer sur un avant-projet législatif ou sur un projet réglementaire, même lorsque les formalités préalables obligatoires n’ont pas été accomplies[3], pour que celle-ci puisse accomplir correctement sa mission, il y a toutefois lieu de lui soumettre des projets de texte à priori définitifs, non seulement pour éviter qu’elle n’examine inutilement un texte qui fera l’objet de modifications ultérieures, mais également pour qu’un projet ne doive lui être soumis à nouveau pour avis en raison de modifications autres que celles résultant de son avis[4].

Les auteurs de l’avant-projet sont invités à se conformer dorénavant à la règle ainsi rappelée.

Na dat overleg zal die Werkgroep opnieuw samenkomen en “[i]ndien er zich in de schoot van de Werkgroep nog problemen stellen bij eventuele aanpassingen die nodig zouden zijn”, zal de ontworpen tekst opnieuw aan de Ministerraad voorgelegd worden. In het andere geval, als er binnen de Werkgroep geen problemen meer zijn, zal het voorontwerp ter ondertekening aan de Koning voorgelegd worden met het oog op indiening bij de Kamer van volksvertegenwoordigers.

De afdeling Wetgeving wijst er voorts op dat het advies van het Controleorgaan op de politionele informatie gegeven is op 21 mei 2021, dat de openbare raadpleging, harerzijds, afgesloten is op 4 juni 2021 en dat het advies van het Vast Comité I, ten slotte, uitgebracht is op 14 juni 2021. Die stukken zijn aan de afdeling Wetgeving overgezonden na de indiening van de adviesaanvraag en zijn *a fortiori* van recentere datum dan het overleg in de Ministerraad dat op 7 mei 2021 plaatsgehad heeft.

Uit het voorgaande blijkt dat de om advies voorgelegde tekst nog vatbaar is voor wijzigingen die niet voortvloeien uit het advies van de afdeling Wetgeving: zo zouden daarin wijzigingen aangebracht kunnen worden naar aanleiding van de openbare raadpleging, de adviezen van de Gegevensbeschermingsautoriteiten, van het Controleorgaan op de politionele informatie en van het Vast Comité I en na afloop van het overleg dat binnen het Interministerieel Comité en het Overlegcomité moet plaatsvinden.

Ook al is de afdeling Wetgeving ertoe gehouden om over een wetgevend voorontwerp of over een ontwerp van besluit advies uit te brengen zelfs indien de verplichte voorafgaande vormvereisten niet vervuld zijn,[3] dienen aan haar evenwel, om haar in staat te stellen haar taak naar behoren te vervullen, definitieve ontwerpteksten voorgelegd te worden, niet alleen om een onnodig onderzoek te vermijden van een tekst die naderhand nog gewijzigd zal worden, maar ook om te vermijden dat een ontwerp ten gevolge van wijzigingen die niet het gevolg zijn van haar advies, opnieuw om advies voorgelegd dient te worden.[4]

De stellers van het voorontwerp worden verzocht zich voortaan te houden aan de regel die aldus in herinnering gebracht is.

---

3 Il résulte de l’article 84, § 3, alinéa 2, des lois ‘sur le Conseil d’État’, coordonnées le 12 janvier 1973, que lorsque l’avis de la section de législation est sollicité dans un délai de trente ou soixante jours, ou de cinq jours ouvrables, l’avis est donné “nonobstant l’inaccomplissement éventuel des formalités prescrites”.

4 Voir, en ce sens l’avis n° 39.690/3 donné le 8 février 2006 sur un avant-projet devenu la loi du 20 juillet 2006 ‘relative à la création et au fonctionnement de l’Agence fédérale des médicaments et des produits de santé’, *http://www.raadvst-consetat.be/dbx/avis/39690.pdf*.

3 Uit artikel 84, § 3, tweede lid, van de wetten ‘op de Raad van State’, gecoördineerd op 12 januari 1973, volgt dat, wanneer het advies gevraagd wordt binnen een termijn van dertig of zestig dagen dan wel van vijf werkdagen, het gegeven wordt “zelfs indien de voorgeschreven vormvereisten niet zijn vervuld”.

4 Zie in deze zin advies 39.690/3, dat op 8 februari 2006 gegeven is over een voorontwerp dat geleid heeft tot de wet van 20 juli 2006 ‘betreffende de oprichting en de werking van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten’, *http://www.raadvst-consetat.be/dbx/adviezen/39690.pdf*.

PORTÉE ET CONTEXTE DE L'AVANT-PROJET

A. Droit et jurisprudence européens et jurisprudence interne

1.1. Par un arrêt du 8 avril 2014, rendu en grande chambre en réponse aux questions préjudicielles de la Haute Cour d'Irlande et de la Cour constitutionnelle d'Autriche[5], la Cour de Justice de l'Union européenne (ci-après "La Cour de Justice") a invalidé la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 'sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, et modifiant la directive 2002/58/CE'.

À la suite de cet arrêt de la Cour de Justice, l'arrêt 84/2015 du 11 juin 2015 de la Cour constitutionnelle a annulé la loi du 30 juillet 2013 'portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle', laquelle avait pour objet d'assurer la transposition partielle de la directive 2006/24/CE.

L'arrêt de la Cour constitutionnelle repose sur la motivation suivante:

"B.10.1. Comme la Cour de justice l'a relevé aux points 56 et 57 de son arrêt, la directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet, couvrant de manière généralisée toute personne et tous les moyens de communication électronique sans distinction en fonction de l'objectif de lutte contre les infractions graves que le législateur de l'Union entendait poursuivre.

La loi attaquée ne se distingue nullement de la directive sur ce point. En effet, ainsi qu'il est dit en B.8, les catégories de données qui doivent être conservées sont identiques à celles énumérées par la directive tandis qu'aucune distinction n'est opérée quant aux personnes concernées ou aux règles particulières à prévoir en fonction de l'objectif de lutte contre les infractions décrites à l'article 126, § 2, de la loi du 13 juin 2005 remplacé par la loi attaquée. Tout comme la Cour de justice l'a constaté à propos de la directive (point 58), la loi s'applique donc également à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel.

[5] C.J.(gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for communications, Marine and Natural Resouces e.a.,* 8 avril 2014, C-293/12, ECLI:EU:C:2014:238 et C.J. (gde ch.), arrêt *Kärntner Landesregierung e.a. c. Autriche*, C-594/12, ECLI:EU:C:2014:238, ci-après, l'arrêt "*Digital Rights*").

REIKWIJDTE EN CONTEXT VAN HET VOORONTWERP

A. Europees recht en Europese rechtspraak en interne rechtspraak

1.1. Bij een arrest van 8 april 2014 van de grote kamer in antwoord op prejudiciële vragen vanwege het Hooggerechtshof van Ierland en het Grondwettelijk Hof van Oostenrijk[5] heeft het Hof van Justitie van de Europese Unie (hierna "het Hof van Justitie") richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 'betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG' ongeldig verklaard.

Naar aanleiding van dat arrest van het Hof van Justitie heeft het Grondwettelijk Hof bij arrest nr. 84/2015 van 11 juni 2015 de vernietiging uitgesproken van de wet van 30 juli 2013 'houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering', welke wet strekte tot de gedeeltelijke omzetting van richtlijn 2006/24/EG.

Dat arrest van het Grondwettelijk Hof steunt op de volgende motivering:

"B.10.1. Zoals het Hof van Justitie heeft opgemerkt in de punten 56 en 57 van zijn arrest, schrijft de richtlijn voor om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren, waardoor zij algemeen van toepassing is op alle personen en alle elektronische communicatiemiddelen, zonder onderscheid op basis van het doel, namelijk zware criminaliteit bestrijden, dat de Uniewetgever wilde nastreven.

De bestreden wet verschilt op dat punt niet van de richtlijn. Zoals in B.8 is vermeld, zijn immers de categorieën van gegevens die moeten worden bewaard identiek aan die welke zijn opgesomd in de richtlijn, terwijl geen enkel onderscheid wordt gemaakt met betrekking tot de betrokken personen of de bijzondere regels die moeten worden bepaald op basis van het doel van bestrijding van de inbreuken beschreven in artikel 126, § 2, van de wet van 13 juni 2005, dat bij de bestreden wet werd vervangen. Net zoals het Hof van Justitie heeft vastgesteld met betrekking tot de richtlijn (punt 58), is de wet dus ook van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - een verband vertoont met de in de bestreden wet opgesomde inbreuken. Op dezelfde wijze is de wet, zonder enige uitzondering, ook van toepassing op personen van wie de communicaties onder het beroepsgeheim vallen.

[5] HvJ (grote kamer), arrest *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e.a.,* 8 april 2014, C-293/12, ECLI:EU:C:2014:238 en HvJ (grote kamer), arrest *Kärntner Landesregierung e.a. v. Oostenrijk*, C-594/12, ECLI:EU:C:2014:238, hierna het arrest "*Digital Rights*").

B.10.2. Pas plus que ce n'est le cas pour la directive, l'article 5 attaqué ne requiert-il une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Il ne limite pas non plus la conservation des données afférentes à une période temporelle ou à une zone géographique déterminée ou encore à un cercle de personnes susceptibles d'être mêlées à une infraction visée par la loi, ou qui pourraient contribuer par la conservation des données, à prévenir, détecter ou poursuivre ces infractions.

B.10.3. Si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l'article 126, § 5, 3°, de la loi du 13 juin 2005, remplacé par l'article 5 de la loi attaquée, aucune condition matérielle ou procédurale n'est définie par la loi quant à cet accès.

B.10.4. Enfin, en ce qui concerne la durée de conservation des données, la loi n'opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

B.11. Par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive 'conservation des données' invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52.1. de la Charte des droits fondamentaux de l'Union européenne.

Partant, l'article 5 précité viole les articles 10 et 11 de la Constitution lus en combinaison avec ces dispositions. Le moyen unique dans l'affaire n° 5856 et le premier moyen dans l'affaire n° 5859 sont fondés.

B.12. En raison de leur caractère indissociable avec l'article 5, il y a lieu d'annuler également les articles 1er à 4, 6 et 7 de la loi du 30 juillet 2013 attaquée et donc l'intégralité de ladite loi".

1.2. Faisant suite à ces deux décisions, le législateur a adopté la loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques'[6].

Cette loi a fait l'objet de quatre recours en annulation auprès de la Cour constitutionnelle, qui a posé, par son arrêt n° 96/2018 du 19 juillet 2018, les questions préjudicielles suivantes à la Cour de Justice:

"1. L'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, § 1er [lire: paragraphe 1], de la Charte des droits fondamentaux de l'Union européenne, doit-il être

6 La section de législation a, le 7 décembre 2015, donné un avis n° 58.449/4 sur un avant-projet devenu cette loi du 29 mai 2016, *http://www.raadvst-consetat.be/dbx/avis/58449.pdf*.

B.10.2. Niet méér dan het geval is voor de richtlijn, vereist het bestreden artikel 5 enig verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Het beperkt evenmin de bewaring van de desbetreffende gegevens tot een bepaalde periode of een bepaalde geografische zone of nog tot een kring van personen die betrokken kunnen zijn bij een door de wet beoogde inbreuk, of die zouden kunnen helpen, door het bewaren van de gegevens, bij het voorkomen, opsporen of vervolgen van die inbreuken.

B.10.3. Ook al worden de autoriteiten die gemachtigd zijn tot toegang tot de bewaarde gegevens, opgesomd in artikel 126, § 5, 3°, van de wet van 13 juni 2005, vervangen bij artikel 5 van de bestreden wet, toch wordt bij de wet geen enkele materiële of procedurele voorwaarde vastgelegd met betrekking tot die toegang.

B.10.4. Wat ten slotte de bewaarperiode van de gegevens betreft, maakt de wet geen enkel onderscheid tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken personen.

B.11. Om dezelfde redenen als die welke het Hof van Justitie van de Europese Unie ertoe hebben gebracht de 'Dataretentierichtlijn' ongeldig te verklaren, dient te worden vastgesteld dat de wetgever, met de aanneming van artikel 5 van de bestreden wet, de grenzen heeft overschreden die worden opgelegd door de eerbiediging van het evenredigheidsbeginsel in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Het voormelde artikel 5 schendt bijgevolg de artikelen 10 en 11 van de Grondwet, in samenhang gelezen met die bepalingen. Het enige middel in de zaak nr. 5856 en het eerste middel in de zaak nr. 5859 zijn gegrond.

B.12. Wegens hun ondeelbaar karakter met artikel 5, dienen ook de artikelen 1 tot 4, 6 en 7 van de bestreden wet van 30 juli 2013, en dus de wet in haar geheel, te worden vernietigd."

1.2. De wetgever heeft aan die beide beslissingen gevolg gegeven door de wet van 29 mei 2016 'betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie' aan te nemen.[6]

De vernietiging van die wet is gevorderd bij vier beroepen die ingesteld zijn bij het Grondwettelijk Hof, dat bij zijn arrest nr. 96/2018 van 19 juli 2018 aan het Hof van Justitie de volgende prejudiciële vragen gesteld heeft:

"1. Dient artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met het recht op veiligheid, gewaarborgd bij artikel 6 van het Handvest van de grondrechten van de Europese Unie, en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van

6 De afdeling Wetgeving heeft op 7 december 2015 advies 58.449/4 uitgebracht over een voorontwerp dat tot die wet van 29 mei 2016 geleid heeft, *http://www.raadvst-consetat.be/dbx/adviezen/58449.pdf*.

interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communication électronique, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe 1, du règlement (UE) 2016/679 et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci?

2. L'article 15, paragraphe 1, de la directive 2002/58/CE, combiné avec les articles 4, 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, si cette réglementation a notamment pour objet de réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et 8 de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques?

3. Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi?".

Dans ce même arrêt, la Cour constitutionnelle a décidé de

"suspend[re] en outre l'examen des affaires jusqu'à ce que la Cour de justice ait statué dans les affaires C-207/16 *Ministerio Fiscal et* C-623/17 *Privacy International* / *Secretary of State for Foreign and Commonwealth Affairs e.a.*".

1.3.1. La Cour de Justice a répondu à ces questions préjudicielles, ainsi qu'à d'autres questions posées par le Conseil

de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, nationale regeling die niet alleen ten doel heeft het onderzoeken, opsporen en vervolgen van feiten van zware criminaliteit, maar ook het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit of het voorkomen van een verboden gebruik van de elektronische communicatiesystemen, of de verwezenlijking van een andere doelstelling die is geïdentificeerd bij artikel 23, lid 1, van de Verordening (EU) 2016/679 en die bovendien onderworpen is aan nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe?

2. Dient artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 4, 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, indien die regeling mede tot doel heeft om de op de overheid rustende positieve verplichtingen ingevolge de artikelen 4 en 8 van het Handvest te bewerkstelligen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt en het effectief mogelijk maakt om de pleger van het misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronische communicatiemiddelen?

3. Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden?"

In datzelfde arrest heeft het Grondwettelijk hof beslist om

"het onderzoek van de zaken voorts op [te schorten] totdat het Hof van Justitie uitspraak zal hebben gedaan in de zaken C-207/16 *Ministerio Fiscal* en C-623/17 *Privacy International* / *Secretary of State for Foreign and Commonwealth Affairs e.a.*".

1.3.1. Op die prejudiciële vragen en op andere vragen die aan het Hof van Justitie voorgelegd waren door de Raad van

d'État de France, dans un arrêt du 6 octobre 2020, rendu en grande chambre[7] (ci-après l'arrêt "*La Quadrature du Net*").

1.3.2. Concernant les deux premières questions préjudicielles posées par la Cour constitutionnelle, l'arrêt de la Cour de Justice a motivé sa réponse comme suit:

"108. S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, il ressort de l'article 6 ainsi que des considérants 22 et 26 de la directive 2002/58 qu'un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 86 et jurisprudence citée).

109. Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.

110.Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par l'un de ces motifs.

111. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de

[7] C.J. (gde ch.), arrêt *La Quadrature du Net et autres c. Premier ministre e.a.,* 6 octobre 2020, C-511/18, ECLI:EU:C:2020:791 et C.J. (gde ch.), arrêt *French Data network e.a*., C-512/18 et C.J. (gde ch.), arrêt *Ordre des barreaux francophones et germanophone et autres*, C-520/18.

State van Frankrijk heeft dat Hof geantwoord in een arrest dat op 6 oktober 2020 uitgesproken is in grote kamer[7] (hierna het arrest "*La Quadrature du Net*").

1.3.2. Wat de eerste twee prejudiciële vragen betreft die door het Grondwettelijk Hof gesteld zijn, heeft het Hof van Justitie zijn antwoord als volgt gemotiveerd in zijn arrest:

"108. Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronischecommunicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van richtlijn 2002/58 dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij zijn geanonimiseerd of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (arrest van 21 december 2016*, Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 86 en aldaar aangehaalde rechtspraak).

109. Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd.

110. Artikel 15, lid 1, van richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

111. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod

[7] HvJ (grote kamer), arrest *La Quadrature du Net e. a. v. Premier ministre e.a.,* 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791 en HvJ (grote kamer), arrest *French Data network e.a*., C-512/18 en HvJ (grote kamer), arrest *Ordre des barreaux francophones et germanophone e. a.*, C-520/18.

cette directive, devienne la règle (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104).

112. Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 52 et jurisprudence citée).

113. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

114. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99P, EU:C:2001:127, point 39, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

115. Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la

om deze gegevens op te slaan de regel wordt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104).

112. Met betrekking tot de doelstellingen die een beperking van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kunnen rechtvaardigen, heeft het Hof reeds geoordeeld dat de in artikel 15, lid 1, eerste zin, van deze richtlijn gegeven opsomming van doelstellingen exhaustief is, zodat een op grond van die bepaling vastgestelde wettelijke maatregel daadwerkelijk en strikt moet berusten op een van die doelstellingen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 52 en aldaar aangehaalde rechtspraak).

113. Bovendien volgt uit artikel 15, lid 1, derde zin, van richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

114. Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie volgens artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, *Connolly/Commissie*, C-274/99 P, EU:C:2001:127, punt 39, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 93 en aldaar aangehaalde rechtspraak).

115. In dit verband dient te worden gepreciseerd dat de bewaring van verkeers- en locatiegegevens als zodanig behalve een uitzondering op het in artikel 5, lid 1, van richtlijn 2002/58 gestelde verbod op de opslag van die gegevens door anderen dan de gebruikers, ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten op eerbiediging van het privéleven en bescherming van

protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNRUE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée; voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 30 janvier 2020, Breyer c. Allemagne, CE:ECHR:2020:0130 JUD005000 112, § 81].

116. Il est également sans pertinence que les données conservées soient ou non utilisées par la suite (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 16 février 2000, Amann c. Suisse, CE:ECHR:2000:0216JUD002779895, § 69, ainsi que 13 février 2020, Trjakovski et Chipovskic Macédoine du Nord, CE:ECHR:2020:0213JUD005320513, § 51), l'accès à de telles données constituant, quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126].

117. Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 27, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 99).

118. Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 28, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 101). Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du

persoonsgegevens vormt, waarbij niet van belang is of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak; zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 30 januari 2020, *Breyer tegen Duitsland*, CE:ECHR:2020:0130JUD005000112, § 81].

116. Het is ook irrelevant of de bewaarde gegevens vervolgens al dan niet worden gebruikt (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 16 februari 2000, *Amann t. Zwisterland*, CE:ECHR:2000:0216JUD002779895, § 69, en 13 februari 2020, *Trjakovski en Chipovski t. Noord-Macedonië*, CE:ECHR:2020:0213JUD005320513, § 51), aangezien de toegang tot die gegevens, ongeacht het latere gebruik ervan, op zichzelf al een inmenging vormt in de in het voorgaande punt genoemde grondrechten [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126].

117. Deze conclusie is des te meer gerechtvaardigd daar verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. In het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 27, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 99).

118. De bewaring van verkeers- en locatiegegevens voor politiële doeleinden kan dus om te beginnen op zichzelf afbreuk doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie en de gebruikers van elektronischecommunicatiemiddelen ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 28, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 101). Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het

23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés.

119. D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

120. Cela étant, en ce qu'il permet aux États membres d'introduire les dérogations visées au point 110 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

121. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

122. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui.

123. À cet égard, l'article 6 de la Charte, auquel se réfèrent le Conseil d'État et la Cour constitutionnelle, consacre le droit de toute personne non seulement à la liberté mais également à la sûreté et garantit des droits correspondant à ceux qui le sont à l'article 5 de la CEDH (voir, en ce sens, arrêts du 15 février 2016, N., C-601/15PPU, EU:C:2016:84, point 47; du 28 juillet 2016, JZ, C-294/16PPU, EU:C:2016:610, point 48, ainsi que du 19 septembre 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, point 42 et jurisprudence citée).

124. En outre, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne. Il convient donc de tenir compte des droits correspondants de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimale [voir, en ce sens, arrêts du 12 février 2019, TC, C-492/18PPU, EU:C:2019:108,

Unierecht melden (*PB* 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn.

119. Bovendien is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene en ongedifferentieerde bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

120. Het feit dat het de lidstaten op grond van artikel 15, lid 1, van richtlijn 2002/58 is toegestaan om te voorzien in de in punt 110 van het onderhavige arrest bedoelde uitzonderingen, heeft ermee te maken dat de in de artikelen 7, 8 en 11 van het Handvest verankerde rechten geen absolute gelding hebben, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).

121. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

122. Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 in het licht van het Handvest moet derhalve ook rekening worden gehouden met het belang van de door de artikelen 3, 4, 6 en 7 van het Handvest gewaarborgde rechten en met dat van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van ernstige criminaliteit, die bijdragen tot de bescherming van de rechten en vrijheden van anderen.

123. Zo heeft ingevolge artikel 6 van het Handvest, waaraan de Conseil d'État en het Grondwettelijk Hof refereren, eenieder niet alleen recht op vrijheid, maar ook op veiligheid, en waarborgt deze bepaling rechten die overeenstemmen met die welke worden gewaarborgd door artikel 5 EVRM (zie in die zin arresten van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 47; 28 juli 2016, *JZ*, C-294/16 PPU, EU:C:2016:610, punt 48, en 19 september 2019, *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, punt 42 en aldaar aangehaalde rechtspraak).

124. Voorts zij eraan herinnerd dat artikel 52, lid 3, van het Handvest beoogt te zorgen voor de nodige samenhang tussen de in het Handvest vervatte rechten en de daarmee corresponderende, door het EVRM gewaarborgde rechten, zonder de autonomie van het Unierecht en van het Hof van Justitie van de Europese Unie aan te tasten. Bijgevolg dient bij de uitlegging van het Handvest rekening te worden gehouden met de overeenkomstige rechten van het EVRM, die het minimale beschermingsniveau bepalen [zie in die zin arresten

point 57, ainsi que du 21 mai 2019, Commission/Hongrie (Usufruits sur terres agricoles), C-235/17, EU:C:2019:432, point 72 et jurisprudence citée].

125. S'agissant de l'article 5 de la CEDH, qui consacre le 'droit à la liberté' et le 'droit à la sûreté', celui-ci vise, selon la jurisprudence de la Cour européenne des droits de l'homme, à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée (voir, en ce sens, Cour EDH, 18 mars 2008, Ladent c. Pologne, CE:ECHR:2008:0318JUD001103603, §§ 45 et 46; 29 mars 2010, Medvedyev et autres c. France, CE:ECHR:2010:0329JUD000339403, §§ 76 et 77, ainsi que 13 décembre 2012, El-Masri v. 'The former Yugoslav Republic of Macedonia', CE:ECHR:2012:1213JUD003963009, § 239). Toutefois, dans la mesure où cette disposition vise une privation de liberté commise par une autorité publique, l'article 6 de la Charte ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales.

126. En revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, évoquée par la Cour constitutionnelle, il convient de souligner que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale [voir, en ce sens, arrêt du 18 juin 2020, Commission/Hongrie (Transparence associative), C-78/18, EU:C:2020:476, point 123 et jurisprudence citée de la Cour européenne des droits de l'homme]. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants.

127. Or, face à ces différentes obligations positives, il convient de procéder à une conciliation nécessaire des différents intérêts et droits en cause.

128. En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la CEDH, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différentes intérêts et droits à protéger (Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, §§ 115 et 116; 4 mars 2004, M.C. c. Bulgarie,

van 12 februari 2019, *TC*, C-492/18 PPU, EU:C:2019:108, punt 57, en 21 mei 2019, *Commissie/Hongarije* (*Vruchtgebruik op landbouwgrond*), C-235/17, EU:C:2019:432, punt 72 en aldaar aangehaalde rechtspraak].

125. Artikel 5 EVRM, waarin het 'recht op vrijheid' en het 'recht op veiligheid' zijn verankerd, beoogt volgens de rechtspraak van het EHRM eenieder te beschermen tegen willekeurige en ongerechtvaardigde vrijheidsontneming (zie in die zin EHRM, 18 maart 2008, *Ladent t. Polen*, CE:ECHR:2008:0318JUD001103603, § § 45 en 46; 29 maart 2010, *Medvedyev e.a. t. Frankrijk*, CE:ECHR:2010:0329JUD000339403, § § 76 en 77, en 13 december 2012, *El-Masri t. 'The former Yugoslav Republic of Macedonia* ', CE:ECHR:2012:1213JUD003963009, § 239). Die bepaling ziet echter op vrijheidsontneming door overheidsinstanties, zodat artikel 6 van het Handvest niet aldus kan worden uitgelegd dat het de overheid een verplichting oplegt om specifieke maatregelen te nemen teneinde bepaalde strafbare handelingen tegen te gaan.

126. Wat daarentegen in het bijzonder de door het Grondwettelijk Hof genoemde effectieve bestrijding betreft van strafbare handelingen waarvan met name minderjarigen en andere kwetsbare personen het slachtoffer zijn, moet worden beklemtoond dat uit artikel 7 van het Handvest positieve verplichtingen voor de overheid kunnen voortvloeien om juridische maatregelen te nemen ter bescherming van het privéleven en het familie- en gezinsleven [zie in die zin arrest van 18 juni 2020, *Commissie/Hongarije* (*Transparantie van verenigingen*), C-78/18, EU:C:2020:476, punt 123 en aldaar aangehaalde rechtspraak van het EHRM). Dergelijke verplichtingen kunnen ook uit dat artikel voortvloeien ten aanzien van de bescherming van iemands woning en communicatie, en uit de artikelen 3 en 4 van het Handvest ten aanzien van de bescherming van iemands lichamelijke en geestelijke integriteit en het verbod op folteringen en onmenselijke en vernederende behandelingen.

127. Gelet op die verschillende positieve verplichtingen is het noodzakelijk de diverse op het spel staande belangen en rechten met elkaar te verzoenen.

128. Het EHRM heeft namelijk geoordeeld dat de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten, met name impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging, hetgeen des te belangrijker is wanneer het lichamelijke en geestelijke welzijn van een kind wordt bedreigd. De bevoegde autoriteiten dienen daarbij echter de wettelijk voorgeschreven procedures en de overige waarborgen die de omvang van de strafrechtelijke onderzoeksbevoegdheden beperken, alsmede de overige vrijheden en rechten volledig in acht te nemen. Met name dient er volgens het EHRM een wettelijk kader te worden ingevoerd dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd, met elkaar te verzoenen (EHRM, 28 oktober 1998, *Osman t. Verenigd Koninkrijk*,

CE:ECHR:2003:1204JUD003927298, § 151; 24 juin 2004, Von Hannover c. Allemagne, CE:ECHR:2004:0624JUD005932000, §§ 57 et 58, ainsi que 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD000287202, §§ 46, 48 et 49).

129. En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est 'nécessaire, appropriée et proportionnée, au sein d'une société démocratique', au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être 'rigoureusement' proportionnée au but poursuivi.

130. À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, points 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 52; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

131. Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55 et jurisprudence citée).

132. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante

CE:ECHR:1998:1028JUD002345294, §§ 115 en 116; 4 maart 2004, *M.C. t. Bulgarij*e, CE:ECHR:2003:1204JUD003927298, § 151; 24 juni 2004, *Von Hannover t. Duitsland*, CE:ECHR:2004:0624JUD005932000, §§ 57 en 58, en 2 december 2008, *K.U. t. Finland*, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 en 49).

129. Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel 'strikt' evenredig moet zijn aan het nagestreefde doel.

130. In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140].

131. Meer bepaald volgt uit de rechtspraak van het Hof dat bij de beoordeling of de lidstaten een beperking van de omvang van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 bedoelde rechten en plichten kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 55 en aldaar aangehaalde rechtspraak).

132. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens

lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 117; avis 1/15(Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

133. Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 191 et jurisprudence citée, ainsi que arrêt du 3 octobre 2019, A e.a., C-70/18, EU:C:2019:823, point 63].

— Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité national.

134. Il y a lieu de faire observer que l'objectif de sauvegarde de la sécurité nationale, évoqué par les juridictions de renvoi et les gouvernements ayant présenté des observations, n'a pas encore été spécifiquement examiné par la Cour dans ses arrêts interprétant la directive 2002/58.

135. À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

136. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].

133. Een regeling die voorziet in de bewaring van persoonsgegevens, moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 191 en aldaar aangehaalde rechtspraak, en arrest van 3 oktober 2019, *A e.a.*, C-70/18, EU:C:2019:823, punt 63].

— Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid

134. Het Hof heeft zich in zijn arresten betreffende de uitlegging van richtlijn 2002/58 nog niet specifiek gebogen over de doelstelling van bescherming van de nationale veiligheid, waaraan is gerefereerd door de verwijzende rechters en de regeringen die opmerkingen hebben ingediend.

135. In dit verband moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten.

136. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van richtlijn 2002/58, met name de doelstellingen van bestrijding van - zelfs ernstige - criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich - zelfs ernstige - spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.

137. Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport.

138. L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.

139. Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale, telles que celles visées aux points 135 et 136 du présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues.

— Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique.

137. In situaties als die welke in de punten 135 en 136 van het onderhavige arrest zijn beschreven, verzet artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich derhalve in beginsel niet tegen een wettelijke maatregel op grond waarvan de bevoegde autoriteiten aan aanbieders van elektronischecommunicatiediensten een bevel kunnen opleggen om de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen gedurende een beperkte periode te bewaren, wanneer er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid als bedoeld in de punten 135 en 136 van het onderhavige arrest, en die bedreiging werkelijk en actueel of voorzienbaar is. Ook al heeft een dergelijke maatregel zonder onderscheid betrekking op alle gebruikers van elektronischecommunicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont.

138. Het bevel om preventief de gegevens te bewaren van alle gebruikers van elektronischecommunicatiemiddelen, mag echter slechts worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk. Het valt weliswaar niet uit te sluiten dat het aan aanbieders van elektronischecommunicatiemiddelen opgelegde bevel tot bewaring van die gegevens kan worden verlengd wegens het voortduren van een dergelijke bedreiging, maar dit neemt niet weg dat elk bevel slechts mag worden gegeven voor een voorzienbare periode. Een dergelijke gegevensbewaring moet bovendien zijn onderworpen aan beperkingen en zijn omgeven met strikte waarborgen die ervoor zorgen dat de persoonsgegevens van de betrokken personen doeltreffend worden beschermd tegen het risico van misbruik. Die bewaring mag derhalve geen stelselmatig karakter hebben.

139. Gelet op de ernst van de inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten die een dergelijke algemene en ongedifferentieerde bewaring van gegevens met zich brengt, dient te worden gewaarborgd dat de toepassing van die maatregel daadwerkelijk beperkt blijft tot situaties waarin de nationale veiligheid ernstig wordt bedreigd, zoals de in de punten 135 en 136 van het onderhavige arrest bedoelde situaties. Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronischecommunicatiediensten een bevel tot een dergelijke gegevensbewaring wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

— Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

140. Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général [voir, en ce sens, arrêts du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 102, ainsi que du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 56 et 57; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 149].

141. Une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 107).

142. En effet, compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 118 du présent arrêt, que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit, comme le prévoit le système mis en place par la directive 2002/58, l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître.

143. En outre, la Cour a souligné qu'une réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi. Une telle réglementation, contrairement à l'exigence rappelée au point 133 du présent arrêt, concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse

140. Als het gaat om de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, kunnen overeenkomstig het evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, zoals die welke voortvloeien uit de bewaring van verkeers- en locatiegegevens. De doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, kan derhalve enkel niet-ernstige inmengingen in die grondrechten rechtvaardigen [zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 102, en 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 56 en 57; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 149].

141. Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 107).

142. Gezien het gevoelige karakter van de informatie die verkeers- en locatiegegevens kunnen prijsgeven, is de vertrouwelijkheid van deze gegevens immers essentieel voor het recht op eerbiediging van het privéleven. Mede gelet op het in punt 118 van het onderhavige arrest bedoelde ontmoedigende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de in de artikelen 7 en 11 van het Handvest verankerde grondrechten, en op de ernst van de inmenging die een dergelijke bewaring met zich brengt, is het in een democratische samenleving dan ook van belang dat deze bewaring, zoals het bij richtlijn 2002/58 ingevoerde stelsel eist, de uitzondering en niet de regel vormt en dat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Deze conclusie geldt zelfs met betrekking tot de doelstellingen van bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen voor de openbare veiligheid en het belang dat aan deze doelstellingen moet worden toegekend.

143. Voorts heeft het Hof benadrukt dat een regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel. Een dergelijke regeling betreft algemeen alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat die personen zich - zelfs maar indirect - in een situatie bevinden die aanleiding kan zijn om strafvervolging in te stellen, wat in strijd is met het in punt 133 van het onderhavige arrest in herinnering gebrachte vereiste. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect

avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 57 et 58, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 105).

144. En particulier, comme l'a déjà jugé la Cour, une telle réglementation n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 59, et du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 106).

145. Or, même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé aux points 126 et 128 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi.

146. En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, *a fortiori*, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation.

147. Ainsi, comme l'a déjà jugé la Cour, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que

of van ver - verband houdt met die doelstelling van bestrijding van zware misdrijven, en vereist met name niet dat er een verband is tussen de te bewaren gegevens en een bedreiging voor de openbare veiligheid (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 105).

144. Zoals het Hof reeds heeft geoordeeld, beperkt een dergelijke regeling met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 59, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 106).

145. Zelfs de positieve verplichtingen die, naargelang van het geval, voor de lidstaten kunnen voortvloeien uit de artikelen 3, 4 en 7 van het Handvest en, zoals in de punten 126 en 128 van het onderhavige arrest is opgemerkt, betrekking hebben op de invoering van regels die een effectieve bestrijding van strafbare feiten mogelijk maken, kunnen geen inmengingen rechtvaardigen die zo ernstig zijn als de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van vrijwel de gehele bevolking die een regeling die voorziet in de bewaring van verkeers- en locatiegegevens met zich brengt, zonder dat de gegevens van de betrokken personen, althans indirect, een verband met het nagestreefde doel aan het licht kunnen brengen.

146. Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onderhavige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, *a fortiori*, bescherming van de nationale veiligheid - gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name het Grondwettelijk Hof heeft gerefereerd - de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt.

147. Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt

la durée de conservation retenue, limitée au strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 108).

148. S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 111).

149. À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.

150. La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.

151. Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.

— Sur les mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique.

152. Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées

(zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 108).

148. De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand van de categorieën betrokken personen, aangezien artikel 15, lid 1, van richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 111).

149. In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zij[n] die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.

150. Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 111). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.

151. Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

— Wettelijke maatregelen die voorzien in de preventieve bewaring van IP-adressen en gegevens inzake de burgerlijke identiteit ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

152. Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde

sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.

153. Toutefois, les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt.

154. Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause exigée par la jurisprudence citée au point 130 du présent arrêt, il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, comme l'ont indiqué plusieurs gouvernements dans leurs observations soumises à la Cour, s'avérer impossible sans avoir recours à une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58. Tel peut notamment être le cas, ainsi que l'ont fait valoir ces gouvernements, des infractions particulièrement graves en matière de pédopornographie, telles que l'acquisition, la diffusion, la transmission ou la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous c), de la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO 2011, L 335, p.1).

155. Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, au sens de la jurisprudence citée au point 133 du présent arrêt, avec les objectifs poursuivis et

communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.

153. Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben.

154. Om de op het spel staande rechten en belangen met elkaar te verzoenen, zoals de in punt 130 van het onderhavige arrest aangehaalde rechtspraak verlangt, moet echter in aanmerking worden genomen dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten na afloop van de periode waarvoor deze adressen werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat, zoals verschillende regeringen hebben aangevoerd in de door hen bij het Hof ingediende opmerkingen, het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel als bedoeld in artikel 15, lid 1, van richtlijn 2002/58. Zoals die regeringen hebben betoogd, kan dit met name het geval zijn bij zeer ernstige strafbare feiten op het gebied van kinderpornografie, zoals het online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie in de zin van artikel 2, onder *c),* van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (*PB* 2011, L 335, blz. 1).

155. In deze omstandigheden moet worden vastgesteld dat, ook al zou een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur die internettoegang mogelijk maakt, personen betreffen bij wie op het eerste gezicht een verband met de nagestreefde doelstellingen in de zin van de in punt 133 van het onderhavige arrest aangehaalde rechtspraak ontbreekt,

que les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.

156. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées.

157. En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 59 et 60).

158. Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 62).

159. Dans ces conditions, eu égard à la conciliation nécessaire des droits et des intérêts en cause et pour les raisons figurant aux points 131 et 158 du présent arrêt, il y a lieu de considérer que, même en l'absence de lien entre l'ensemble des utilisateurs des moyens de communications électroniques et les objectifs poursuivis, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi

en ook al moeten internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, een wettelijke maatregel die voorziet in de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen, in beginsel niet in strijd is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van die gegevens dienen te regelen.

156. Gelet op het feit dat die bewaring een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, kunnen enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid, die inmenging rechtvaardigen. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk is gelet op het nagestreefde doel. Tot slot moet een dergelijke maatregel voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de online communicatie en de online activiteiten van de betrokken personen.

157. Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als 'ernstig' worden aangemerkt (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 59 en 60).

158. Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van [de] richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 62).

159. Gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, moet in deze omstandigheden om de in de punten 131 en 158 van het onderhavige arrest uiteengezette redenen worden geoordeeld dat, ook al bestaat er geen verband tussen alle gebruikers van elektronischecommunicatiemiddelen en de nagestreefde doelstellingen, artikel 15, lid 1, van richtlijn 2002/58, gelezen in

que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à une mesure législative imposant, sans délai particulier, aux fournisseurs de services de communications électroniques la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs des moyens de communications électroniques aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique, sans qu'il soit nécessaire que les infractions pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves.

— Sur les mesures législatives prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de lutte contre la criminalité grave

160. En ce qui concerne les données relatives au trafic et les données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58, ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de celle-ci, telles que décrites aux points 134 à 159 du présent arrêt, il y a lieu de relever que ces données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant cette directive, leur traitement et leur stockage.

161. Toutefois, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée.

162. À cet égard, il y a lieu de relever que la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens – n° 185), laquelle a été signée par les 27 États membres et ratifiée par 25 d'entre eux, et dont l'objectif est de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques, prévoit, à son article 14, que les parties contractantes adoptent aux fins d'enquêtes ou de procédures pénales spécifiques certaines mesures quant aux données relatives au trafic déjà stockées, telles que la conservation rapide de ces données. En particulier, l'article 16, paragraphe 1, de cette convention stipule que les parties contractantes adoptent les mesures législatives qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide des données relatives au trafic stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

163. Dans une situation telle que celle visée au point 161 du présent arrêt, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts en cause

het licht van de artikelen 7, 8 en 11 en artikel 52, lid 2, van het Handvest, zich niet verzet tegen een wettelijke maatregel op grond waarvan aanbieders van elektronischecommunicatiediensten verplicht zijn om de gegevens inzake de burgerlijke identiteit van alle gebruikers van elektronischecommunicatiemiddelen gedurende een niet nader bepaalde periode te bewaren ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.

— Wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit

160. Met betrekking tot de verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen als beschreven in de punten 134 tot en met 159 van het onderhavige arrest, dient te worden opgemerkt dat deze gegevens in beginsel moeten worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen waarbinnen zij overeenkomstig de nationale bepalingen tot omzetting van die richtlijn moeten worden verwerkt en opgeslagen.

161. Gedurende die verwerking en opslag kunnen zich evenwel situaties voordoen die het noodzakelijk maken om de betrokken gegevens ook na het verstrijken van die termijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

162. In dit verband zij erop gewezen dat het op 23 november 2001 onder auspiciën van de Raad van Europa gesloten Cybercrimeverdrag (Serie Europese Verdragen - nr. 185), dat door alle 27 lidstaten is ondertekend en door 25 lidstaten is geratificeerd, en dat tot doel heeft de bestrijding van door middel van een computersysteem begane strafbare feiten te vergemakkelijken, in artikel 14 bepaalt dat de verdragsluitende partijen ten behoeve van specifieke strafrechtelijke onderzoeken of procedures bepaalde maatregelen moeten nemen met betrekking tot reeds opgeslagen verkeersgegevens, zoals de spoedbewaring van die gegevens. Met name is in artikel 16, lid 1, van dit verdrag bepaald dat de verdragsluitende partijen de wetgevende en andere maatregelen moeten nemen die nodig zijn om hun bevoegde autoriteiten in staat te stellen de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van verkeersgegevens die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat die gegevens vatbaar zijn voor verlies of wijziging.

163. In een situatie als bedoeld in punt 161 van het onderhavige arrest staat het de lidstaten, gelet op de in punt 130 van het onderhavige arrest genoemde noodzaak om de op het

visée au point 130 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent.

164. Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, *a fortiori*, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

165. À cet égard, il importe de préciser qu'une telle conservation rapide ne doit pas être limitée aux données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale. Tout en respectant le cadre dressé par l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, et compte tenu des considérations figurant au point 133 du présent arrêt, une telle mesure peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. En outre, l'accès des autorités compétentes aux données ainsi conservées doit s'effectuer dans le respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 (voir, en ce sens, arrêt du 21 décembre 2016, Téle2, C-203/15 et C-698/15, EU:C:2016:970, points 118 à 121 et jurisprudence citée).

spel staande rechten en belangen met elkaar te verzoenen, vrij om in een op grond van artikel 15, lid 1, van richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

164. Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen enkel de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

165. In dit verband moet worden gepreciseerd dat een dergelijke spoedbewaring niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht. Mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 133 van het onderhavige arrest, kan een dergelijke maatregel naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd. Bovendien moet aan de bevoegde autoriteiten toegang tot de aldus bewaarde gegevens worden verleend met inachtneming van de voorwaarden die voortvloeien uit de arresten waarin richtlijn 2002/58 is uitgelegd

166. Il convient encore d'ajouter que, ainsi qu'il ressort en particulier des points 115 et 133 du présent arrêt, l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, *a fortiori*, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale.

167. À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58".

En ce qui concerne les premières et deuxièmes questions préjudicielles posées par la Cour Constitutionnelle, la Cour de Justice a, dans le dispositif de l'arrêt, dit pour droit:

"L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives

(zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 118-121 en aldaar aangehaalde rechtspraak).

166. Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, *a fortiori*, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, [mits] de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167. In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/58."

Met betrekking tot de eerste en de tweede prejudiciële vraag die het Grondwettelijk Hof aan het Hof van Justitie voorgelegd had, heeft dat Hof in het *dictum* van dat arrest voor recht verklaard:

"Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, verzet zich daarentegen niet tegen wettelijke maatregelen

– permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

– permettant, aux fins de la lutte contre la criminalité grave et, *a fortiori*, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus. […]".

1.3.3. Concernant la troisième question préjudicielle posée par la Cour Constitutionnelle, la Cour de justice a dit pour droit:

– die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en

– die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik. […]"

1.3.3. Met betrekking tot de derde prejudiciële vraag van het Grondwettelijk Hof heeft het Hof van Justitie voor recht verklaard:

"Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits".

1.4. À la suite de l'arrêt *La Quadrature du Net* de la Cour de Justice, dans son arrêt n° 57/2021 du 22 avril 2021, la Cour constitutionnelle s'est prononcée sur les recours dirigés contre la loi du mai 2016.

1.4.1. Dans cet arrêt, la Cour cite tout d'abord deux autres décisions de la Cour de Justice, à savoir:

1° l'arrêt du 2 octobre 2018 en cause *Ministerio Fiscal* (C-207/16) (ci-après l'arrêt "*Ministerio Fiscal*"), dans lequel la Cour de Justice dit pour droit:

"L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la charte des droits fondamentaux, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave".

Dans cet arrêt, la Cour de Justice a motivé sa décision comme suit:

"Een nationale rechterlijke instantie mag geen bepaling van haar nationale recht toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten."

1.4. Naar aanleiding van arrest *La Quadrature du Net* van het Hof van Justitie heeft het Grondwettelijk Hof zich in zijn arrest nr. 57/2021 van 22 april 2021 uitgesproken over de beroepen die gericht waren tegen de wet van 29 mei 2016.

1.4.1. In dat arrest citeert het Grondwettelijk Hof eerst twee andere beslissingen van het Hof van Justitie, namelijk:

1° het arrest van 2 oktober 2018 in zake *Ministerio Fiscal* (C-207/16) (hierna het arrest *Ministerio Fiscal*), waarin het Hof van Justitie voor recht verklaard heeft:

"Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in samenhang met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang – op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit."

In dat arrest heeft het Hof van Justitie voor zijn beslissing op volgende overwegingen gesteund:

"*Sur le fond*

48. Par ses deux questions, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui présente une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave et, dans l'affirmative, à l'aune de quels critères la gravité de l'infraction en cause doit être appréciée.

49. À cet égard, il ressort de la décision de renvoi que, comme l'a relevé en substance M. l'avocat général au point 38 de ses conclusions, la demande de décision préjudicielle ne vise pas à déterminer si les données à caractère personnel en cause au principal ont été conservées par les fournisseurs de services de communications électroniques dans le respect des conditions visées à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte. Cette demande porte, ainsi qu'il ressort du point 46 du présent arrêt, uniquement sur la question de savoir si et dans quelle mesure l'objectif poursuivi par la réglementation en cause au principal est susceptible de justifier l'accès d'autorités publiques, telles que la police judiciaire, à de telles données, sans que les autres conditions d'accès résultant de cet article 15, paragraphe 1, fassent l'objet de cette demande.

50. En particulier, cette juridiction s'interroge sur les éléments à prendre en compte afin d'apprécier si les infractions au regard desquelles des autorités policières peuvent être autorisées, à des fins d'enquête, à accéder à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, sont d'une gravité suffisante pour justifier l'ingérence que comporte un tel accès dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, tels qu'interprétés par la Cour dans ses arrêts du 8 avril 2014*, Digital Rights Ireland e.a.* (C-293/12 et C-594/12, EU:C:2014:238), et *Télé2 Sverige et Watson e.a.*

51. Quant à l'existence d'une ingérence dans ces droits fondamentaux, il y a lieu de rappeler que, comme l'a relevé M. l'avocat général aux points 76 et 77 de ses conclusions, l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de 'grave' et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Un tel accès

"Ten gronde

48. Met zijn twee vragen, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - een zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van deze laatsten vormt dat die toegang, wat het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten betreft, zou moeten worden beperkt tot de bestrijding van zware criminaliteit en, zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld.

49. In dit verband blijkt uit de verwijzingsbeslissing dat, zoals de advocaat-generaal in punt 38 van zijn conclusie in wezen heeft opgemerkt, het verzoek om een prejudiciële beslissing er niet toe strekt om uit te maken of de aanbieders van elektronische-communicatiediensten de in het hoofdgeding aan de orde zijnde persoonsgegevens hebben bewaard met inachtneming van de voorwaarden van artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest. Zoals uit punt 46 van het onderhavige arrest blijkt, betreft het verzoek uitsluitend de vraag of en in welke mate het doel dat met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan rechtvaardigen dat overheidsinstanties zoals de gerechtelijke politie toegang hebben tot dergelijke gegevens, en gaat het verzoek niet over de andere toegangsvoorwaarden die uit voormeld artikel 15, lid 1, voortvloeien.

50. De verwijzende rechter vraagt zich in het bijzonder af welke elementen in aanmerking moeten worden genomen bij de beoordeling of delicten waarvoor politiediensten in het kader van een onderzoek toegang kan worden verleend tot persoonsgegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, voldoende ernstig zijn om de inmenging die een dergelijke toegang betekent in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uitgelegd door het Hof in zijn arrest van 8 april 2014, Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2014:238), en in het arrest Tele2 Sverige en Watson e.a., te rechtvaardigen.

51. Wat betreft de vraag of sprake is van inmenging in die grondrechten, zij eraan herinnerd dat, zoals de advocaat-generaal in de punten 76 en 77 van zijn conclusie heeft aangegeven, de toegang van overheidsinstanties tot dergelijke gegevens inmenging in het in artikel 7 van het Handvest neergelegde grondrecht op eerbiediging van het privéleven vormt, zelfs al kan die inmenging om bepaalde redenen niet als 'ernstig' worden aangemerkt en zonder dat van belang is of de informatie over het privéleven al dan niet gevoelig is en of de betrokkenen door die inmenging enig nadeel hebben ondervonden. Een dergelijke toegang vormt tevens inmenging

constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée].

52. En ce qui concerne les objectifs susceptibles de justifier une réglementation nationale, telle que celle en cause au principal, régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, il convient de rappeler que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt *Télé2 Sverige et Watson e.a.*, points 90 et 115).

53. Or, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, il y a lieu d'observer que le libellé de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les 'infractions pénales' en général.

54. À cet égard, la Cour a, certes, jugé que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées (voir, en ce sens, arrêt *Télé2 Sverige et Watson e.a.*, point 99).

55. La Cour a toutefois motivé cette interprétation par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne (voir, en ce sens, arrêt *Télé2 Sverige et Watson e.a.*, point 115).

56. En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de 'grave'.

57. En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d''infractions pénales' en général.

58. Il convient donc, avant tout, de déterminer si, en l'occurrence, en fonction des circonstances de l'espèce, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire aux données en

in het door artikel 8 van het Handvest gewaarborgde grondrecht op bescherming van persoonsgegevens, aangezien die toegang een verwerking van persoonsgegevens is [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak].

52. Wat betreft de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling als die in het hoofdgeding, die de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt en die aldus afwijkt van het beginsel van de vertrouwelijkheid van elektronische communicatie, zij eraan herinnerd dat de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gegeven opsomming van doelstellingen exhaustief is, zodat die toegang daadwerkelijk en strikt op een van die doelstellingen moet berusten (zie in die zin arrest Tele2 Sverige en Watson e.a., punten 90 en 115).

53. Aangaande de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, dient te worden geconstateerd dat het daarbij volgens de bewoordingen van artikel 15, lid 1, eerste zin, van richtlijn 2002/58 evenwel niet alleen over de bestrijding van ernstige delicten maar over 'strafbare feiten' in het algemeen gaat[.]

54. Stellig heeft het Hof in dit verband geoordeeld dat ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens waaruit, in hun geheel beschouwd, precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen (zie in die zin arrest Tele2 Sverige en Watson e.a., punt 99).

55. Het Hof heeft die uitlegging echter gemotiveerd met de overweging dat de met een toegangsregeling nagestreefde doelstelling in verhouding moet staan tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt (zie in die zin arrest Tele2 Sverige en Watson e.a., punt 115).

56. Volgens het evenredigheidsbeginsel kan ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, ernstige inmenging immers slechts worden gerechtvaardigd door de doelstelling om - eveneens 'ernstige' - criminaliteit te bestrijden.

57. Is de inmenging die een dergelijke toegang veroorzaakt daarentegen niet ernstig, dan kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van 'strafbare feiten' in het algemeen.

58. Allereerst moet dus worden uitgemaakt of in casu, gelet op de omstandigheden van de onderhavige zaak, de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die zou voortvloeien uit het feit

cause au principal comporterait doit être considérée comme étant ‘grave’.

59. À cet égard, la demande en cause au principal par laquelle la police judiciaire sollicite, pour les besoins d’une enquête pénale, l’autorisation judiciaire d’accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d’identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. Ainsi qu’il a été relevé au point 40 du présent arrêt, cette demande vise l’accès aux seuls numéros de téléphone correspondant à ces cartes SIM ainsi qu’aux données relatives à l’identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne portent pas, comme l’ont confirmé tant le gouvernement espagnol que le ministère public lors de l’audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.

60. Il apparaît donc que les données visées par la demande d’accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l’identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l’heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.

61. Dans ces conditions, l’accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d’ingérence ‘grave’ dans les droits fondamentaux des personnes dont les données sont concernées.

62. Ainsi qu’il ressort des points 53 à 57 du présent arrêt, l’ingérence que comporterait un accès à de telles données est donc susceptible d’être justifiée par l’objectif de prévention, de recherche, de détection et de poursuite d’’infractions pénales’ en général, auquel se réfère l’article 15, paragraphe 1, première phrase, de la directive 2002/58, sans qu’il soit nécessaire que ces infractions soient qualifiées de ‘graves’.

63. Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que l’article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l’accès d’autorités publiques aux données visant à l’identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès

dat aan de gerechtelijke politie toegang tot de in het hoofdgeding aan de orde zijnde gegevens wordt verleend, als ‘ernstig’ moet worden beschouwd.

59. In dit verband heeft het verzoek in het hoofdgeding, waarmee de gerechtelijke politie in een strafrechtelijk onderzoek via rechterlijke toestemming toegang wil verkrijgen tot door aanbieders van elektronischecommunicatiediensten bewaarde persoonsgegevens, louter tot doel de houders te identificeren van de simkaarten die gedurende een periode van twaalf dagen met het IMEI-nummer van de gestolen mobiele telefoon zijn geactiveerd. Zoals in punt 40 van het onderhavige arrest is uiteengezet, strekt dat verzoek er enkel toe om toegang te verkrijgen tot de telefoonnummers die overeenstemmen met die simkaarten en tot de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. Zoals zowel de Spaanse regering als het openbaar ministerie ter terechtzitting heeft bevestigd, gaat het daarbij echter niet over de communicatie die met de gestolen mobiele telefoon tot stand is gebracht of over de locatie van die telefoon.

60. Met de via het toegangsverzoek in het hoofdgeding beoogde gegevens is het dus blijkbaar alleen mogelijk om, gedurende een bepaalde periode, de met de gestolen mobiele telefoon geactiveerde simkaart(en) in verband te brengen met de civiele identiteit van de houders van die simkaarten. Zonder aanvullende gegevens over de communicatie die met die simkaarten tot stand is gebracht en over de locatie, kan met die gegevens noch de datum, het uur, de duur of de ontvanger van de met de betrokken simkaart(en) verrichte oproepen worden achterhaald, noch waar die communicatie heeft plaatsgevonden of hoe vaak in een gegeven periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken.

61. In die omstandigheden kan de toegang tot de in het verzoek in het hoofdgeding bedoelde gegevens niet worden aangemerkt als een ‘ernstige’ inmenging in de grondrechten van de personen waarop de gegevens betrekking hebben.

62. Zoals uit de punten 53 tot en met 57 van dit arrest blijkt, kan de inmenging die een dergelijke gegevenstoegang zou veroorzaken dus worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 vermelde doelstelling om ‘strafbare feiten’ in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, zonder dat deze strafbare feiten als ‘ernstig’ moeten worden aangemerkt.

63. Gelet op het voorgaande dient op de gestelde vragen te worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang - op het gebied van het voorkomen,

devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave".

2° L'arrêt du 6 octobre 2020, en cause *Privacy International* (C-623/17) (ci-après l'arrêt "*Privacy International*"), prononcé en grande chambre, dans lequel la Cour de justice dit pour droit:

"L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement".

Cet arrêt repose sur la motivation suivante:

"*Sur la seconde question*

50. Par sa seconde question, la juridiction de renvoi cherche, en substance, à savoir si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

51. À titre liminaire, il convient de rappeler que, selon les indications figurant dans la demande de décision préjudicielle, l'article 94 de la loi de 1984 autorise le ministre à imposer aux fournisseurs de services de communications électroniques, par voie d'instructions, lorsqu'il l'estime nécessaire dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger, de transmettre aux services de sécurité et de renseignement les données relatives aux communications en masse, ces données incluant les données relatives au trafic et les données de localisation ainsi que des informations sur les services utilisés, au sens de l'article 21, paragraphes 4 et 6, de la RIPA. Cette dernière disposition couvre, entre autres, les données nécessaires pour identifier la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, le numéro de téléphone de l'appelant et le numéro appelé, les adresses IP de la source et du destinataire de la communication ainsi que les adresses des sites Internet visités.

2° Het arrest van 6 oktober 2020 in zake *Privacy International* (C-623/17), (hierna het arrest *Privacy International*), uitgesproken in grote kamer, waarin het Hof van Justitie voor recht verklaard heeft:

"Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen."

Dat arrest steunt op volgende overwegingen:

"Tweede vraag

50. Met zijn tweede vraag wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

51. Om te beginnen zij eraan herinnerd dat section 94 van de wet van 1984 volgens de informatie in het verzoek om een prejudiciële beslissing de Secretary of State de mogelijkheid biedt om aanbieders van elektronischecommunicatiediensten door middel van aanwijzingen de verplichting op te leggen om bulkcommunicatiegegevens door te zenden aan de veiligheids- en inlichtingendiensten, indien hij dit noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met een buitenlandse regering. Deze gegevens omvatten verkeers- en locatiegegevens alsmede informatie over de gebruikte diensten, in de zin van section 21, leden 4 en 6, RIPA. Deze laatste bepaling ziet onder meer op de gegevens die nodig zijn om de bron en de bestemming van een communicatie te identificeren, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte materiaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren met name de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, het bron- en het doel-IP-adres en de adressen van de bezochte websites.

52. Une telle communication par transmission des données concerne l'ensemble des utilisateurs des moyens de communications électroniques, sans qu'il soit précisé si cette transmission doit intervenir en temps réel ou de manière différée. Une fois transmises, ces données sont, selon les indications figurant dans la demande de décision préjudicielle, conservées par les services de sécurité et de renseignement et demeurent à la disposition de ces derniers aux fins de leurs activités, à l'instar des autres bases de données que ces services détiennent. En particulier, les données ainsi recueillies, qui sont soumises à des traitements et à des analyses de masse et automatisés, peuvent être recoupées avec d'autres bases de données comportant différentes catégories de données à caractère personnel en masse ou être divulguées hors de ces services et à des États tiers. Enfin, ces opérations ne sont pas subordonnées à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante et ne donnent lieu à aucune information des personnes concernées.

53. La directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM(2000)385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu 'faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée'.

54. À cet effet, l'article 5, paragraphe 1, de la directive 2002/58 dispose que 'les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes'. Cette même disposition souligne également que, '[e]n particulier, [les États membres] interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1', et précise que '[ce] paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité'.

55. Ainsi, cet article 5, paragraphe 1, consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne

52. Een dergelijke verstrekking van gegevens door middel van doorzending betreft alle gebruikers van elektronischecommunicatiemiddelen, zonder dat wordt gespecificeerd of die doorzending wel of niet in real time moet plaatsvinden. De doorgezonden gegevens worden volgens de informatie in het verzoek om een prejudiciële beslissing door de veiligheids- en inlichtingendiensten bewaard en blijven ter beschikking van deze diensten ten behoeve van hun activiteiten, net zoals de andere databases van deze diensten. Met name kunnen de aldus verworven gegevens, waarop automatische bulkverwerking en -analyse worden toegepast, worden onderworpen aan kruiscontroles met andere databases die verschillende categorieën bulkpersoonsgegevens bevatten, of buiten die diensten worden bekendgemaakt, ook aan derde staten. Tot slot is voor die bewerkingen geen voorafgaande toestemming van een rechterlijke instantie of een onafhankelijk bestuursorgaan vereist en geldt er geen verplichting om de betrokkenen te informeren.

53. Zoals met name uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen 'zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie'.

54. Daartoe bepaalt artikel 5, lid 1, van richtlijn 2002/58 dat '[d]e lidstaten […] via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten [garanderen]'. In diezelfde bepaling wordt benadrukt dat de lidstaten 'met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers [verbieden], indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1,' en gepreciseerd dat '[d]it lid […] de technische opslag die nodig is voor het overbrengen van informatie onverlet [laat], onverminderd het vertrouwelijkheidsbeginsel'.

55. Artikel 5, lid 1, legt aldus het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert met name dat het anderen dan de gebruikers in beginsel moet

autre que les utilisateurs, de stocker, sans le consentement de ceux-ci, ces communications et ces données. Eu égard au caractère général de son libellé, cette disposition couvre nécessairement toute opération permettant à des tiers de prendre connaissance des communications et des données y afférentes à des fins autres que l'acheminement d'une communication.

56. L'interdiction d'intercepter les communications et les données y afférentes figurant à l'article 5, paragraphe 1, de la directive 2002/58 englobe donc toute forme de mise à disposition par les fournisseurs de services de communications électroniques de données relatives au trafic et de données de localisation à des autorités publiques, tels des services de sécurité et de renseignement, ainsi que la conservation desdites données par ces autorités, quelle que soit l'utilisation ultérieure qui est faite de celles-ci.

57. Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 109).

58. Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par l'un de ces motifs.

59. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêts du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 111).

60. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes

worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd. Gelet op haar algemene bewoordingen, bestrijkt die bepaling noodzakelijkerwijs elke voor andere doeleinden dan het overbrengen van informatie uitgevoerde bewerking die derden in staat stelt om kennis te nemen van de communicatie en de daarmee verband houdende gegevens.

56. Het in artikel 5, lid 1, van richtlijn 2002/58 neergelegde verbod op het onderscheppen van de communicatie en de daarmee verband houdende verkeersgegevens omvat dus elke vorm van beschikbaarstelling door aanbieders van elektronischecommunicatiediensten van verkeers- en locatiegegevens aan overheidsinstanties, zoals veiligheids- en inlichtingendiensten, alsmede de bewaring van de beschikbaar gestelde gegevens door die instanties, ongeacht het latere gebruik van die gegevens.

57. Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 109).

58. Artikel 15, lid 1, van richtlijn […] 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

59. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arresten van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104, en 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 111).

60. Bovendien volgt uit artikel 15, lid 1, derde zin, van richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn

généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement, à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

61. Ces mêmes questions se posent également pour d'autres types de traitement de données, tels que leur transmission à des personnes autres que les utilisateurs ou l'accès à ces données en vue de leur utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 122 et 123 ainsi que jurisprudence citée].

62. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99 P, EU:C:2001:127, point 39, et du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

63. Toutefois, les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

64. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

65. Il convient d'ajouter que l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet

met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

61. Diezelfde vragen rijzen ook voor andere vormen van gegevensverwerking, zoals de doorzending van gegevens aan anderen dan de gebruikers of de toegang tot die gegevens met het oog op het gebruik ervan [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 122 en 123 en aldaar aangehaalde rechtspraak].

62. Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, Connolly/Commissie, C-274/99 P, EU:C:2001:127, punt 39, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 93 en aldaar aangehaalde rechtspraak).

63. De in de artikelen 7, 8 en 11 van het Handvest verankerde rechten hebben echter geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).

64. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

65. Hieraan dient te worden toegevoegd dat het vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging

l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné (arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 175 ainsi que jurisprudence citée).

66. En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est 'nécessaire, appropriée et proportionnée, au sein d'une société démocratique', au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être 'rigoureusement' proportionnée au but poursuivi.

67. À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre l'objectif et les intérêts et droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, points 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 52; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

68. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 117; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 175 en aldaar aangehaalde rechtspraak).

66. Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel 'strikt' evenredig moet zijn aan het nagestreefde doel.

67. In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, Satakunnan Markkinapörssi en Satamedia, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, Volker und Markus Schecke en Eifert, C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140].

68. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].

69. S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause au principal, satisfait aux exigences de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, il convient de relever que la transmission des données relatives au trafic et des données de localisation à des personnes autres que les utilisateurs, telles que des services de sécurité et de renseignement, déroge au principe de confidentialité. Dès lors que cette opération est effectuée, comme en l'occurrence, de manière généralisée et indifférenciée, elle a pour effet de faire de la dérogation à l'obligation de principe de garantir la confidentialité des données la règle, alors que le système mis en place par la directive 2002/58 exige qu'une telle dérogation demeure l'exception.

70. En outre, conformément à la jurisprudence constante de la Cour, la transmission des données relatives au trafic et des données de localisation à un tiers constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure qui est faite de ces données. À cet égard, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée, et arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, points 115 et 116].

71. L'ingérence que comporte la transmission des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement dans le droit consacré à l'article 7 de la Charte doit être considérée comme étant particulièrement grave, compte tenu notamment du caractère sensible des informations que peuvent fournir ces données et, notamment, de la possibilité d'établir à partir de celles-ci le profil des personnes concernées, une telle information étant tout aussi sensible que le contenu même des communications. En outre, elle est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 27 et 37, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 99 et 100).

72. Il convient de relever encore qu'une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE)2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En

69. Wat de vraag betreft of een nationale regeling als die van het hoofdgeding voldoet aan de vereisten van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, dient te worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan anderen dan de gebruikers, zoals de veiligheids- en inlichtingendiensten, afwijkt van het vertrouwelijkheidsbeginsel. Wanneer die bewerking, zoals in casu, op algemene en ongedifferentieerde wijze wordt uitgevoerd, heeft zij tot gevolg dat de afwijking van de principeverplichting tot waarborging van de vertrouwelijkheid van de gegevens de regel wordt, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat die afwijking de uitzondering blijft.

70. Voorts vormt de doorzending van verkeers- en locatiegegevens aan een derde volgens vaste rechtspraak van het Hof een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. In dit verband is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak, en arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punten 115 en 116].

71. De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 27 en 37, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 99 en 100).

72. Tevens moet worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan overheidsinstanties voor veiligheidsdoeleinden op zichzelf afbreuk kan doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie, en de gebruikers van elektronischecommunicatiemiddelen kan ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen. Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde

outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 28; du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 101, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 118).

73. Enfin, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

74. S'agissant des objectifs susceptibles de justifier de telles ingérences, plus particulièrement de l'objectif de sauvegarde de la sécurité nationale, en cause au principal, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 135).

75. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, mêmes graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 136).

76. Toutefois, pour satisfaire à l'exigence de proportionnalité rappelée au point 67 du présent arrêt, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, une réglementation nationale comportant une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte doit respecter les

gegevens talrijk en gevarieerd zijn (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 28; 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 101, en 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 118).

73. Ten slotte is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

74. Wat de doelstellingen betreft die dergelijke inmengingen kunnen rechtvaardigen, meer in het bijzonder de in het hoofdgeding aan de orde zijnde doelstelling van bescherming van de nationale veiligheid, moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 135).

75. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van richtlijn 2002/58, met name de doelstellingen van bestrijding van - zelfs ernstige - criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich - zelfs ernstige - spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 136).

76. Om te voldoen aan het in punt 67 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, dient een nationale regeling die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, evenwel in

exigences résultant de la jurisprudence citée aux points 65, 67 et 68 du présent arrêt.

77. En particulier, s'agissant de l'accès d'une autorité à des données à caractère personnel, une réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 192 et jurisprudence citée].

78. Ainsi, et dès lors qu'un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, une réglementation nationale régissant l'accès aux données relatives au trafic et aux données de localisation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause (voir, en ce sens, arrêt du 21 décembre 2016, Téléd2, C-203/15 et C-698/15, EU:C:2016:970, point 119 et jurisprudence citée).

79. Ces exigences s'appliquent, *a fortiori*, à une mesure législative, telle que celle en cause au principal, sur le fondement de laquelle l'autorité nationale compétente peut imposer aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement. En effet, une telle transmission a pour effet de mettre ces données à la disposition des autorités publiques [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 212].

80. Dès lors que la transmission des données relatives au trafic et des données de localisation a lieu de manière généralisée et indifférenciée, elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement pourrait avoir un lien, même indirect ou lointain, avec l'objectif de sauvegarde de la sécurité nationale et, en particulier, sans que soit établie une relation entre les données dont la transmission est prévue et une menace pour la sécurité nationale (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 57 et 58, ainsi que du 21 décembre 2016, Téléd2, C-203/15 et C-698/15, EU:C:2016:970, point 105). Eu égard au fait que la transmission de telles données aux autorités publiques équivaut, conformément à ce qui a été constaté au point 79 du présent arrêt, à un accès, il convient de considérer qu'une réglementation permettant une transmission généralisée et indifférenciée des données aux autorités publiques, implique un accès général.

81. Il en résulte qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic

overeenstemming te zijn met de eisen die voortvloeien uit de in de punten 65, 67 en 68 van het onderhavige arrest aangehaalde rechtspraak.

77. Wat in het bijzonder de toegang van een autoriteit tot persoonsgegevens betreft, mag een regeling zich niet ertoe beperken te eisen dat de toegang tot deze gegevens wordt verleend voor het met die regeling beoogde doel, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 192 en aldaar aangehaalde rechtspraak].

78. Een nationale regeling die de toegang tot locatie- en verkeersgegevens regelt, moet dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de betrokken gegevens moet worden verleend, aangezien een algemene toegang tot alle bewaarde gegevens, los van enig - zelfs maar indirect - verband met het nagestreefde doel, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 119 en aldaar aangehaalde rechtspraak).

79. Die vereisten zijn *a fortiori* van toepassing op een wettelijke maatregel als aan de orde in het hoofdgeding, op grond waarvan de bevoegde nationale autoriteit aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Een dergelijke doorzending heeft immers tot gevolg dat die gegevens ter beschikking worden gesteld aan overheidsinstanties [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 212].

80. Het feit dat de doorzending van de verkeers- en locatiegegevens geschiedt op algemene en ongedifferentieerde wijze, betekent dat die doorzending algemeen alle personen betreft die gebruikmaken van elektronischecommunicatiediensten, dat wil zeggen zelfs personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - een verband vertoont met de doelstelling van bescherming van de nationale veiligheid. Met name is er geen enkel verband vereist tussen de gegevens die moeten worden doorgezonden en een bedreiging van de nationale veiligheid (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 105). Gelet op het feit dat de doorzending van dergelijke gegevens aan overheidsinstanties - overeenkomstig de vaststelling in punt 79 van het onderhavige arrest - gelijkstaat aan het verlenen van toegang tot deze gegevens, moet worden geoordeeld dat een regeling die de algemene en ongedifferentieerde doorzending van gegevens aan overheidsinstanties mogelijk maakt, een algemene toegang tot die gegevens impliceert.

81. Daaruit volgt dat een nationale regeling die aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten

et des données de localisation aux services de sécurité et de renseignement, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte.

82. Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la seconde question que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement".

1.4.2. Après avoir cité ces deux décisions de la Cour de Justice, la Cour constitutionnelle énonce la motivation et le dispositif de l'arrêt *La Quadrature du Net* de la Cour de Justice, répondant aux questions préjudicielles posées par son arrêt n° 96/2018.

Elle motive ensuite sa décision comme suit:

"B.15. Il ressort de l'arrêt de la Cour de justice du 6 octobre 2020 en cause. *La Quadrature du Net et autres*, précité, que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, sauf dans les hypothèses limitées décrites par l'arrêt précité.

En ce qu'elle prévoit, par principe et sans limitation à ces hypothèses, une conservation généralisée et indifférenciée, par les opérateurs et fournisseurs de services de communications électroniques, des données d'identification, des données d'accès et de connexion, ainsi que des données de communication, visées à l'article 126, § 3, de la loi du 13 juin 2005, la loi attaquée viole par conséquent l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des dispositions précitées de la Charte des droits fondamentaux de l'Union européenne, et en combinaison avec les articles 10 et 11 de la Constitution.

B.16.1. Dans le dispositif de l'arrêt du 6 octobre 2020 en cause *La Quadrature du Net et autres*, précité, la Cour de justice précise cependant que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, ne s'oppose pas à divers types de mesures législatives que la Cour énumère.

oplegt, verder gaat dan strikt noodzakelijk is en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist.

82. Gelet op een en ander moet op de tweede vraag worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen."

1.4.2. Na die twee beslissingen van het Hof van Justitie aangehaald te hebben, geeft het Grondwettelijk Hof de motivering en het dictum weer van het arrest *La Quadrature du Net* van het Hof van Justitie, in antwoord op de in zijn arrest nr. 96/2018 gestelde prejudiciële vragen.

Vervolgens motiveert het Grondwettelijk Hof zijn beslissing als volgt:

"B.15. Uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.,* blijkt dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, § 1, genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in de in het voormelde arrest beschreven beperkte gevallen.

In zoverre zij principieel en zonder beperking tot die gevallen voorziet in een algemene en ongedifferentieerde bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de identificatiegegevens, de toegangs- en verbindingsgegevens, alsook van de communicatiegegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, schendt de bestreden wet bijgevolg artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest van de grondrechten van de Europese Unie, en in samenhang met de artikelen 10 en 11 van de Grondwet.

B.16.1. In het dictum van het voormelde arrest van 6 oktober 2020, in zake *La Quadrature du Net e.a.,* preciseert het Hof van Justitie echter dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn

Sont ainsi admissibles, notamment, des mesures législatives ‘prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d’une connexion, pour une période temporellement limitée au strict nécessaire’, ou encore des mesures législatives ‘prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l’identité civile des utilisateurs de moyens de communications électroniques’. Ces mesures législatives doivent assurer, ‘par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d’abus’.

B.16.2. Sur la base de ces précisions de la Cour de justice, le Conseil des ministres soutient dans ses mémoires complémentaires qu’en tout état de cause, la loi attaquée ne doit pas être annulée en ce qu’elle prévoit l’obligation généralisée et indifférenciée de conservation, par les opérateurs et fournisseurs de services de communications électroniques, des adresses IP attribuées à la source d’une connexion, d’une part, et des données relatives à l’identité civile des utilisateurs de moyens de communications électroniques, d’autre part.

Le Conseil des ministres en conclut que seuls doivent être annulés, le cas échéant, les alinéas 2 et 3 de l’article 126, § 3, de la loi du 13 juin 2005, qui visent respectivement les données de connexion et de localisation et les données de communication. Il estime que l’alinéa 1er de l’article 126, § 3, précité, qui vise les données d’identification, ne doit en revanche pas être annulé, pas plus que les autres dispositions de la loi attaquée, dès lors qu’elles contiennent les garanties nécessaires en termes de conservation des données et d’accès à celles-ci.

B.17. En l’espèce, il y a lieu de constater que la loi attaquée repose, dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l’ensemble des données visées à l’article 126, § 3, de la loi du 13 juin 2005, et qu’elle poursuit, d’une manière générale, comme il est dit en B.3 et en B.4, des objectifs plus larges que la lutte contre la criminalité grave ou le risque d’atteinte à la sécurité publique.

La distinction que l’article 126, § 3, de la loi du 13 juin 2005 opère entre trois catégories de données (à savoir: les données d’identification, les données d’accès et de connexion, ainsi que les données de communication) n’a d’incidence que sur le point de départ de la durée de conservation des données, de douze mois en toute hypothèse, et éventuellement sur les possibilités d’accéder à celles-ci, pour les instances habilitées (voy. l’article 46*bis* du Code d’instruction criminelle et l’article 126, § 2, de la loi du 13 juin 2005). Cette catégorisation ne correspond par ailleurs pas aux distinctions qui sont opérées par la Cour de justice dans son arrêt du 6 octobre 2020 en ce qui concerne les différentes catégories de données susceptibles

aldus, met name, wettelijke maatregelen ‘die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk’, of nog wettelijke maatregelen ‘die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen’. Die wettelijke maatregelen moeten, ‘door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik’.

B.16.2. Op grond van die preciseringen van het Hof van Justitie betoogt de Ministerraad in zijn aanvullende memories dat de bestreden wet in elk geval niet dient te worden vernietigd in zoverre zij voorziet in de algemene en ongedifferentieerde verplichting tot bewaring, door de operatoren en aanbieders van elektronischecommunicatiediensten, van de IP-adressen die zijn toegewezen aan de bron van een verbinding, enerzijds, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, anderzijds.

De Ministerraad besluit daaruit dat, in voorkomend geval, enkel het tweede en het derde lid van artikel 126, § 3, van de wet van 13 juni2005 dienen te worden vernietigd, waarin respectievelijk de verbindings- en locatiegegevens en de communicatiegegevens worden beoogd. Hij is van mening dat het eerste lid van het voormelde artikel 126, § 3, waarin de identificatiegegevens worden beoogd, daarentegen niet dient te worden vernietigd, net zomin als de andere bepalingen van de bestreden wet, aangezien zij de nodige waarborgen bevatten op het vlak van bewaring van en toegang tot de gegevens.

B.17. Te dezen dient te worden vastgesteld dat de bestreden wet, wat het beginsel zelf ervan betreft, berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen, zoals in B.3 en B.4 is vermeld, ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid.

Het onderscheid dat bij artikel 126, § 3, van de wet van 13 juni2005 wordt gemaakt tussen drie categorieën van gegevens (te weten: identificatiegegevens, toegangs- en verbindingsgegevens, alsook communicatiegegevens) heeft slechts een weerslag op het startpunt van de bewaringstermijn van de gegevens - in elk geval twaalf maanden -, en eventueel op de mogelijkheden voor de gemachtigde instanties om toegang tot die gegevens te hebben (zie artikel 46*bis* van het Wetboek van strafvordering en artikel 126, § 2, van de wet van 13 juni 2005). Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie in zijn arrest van 6 oktober 2020 wordt gemaakt voor wat betreft

de faire l'objet d'une obligation de conservation généralisée et indifférenciée, moyennant le respect de plusieurs conditions (à savoir, en l'occurrence: les adresses IP attribuées à la source d'une connexion et les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques).

B.18. L'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué: l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours 'répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi' (points 132 et 133).

B.19. Il appartient au législateur d'élaborer une réglementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatibles avec l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. En particulier, il appartient également au législateur, dans ce contexte, d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire.

B.20. Compte tenu de ce qui précède, il y a lieu d'annuler les articles 2, b), 3 à 11 et 14 de la loi attaquée, qui sont indissociablement liés".

Pour ces motifs, la Cour constitutionnelle, dans son arrêt n° 57/2021 du 22 avril 2021 décide d'annuler, sans en maintenir les effets pour une période déterminée, les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016. Elle rejette le recours pour le surplus.

1.5. L'avant-projet à l'examen se donne pour objet de faire suite à cet arrêt de la Cour constitutionnelle du 22 avril 2021, ainsi qu'à la jurisprudence de la Cour de Justice qui fonde cet arrêt, spécialement l'arrêt *La Quadrature du Net*.

2. Compte-tenu de ce qui précède, l'avant-projet doit être plus spécialement examiné au regard de l'article 15 de la directive 2002/58/CE du Parlement et du Conseil du 12 juillet 2002 qui dispose comme suit:

"Application de certaines dispositions de la directive 95/46/CE

de verschillende categorieën van gegevens die het voorwerp kunnen uitmaken van een verplichting tot algemene en ongedifferentieerde bewaring, mits verscheidene voorwaarden in acht worden genomen (te weten, te dezen: de IP-adressen die zijn toegewezen aan de bron van een verbinding en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen).

B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt: de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds 'beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel' (punten 132 en 133).

B.19. Het staat aan de wetgever een regeling tot stand te brengen waarbij de beginselen in acht worden genomen die van toepassing zijn inzake bescherming van persoonsgegevens, in het licht van de rechtspraak van het Hof van Justitie, en, in voorkomend geval, rekening te houden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die verenigbaar worden geacht met artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. In het bijzonder staat het, in die context, ook aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

B.20. Rekening houdend met hetgeen voorafgaat, dienen de artikelen 2, b), 3 tot 11 en 14 van de bestreden wet, die onlosmakelijk met elkaar verbonden zijn, te worden vernietigd."

Om die redenen beslist het Grondwettelijk Hof in zijn arrest nr. 57/2021 van 22 april 2021 de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 te vernietigen zonder de gevolgen ervan gedurende een bepaalde periode te handhaven. Voor het overige verwerpt het Hof het beroep.

1.5. Het voorliggende voorontwerp strekt ertoe gevolg te geven aan dat arrest van het Grondwettelijk Hof van 22 april 2021 evenals aan de rechtspraak van het Hof van Justitie waarop dat arrest gebaseerd is, meer bepaald het arrest *La Quadrature du Net*.

2. Gelet op wat voorafgaat, moet het voorontwerp meer in het bijzonder onderzocht worden in het licht van artikel 15 van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 dat als volgt luidt:

"Toepassing van een aantal bepalingen van richtlijn 95/46/EG

1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

1*bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication[8] aux fins visées à l'article 1er, paragraphe 1, de ladite directive.

1*ter*. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse.

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques".

3. Concernant le droit interne, dès lors que les dispositions de la loi du 29 mai 2016, et avant celles-ci, les dispositions de la loi du 30 juillet 2013, ont été annulées, elles sont censées ne jamais avoir existé et les dispositions abrogées ou modifiées par ces lois redeviennent applicables telles quelles sont en

1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

1*bis*. Lid 1 is niet van toepassing op de uit hoofde van richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken[8] te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden.

1*ter*. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.

2. Het bepaalde in hoofdstuk III van richtlijn 95/46/EG inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

3. De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, ingesteld bij artikel 29 van richtlijn 95/46/EG, voert de in artikel 30 van die richtlijn vermelde taken ook uit ten aanzien van aangelegenheden die onder de onderhavige richtlijn vallen, namelijk de bescherming van de fundamentele rechten en vrijheden en van rechtmatige belangen in de sector elektronische communicatie."

3. Aangezien de bepalingen van de wet van 29 mei 2016 en daarvóór de bepalingen van de wet van 30 juli 2013 vernietigd zijn, worden ze, wat het interne recht betreft, geacht nooit te hebben bestaan en worden de bepalingen die bij die wetten zijn opgeheven of gewijzigd opnieuw toepasselijk zoals ze

[8] *Note de bas de page 1 de la directive citée:* JO L 105 du 13.4 2006, p. 54.

[8] *Voetnoot 1 van de geciteerde richtlijn:* PB L 105 van 13.4 2006, blz. 54.

vigueur, sans avoir égard aux modifications apportées par les deux lois précitées.

4. C'est dans ce contexte que les auteurs de l'avant-projet entendent dès lors adopter un dispositif qui a pour objet de mettre en place un système de conservation des données qui permettraient d'atteindre les objectifs dont la Cour de justice et la Cour constitutionnelle ont reconnu le caractère légitime, tout en se conformant aux décisions de ces hautes juridictions, dans leur dispositif et leur motivation, en particulier les limites et critères qui résultent de celles-ci en matière de conservation des données de trafic et de localisation par les opérateurs intervenant dans le secteur des communications électroniques, et d'accès à ces données par les autorités.

B. Mise en œuvre, par le texte en projet, des exigences découlant des arrêts de la cour de justice et de la cour constitutionnelle, ainsi que de la jurisprudence pertinente récente de la cour européenne des droits de l'homme

À titre préalable, la section de législation rappelle que sa saisine est limitée, par définition, au texte en projet et qu'il ne lui appartient pas, dans ces conditions, d'examiner si l'ensemble du droit positif belge, notamment judiciaire et relatif aux services de renseignement et de sécurité, est de nature à garantir le respect du droit à la vie privée, conformément notamment à la jurisprudence de la Cour européenne des droits de l'homme, dans la collecte et l'usage qui seraient faits des données dont la conservation est ici prévue. Ainsi, la compatibilité de la chaine de collecte, de conservation, d'accès et d'utilisation des données concernées avec les libertés et droits fondamentaux en cause, dépend d'autres dispositions en vigueur, qu'elles aient ou non une portée générale, dont la section de législation n'est pas saisie[9].

I.1. Les enseignements des arrêts *Digital Rights*, *Ministerio Fiscal*, et *La Quadrature du Net*

1.1. Des arrêts *Digital Rights*, *Ministerio Fiscal* et *La Quadrature du Net,* ainsi que de l'arrêt n° 84/2015 prononcé subséquemment par la Cour constitutionnelle, il convient essentiellement de retenir les éléments suivants:

1° La conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, constitue une ingérence dans le droit fondamental au respect de la vie privée et les autres droits consacrés à l'article 7 et à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, aggravée par la circonstance que les autorités pourront prendre connaissance de ces données.

2° Cette ingérence n'est toutefois pas de nature à porter atteinte au contenu essentiel de ces droits, lorsque l'accès donné au autorités nationales aux données concernées ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

[9] En ce sens, voir l'avis n° 58.449/4.

gelden, ongeacht de wijzigingen die bij de twee voormelde wetten aangebracht zijn.

4. Het is in die context dat de stellers van het voorontwerp derhalve een regeling voor gegevensbewaring willen invoeren om de doelstellingen te bereiken die het Hof van Justitie en het Grondwettelijk Hof legitiem hebben geacht en die in overeenstemming is met het dictum en de motivering van de beslissingen van die hoge rechtscolleges, in het bijzonder met de uit die beslissingen voortvloeiende grenzen en criteria inzake het bewaren van verkeers- en locatiegegevens door de operatoren die actief zijn in de sector van de elektronische communicatie alsook inzake de toegang tot die gegevens door de overheden.

B. Bepalingen ingevoerd bij de ontworpen tekst om tegemoet te komen aan de vereisten waaraan volgens de arresten van het Hof van Justitie en van het Grondwettelijk Hof alsook volgens de relevante recente rechtspraak van het Europees Hof voor de Rechten van de Mens voldaan moet zijn

Vooraf wijst de afdeling Wetgeving erop dat haar adiëring per definitie beperkt is tot de ontworpen tekst en dat het haar gelet op het voorgaande niet toekomt te onderzoeken of het geheel van het Belgisch positief recht, inzonderheid het gerechtelijk recht en het recht betreffende de inlichtingen- en veiligheidsdiensten, overeenkomstig met name de rechtspraak van het Europees Hof voor de Rechten van de Mens, het recht op eerbiediging van het privéleven kan waarborgen bij het verzamelen en het gebruiken van de gegevens waarvan dit ontwerp de bewaring regelt. Aldus hangt de vraag of de aaneenschakeling van de verzameling van, de bewaring van, de toegang tot en het gebruik van de betrokken gegevens verenigbaar is met de fundamentele rechten en vrijheden in kwestie af van andere geldende bepalingen, ongeacht of ze al dan niet een algemene strekking hebben, die niet aan de afdeling Wetgeving voorgelegd zijn.[9]

I.1. Lering van de arresten *Digital Rights*, *Ministerio Fiscal* en *La Quadrature du Net*

1.1. Uit de arresten inzake *Digital Rights, Ministerio Fiscal en La Quadrature du Net* evenals uit het daarop aansluitend arrest nr. 84/2015 van het Grondwettelijk Hof moet voornamelijk het volgende onthouden worden:

1° De bewaring van gegevens met de bedoeling dat de bevoegde nationale overheden eventueel tot die gegevens toegang hebben, vormt een inmenging in het fundamentele recht op eerbiediging van de persoonlijke levenssfeer en in de andere rechten die zijn neergelegd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, met als verzwarende omstandigheid dat de overheden kennis moeten kunnen nemen van die gegevens.

2° De wezenlijke inhoud van die rechten kan evenwel niet door die inmenging worden aangetast, wanneer het op grond van de toegang die de nationale overheden tot de betrokken gegevens krijgen niet mogelijk is om van de inhoud zelf van de elektronische communicatie kennis te nemen.

[9] Zie in die zin advies 58.449/4.

3° Cette ingérence répond par ailleurs à un objectif d'intérêt général lorsqu'elle a pour objet la lutte contre le terrorisme international, la lutte contre la criminalité grave afin de garantir la sécurité publique et le droit de toute personne à la sûreté.

4° La question se pose dès lors de savoir si l'ingérence concernée est proportionnée au but poursuivi, à savoir si elle comprend les mesures strictement nécessaires pour atteindre ce but; à ce propos, la réglementation en cause "doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données".

Sur ce point, ne satisfait pas à cette exigence de proportionnalité une législation qui:

a) couvre de manière généralisée toute personne et tous les moyens de communications électroniques ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves;

b) n'impose pas que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales et ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel;

c) ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, n'est pas limitée à une conservation portant:

– soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave;

– soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves;

d) "ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence"; à cet égard, est problématique une législation qui "ne contient pas les conditions matérielles et procédurales y afférentes" et "ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci"; il en va

3° Die inmenging beantwoordt voorts aan een doelstelling van algemeen belang, wanneer ze de bestrijding van het internationale terrorisme, de bestrijding van de zware criminaliteit met het oog op de openbare veiligheid en het recht van eenieder op veiligheid tot doel heeft.

4° De vraag rijst dus of de beoogde inmenging evenredig is met het nagestreefde doel, namelijk of het gaat om maatregelen die absoluut noodzakelijk zijn om dat doel te bereiken. Wat dat betreft moet de regeling in kwestie "duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens".

In dat opzicht wordt niet aan dat evenredigheidsvereiste voldaan door een wetgeving die:

a) algemeen van toepassing is op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel zware criminaliteit te bestrijden;

b) niet bepaalt dat de personen van wie de gegevens bewaard worden zich, zelfs indirect, in een situatie moeten bevinden die aanleiding kan geven tot strafrechtelijke vervolging en geen uitzonderingen bevat, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het beroepsgeheim vallen;

c) geen enkel verband vereist tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid en met name de bewaring niet beperkt tot:

– hetzij gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit;

– hetzij personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit;

d) "geen objectieve criteria bevat ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen"; in dat opzicht kunnen er problemen rijzen op grond van een wetgeving die "geen materiële en procedurele voorwaarden bevat" en "niet uitdrukkelijk bepaalt dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen"; dat geldt in het

spécialement ainsi lorsque la législation ne comporte “aucun critère objectif permettant de limiter le nombre de personnes disposant de l’autorisation d’accès et d’utilisation ultérieure des données conservées au strict nécessaire au regard de l’objectif poursuivi” et que “l’accès aux données conservées par les autorités nationales compétentes n’est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l’accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d’atteindre l’objectif poursuivi et intervient à la suite d’une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales”;

e) prévoit une durée générale de conservation des données “sans que soit opérée une quelconque distinction entre les catégories de données […] en fonction de leur utilité éventuelle aux fins de l’objectif poursuivi ou selon les personnes concernées” et ne précise pas “que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire”. Il peut en être déduit qu’il est requis que “l’ingérence soit précisément encadrée par des dispositions permettant de garantir qu’elle est effectivement limitée au strict nécessaire”;

f) ne prévoit pas de “règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée, au caractère sensible de ces données ainsi qu’au risque d’accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité”; il en va plus spécialement ainsi lorsque la législation n’impose pas aux opérateurs “un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles”, qui garantisse en outre la “destruction irrémédiable des données au terme de la durée de conservation de celles-ci”;

g) n’impose pas que les données en cause soient conservées sur le territoire de l’Union, avec pour conséquence que n’est dès lors pas “pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l’article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents”.

2. En ce qui concerne spécifiquement la portée de l’article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière de l’article 4, paragraphe 2 TUE ainsi que des articles 7, 8 et 11, de la Charte des droits fondamentaux de l’Union européenne, il y a lieu, pour l’essentiel, de retenir des arrêts *Ministerio Fiscal*, *Privacy International* et *La Quadrature du Net,* les éléments suivants:

1° N’est pas admissible une réglementation nationale permettant à une autorité étatique d’imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission

bijzonder wanneer de wetgeving “geen objectieve criteria bevat op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel” en “de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen is aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten”;

e) voorziet in een algemene bewaartermijn van de gegevens “zonder dat enig onderscheid wordt gemaakt tussen (…) categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen” en die niet preciseert “dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is”. Daaruit kan afgeleid worden dat vereist is dat “deze inmenging nauwkeurig omkaderd is door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke”;

f) niet voorziet in “specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die volgens deze richtlijn moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd, en die met name ertoe strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen”; dat geldt meer in het bijzonder wanneer de wetgeving niet van de operatoren vereist dat ze “via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden” dat bovendien waarborgt dat “de gegevens na de bewaarperiode onherroepelijk worden vernietigd”;

g) niet voorschrijft dat de gegevens in kwestie op het grondgebied van de Unie moeten worden bewaard, met als gevolg dat “niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest”.

2. Specifiek wat betreft de strekking van artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van artikel 4, lid 2, VEU en van de artikelen 7, 8 en 11 van het Handvest van de grondrechten van de Europese Unie, moet uit de arresten *Ministerio Fiscal*, *Privacy International* en *La Quadrature du Net* voornamelijk het volgende onthouden worden:

1° Niet toelaatbaar is een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een verplichting tot algemene en

généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement;

2° Est admissible une législation nationale qui permet aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et cette injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace;

3° Est admissible une législation nationale qui permet aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable;

4° Est admissible une législation nationale prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire;

5° Est admissible une législation nationale qui prévoit, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques;

6° Est admissible une législation nationale qui permet, aux fins de la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services;

7° Plus ponctuellement, est admissible une législation qui permet l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un

ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen;

2° Toelaatbaar is een nationale wettelijke regeling die het mogelijk maakt om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

3° Toelaatbaar is een nationale wettelijke regeling die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorziet in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

4° Toelaatbaar is een nationale wettelijke regeling die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorziet in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

5° Toelaatbaar is een nationale wettelijke regeling die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorziet in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen;

6° Toelaatbaar is een nationale wettelijke regeling die het mogelijk maakt om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode;

7° Toelaatbaar is meer specifiek een wetgeving die de toegang van overheidsinstanties mogelijk maakt tot de identificatiegegevens van de houders van met een gestolen

téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires: une telle réglementation comporte certes une ingérence dans les droits fondamentaux de ces derniers, mais cette ingérence ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

Concernant les points 2° à 6° qui précédent, les législations concernées ne sont admissibles que si, en outre, elles assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

3. Enfin, il faut également avoir à l'esprit que, dans son arrêt *La Quadrature du Net*, la Cour de Justice s'est également

mobiele telefoon geactiveerde simkaarten – zoals hun naam, voornaam en, in voorkomend geval, adres – een dergelijke regeling levert weliswaar een inmenging in de grondrechten van laatstgenoemden op, maar het betreft geen zodanig ernstige inmenging dat die toegang – op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit.

Wat de hiervoor vermelde punten 2° tot 6° betreft, zijn de betrokken wetgevingen enkel toelaatbaar als ze bovendien door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

3. Ten slotte moet ook voor ogen gehouden worden dat het Hof van Justitie zich in zijn arrest *La Quadrature du Net*

prononcée sur d'autres questions préjudicielles[10-11], posées par le Conseil d'État de France.

eveneens uitgesproken heeft over andere prejudiciële vragen[10-11] van de Raad van State van Frankrijk.

---

10 Dans l'affaire C-511/18, le Conseil d'État de France a posé les questions suivantes:
"1) L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58], ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE]?

2) La directive [2002/58] lue à la lumière de la [Charte] doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données?

3) La directive [2002/58], lue à la lumière de la [Charte], doit-elle être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou de telles procédures peuvent-elles être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours?".

11 Dans l'affaire C-512/18, le Conseil d'État de France a posé les questions préjudicielles suivantes:
"1) L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58], ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE]?

2) Les dispositions de la directive [2000/31], lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale?".

---

10 In de zaak C-511/18 heeft de Raad van State van Frankrijk de volgende vragen gesteld:
"1) Moet de verplichting tot algemene en ongedifferentieerde bewaring, die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van richtlijn [2002/58/EG] van 12 juli 2002, in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name door terreurgevaar, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van het Handvest van de grondrechten van de Europese Unie, en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 van het Verdrag betreffende de Europese Unie uitsluitend op de lidstaten rust?
2) Dient de richtlijn van 12 juli 2002, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie, aldus te worden uitgelegd dat zij het mogelijk maakt om wetgevende maatregelen te nemen, zoals maatregelen voor het in real time opvragen van verkeers- en locatiegegevens van welbepaalde personen, die weliswaar van invloed zijn op de rechten en verplichtingen van de aanbieders van een elektronische communicatiedienst, maar hun geen specifieke verplichting opleggen tot bewaring van hun gegevens?
3) Moet de richtlijn van 12 juli 2002, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie, aldus worden uitgelegd dat zij de regelmatigheid van de procedures voor het opvragen van verbindingsgegevens in alle gevallen afhankelijk stelt van het vereiste om de betrokken personen te informeren wanneer dergelijke informatie het onderzoek van de bevoegde autoriteiten niet langer in gevaar kan brengen, dan wel dat dergelijke procedures als regelmatig kunnen worden beschouwd gelet op alle andere bestaande procedurele waarborgen, aangezien deze waarborgen de doeltreffendheid van het recht op beroep garanderen?"

11 In de zaak C-512/18, heeft de Raad van State van Frankrijk de volgende vragen gesteld:
"1) Moet de verplichting tot algemene en ongedifferentieerde bewaring, die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van richtlijn [2002/58/EG] van 12 juli 2002, met name gelet op de waarborgen en controles die vervolgens gelden voor zowel het opvragen als het gebruiken van die verbindingsgegevens, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van het Handvest van de grondrechten van de Europese Unie en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 van het Verdrag betreffende de Europese Unie uitsluitend op de lidstaten rust?
2) Moeten de bepalingen van richtlijn [2000/31/EG] van 8 juni 2000, gelezen tegen de achtergrond van de artikelen 6, 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus worden uitgelegd dat zij toestaan dat een staat een nationale regeling invoert die de personen van wie de activiteit erin bestaat online toegang tot communicatiediensten aan het publiek aan te bieden, en de natuurlijke of rechtspersonen die, zelfs gratis, met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard, verplicht om gegevens te bewaren die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of van om het even welke inhoud van de diensten waarvan zij aanbieder zijn, zodat de gerechtelijke autoriteit in voorkomend geval om mededeling ervan kan verzoeken om de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven?"

C'est dans ce contexte que dans cet arrêt, la Cour de Justice a dit pour droit:

"L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque

– le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues, et que

– le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais".

4. Ceci étant rappelé, comme la section de législation l'a déjà souligné dans son avis n° 58.449/4, il y a lieu d'avoir égard à la portée circonscrite des différentes décisions de la Cour de Justice et de la Cour constitutionnelle.

Ainsi, l'affaire *Digital Rights* concerne la conservation et l'accès subséquent à des données, telles que visées par la directive 2006/24/UE, à savoir la conservation et l'accès à des données "en vue de garantir la disponibilité [de celles-ci] à des fins de recherche, de détection et de poursuite d'infractions graves". La portée de l'arrêt de la Cour de Justice et des conséquences à en tirer, aussi rigoureuses soient-elles, sont donc limitées à une conservation de données dont la finalité est, en sa phase ultime, la sanction pénale, par hypothèse, nécessairement non anodine, de comportements et d'actes constitutifs d'infractions graves.

Dans l'affaire *La Quadrature du Net*, la Cour de Justice s'est prononcée dans un contexte dans lequel la conservation considérée avait pour objectif, selon le cas, la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et la

In die context heeft het Hof van Justitie in dat arrest het volgende voor recht gezegd:

"Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer

– die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer

– het in real time verzamelen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden."

4. Zoals de afdeling Wetgeving reeds in advies 58.449/4 opgemerkt heeft, moet in het licht van deze bewoordingen rekening gehouden worden met de afgebakende draagwijdte van de verschillende beslissingen van het Hof van Justitie en van het Grondwettelijk Hof.

Zo heeft de zaak *Digital Rights* betrekking op de bewaring van en de daaropvolgende toegang tot gegevens zoals bedoeld in richtlijn 2006/24/EU, namelijk de bewaring en de toegang tot gegevens "teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit". De strekking van het arrest van het Hof van Justitie en de gevolgtrekkingen die daaruit moeten worden gemaakt, hoe strikt deze ook zijn, hebben dus enkel betrekking op het bewaren van gegevens waarvan het uiteindelijke doel erin bestaat gedragingen en handelingen die zware overtredingen vormen, strafrechtelijk te bestraffen, wat per definitie geen lichte bestraffing kan zijn.

In de zaak *La Quadrature du Net* heeft het Hof van Justitie zich uitgesproken in een context waarin de bewuste bewaring naargelang van het geval de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en

prévention des menaces graves contre la sécurité publique, ou la lutte contre la criminalité et la sauvegarde de la sécurité publique. Elle s'est également prononcée sur l'analyse automatisée de données en cas de menace grave pour la sécurité nationale, réelle, actuelle ou prévisible, et sur le recueil en temps réel de données relatives au trafic et des données de localisation limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées dans des activités de terrorisme.

Dans l'affaire *Ministerio Fiscal*, la Cour de Justice s'est prononcée à propos de l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé.

Enfin, dans l'arrêt *Privacy International*, la Cour de Justice était saisie d'une question portant sur une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de renseignement de sécurité.

L'avant-projet de loi doit donc être examiné en tenant compte de la circonstance que les exigences qui résultent des décisions précitées se situent essentiellement dans un contexte de lutte contre la criminalité, qui selon le cas, présente ou pas un caractère de gravité, et de protection de la sécurité nationale spécialement dans des cas où celle-ci est gravement menacée, en particulier par des actes de terrorisme.

Rien ne permet, à priori, d'étendre la portée de cet arrêt à une conservation ou à un accès à des données conservées qui auraient d'autres finalités comme la recherche, par un service de médiation, de l'auteur d'appels malveillants, l'identification de l'appelant ou du lieu d'un appel aux service d'urgence, en vue de permettre à ceux-ci d'intervenir afin de pouvoir garantir la sauvegarde des biens et des personnes, ou la recherche, indépendante de tout contexte infractionnel, d'une personne dont la disparition est inquiétante et dont il apparait que la vie pourrait être en danger imminent, ni même aux activités des services de renseignement et de sécurité.

Ces dernières hypothèses doivent donc être examinées non pas tant au regard de la jurisprudence précitée que de l'article 15, paragraphe 1, de la directive 2002/58/CE, dans la mesure où cette disposition permet d'autres dérogations que celles examinées dans les arrêts précités, ainsi qu'au regard des aspects plus généraux du droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, par l'article 7 de la Chartre des droits fondamentaux de l'Union

de voorkoming van ernstige bedreigingen van de openbare veiligheid of de bestrijding van criminaliteit en de bescherming van de openbare veiligheid tot doel had. Het Hof heeft zich ook uitgesproken over het op geautomatiseerde wijze analyseren van gegevens in geval van een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid en over het in real time verzamelen van verkeers- en locatiegegevens dat zich beperkt tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten.

In de zaak *Ministerio Fiscal* heeft het Hof van Justitie zich uitgesproken over de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten.

In het arrest *Privacy International* ten slotte werd aan het Hof van Justitie een vraag gesteld over een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

Bij het onderzoek van het voorontwerp van wet moet dus rekening gehouden worden met de omstandigheid dat de vereisten waaraan volgens de voormelde beslissingen voldaan moet zijn hoofdzakelijk te maken hebben met de bestrijding van de criminaliteit, waarbij het naargelang van het geval om al dan niet zware criminaliteit gaat, en met de bescherming van de nationale veiligheid, inzonderheid in gevallen waarin deze laatste ernstig bedreigd wordt, in het bijzonder door terroristische daden.

De strekking van dat arrest kan *a priori* niet worden uitgebreid tot een bewaring van gegevens of een toegang tot bewaarde gegevens die andere doeleinden zouden dienen, zoals het opsporen door een ombudsdienst van een persoon die kwaadwillige oproepen pleegt, de identificatie van de persoon die een hulpdienst belt of van de plaats van waaruit zo'n oproep wordt gedaan zodat de hulpdienst kan optreden en kan zorgen voor de bescherming van goederen en personen, of het opsporen buiten iedere strafrechtelijke context van een persoon van wie de verdwijning onrustwekkend is wanneer blijkt dat zijn leven in onmiddellijk gevaar zou kunnen zijn en zelfs niet tot de activiteiten van de inlichtingen- en veiligheidsdiensten.

Deze laatste gevallen moeten dus niet zozeer onderzocht worden in het licht van de voormelde rechtspraak, maar wel in het licht van artikel 15, lid 1, van richtlijn 2002/58/EG, in zoverre die bepaling andere afwijkingen toestaat dan die welke in de voornoemde arresten onderzocht zijn, alsook vanuit het oogpunt van de meer algemene aspecten van het recht op eerbiediging van het privéleven dat gewaarborgd wordt door artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden,

européenne et par l'article 22 de la Constitution[12], et du droit à la protection des données à caractère personnel, garanti spécifiquement par l'article 8 de la Chartre des droits fondamentaux de l'Union européenne ainsi que de la réglementation européenne y afférente, comme le règlement (UE) 2016/679 du parlement européen du Conseil du 27 avril 2016 'relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)' (ci-après le "RGPD").

5. Précisément en ce qui concerne le RGPD, l'arrêt *La Quadrature du Net* comporte des enseignements qui doivent être retenus.

Ainsi, dans son arrêt, la Cour de Justice a considéré:

"193. Par la seconde question dans l'affaire C-512/18, la juridiction de renvoi cherche, en substance, à savoir si les dispositions de la directive 2000/31, lues à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétées en ce sens qu'elles s'opposent à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

194. Tout en considérant que de tels services relèvent du champ d'application de la directive 2000/31, et non de celui de la directive 2002/58, la juridiction de renvoi est d'avis que l'article 15, paragraphes 1 et 2, de la directive 2000/31, lu en combinaison avec les articles 12 et 14 de celle-ci, n'instaure pas, par lui-même, une interdiction de principe de conserver des données relatives à la création de contenu à laquelle il pourrait seulement être dérogé de manière exceptionnelle. Cette juridiction se demande néanmoins si cette appréciation doit être retenue, compte tenu du respect nécessaire des droits fondamentaux consacrés aux articles 6 à 8 et 11 de la Charte.

195. En outre, la juridiction de renvoi précise que sa question vise l'obligation de conservation prévue à l'article 6 de la LCEN, lu en combinaison avec le décret n° 2011-219. Les données que doivent conserver les fournisseurs de services concernés à ce titre incluent, notamment, les données relatives à l'identité civile des personnes ayant fait usage de ces services, tels que leurs nom, prénom, leurs adresses

[12] Voir e.a., L. Tassone, *"La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme"* in "Enjeux européens et mondiaux de la protection des données personnelles", ouvrage collectif sous la direction d'A. Grosjean, Larcier, coll. Création Information Communication, p. 53 et s., et les références citées; concernant les services de renseignement et de sécurité, voir e.a. l'avis n° 42.178/2 donné le 19 février 2007 sur un avant-projet devenu la loi du 4 février 2010 'relative aux méthodes de recueil des données par les services de renseignement et de sécurité', *Doc. parl.*, Sénat, 2006-2007, n° 3-2138/1, pp. 279-297, *http://www.raadvst-consetat.be/dbx/avis/42178.pdf*.

door artikel 7 van het Handvest van de grondrechten van de Europese Unie en door artikel 22 van de Grondwet[12], evenals in het licht van het recht op bescherming van persoonsgegevens, dat specifiek gewaarborgd wordt door artikel 8 van het Handvest van de grondrechten van de Europese Unie, en in het licht van de desbetreffende Europese regelgeving, zoals verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming)' (hierna "de AVG").

5. Wat meer bepaald de AVG betreft, levert het arrest *La Quadrature du Net* leringen op die onthouden moeten worden.

Zo heeft het Hof van Justitie in zijn arrest het volgende geoordeeld:

"193. Met de tweede vraag in zaak C-512/18 wenst de verwijzende rechter in wezen te vernemen of de bepalingen van richtlijn 2000/31, gelezen in het licht van de artikelen 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moeten worden uitgelegd dat zij zich verzetten tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

194. De verwijzende rechter, die van mening is dat dergelijke diensten binnen de werkingssfeer van richtlijn 2000/31 en niet binnen die van richtlijn 2002/58 vallen, stelt zich op het standpunt dat artikel 15, leden 1 en 2, van richtlijn 2000/31, gelezen in samenhang met de artikelen 12 en 14 van deze richtlijn, als zodanig geen principieel verbod op het bewaren van gegevens inzake de creatie van inhoud invoert waarvan slechts bij wijze van uitzondering zou kunnen worden afgeweken. Hij vraagt zich niettemin af of dit standpunt aanvaardbaar is, gelet op de noodzaak om de in de artikelen 6 tot en met 8 en 11 van het Handvest verankerde grondrechten te eerbiedigen.

195. De verwijzende rechter verduidelijkt voorts dat zijn vraag ziet op de bewaarplicht die is neergelegd in artikel 6 LCEN, gelezen in samenhang met decreet nr. 2011-219. Tot de gegevens die de betrokken aanbieders van diensten uit dien hoofde dienen te bewaren, behoren onder meer de gegevens betreffende de burgerlijke identiteit van de personen die van die diensten hebben gebruikgemaakt, zoals hun naam,

[12] Zie onder meer L. Tassone, "La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme" in A. Grosjean (ed.), *Enjeux européens et mondiaux de la protection des données personnelles*, verzamelwerk, Larcier, coll. Création Information Communication, 53 e.v., en de verwijzingen aldaar; over de inlichtingen- en veiligheidsdiensten zie onder meer advies 42.178/2, op 19 februari 2007 gegeven over een voorontwerp dat ontstaan gegeven heeft aan de wet van 4 februari 2010 'betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten' *Parl.St.* Senaat 2006-07, nr. 3-2138/1, 279-297, *http://www.raadvst-consetat.be/dbx/avis/42178.pdf*.

postales associées, leurs adresses de courrier électronique ou de compte associées, leurs mots de passe et, lorsque la souscription du contrat ou du compte est payante, le type de paiement utilisé, la référence du paiement, le montant ainsi que la date et l'heure de la transaction.

196. De même, les données visées par l'obligation de conservation couvrent les identifiants des abonnés, des connexions et des équipements terminaux utilisés, les identifiants attribués aux contenus, les dates et heures de début et de fin des connexions et des opérations ainsi que les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus. L'accès à ces données, dont la durée de conservation s'élève à un an, peut être sollicité dans le cadre des procédures pénales et civiles, en vue de faire respecter les règles relatives à la responsabilité civile ou pénale, ainsi que dans le cadre de mesures de recueil de renseignement auxquelles l'article L. 851-1 du CSI s'applique.

197. À cet égard, il y a lieu de relever que, conformément à son article 1er, paragraphe 2, la directive 2000/31 rapproche certaines dispositions nationales applicables aux services de la société de l'information visés à son article 2, sous a).

198. De tels services englobent, certes, ceux qui sont fournis à distance au moyen d'équipements électroniques de traitement et de stockage de données, à la demande individuelle d'un destinataire de services et, normalement, contre rémunération, tels que des services d'accès à Internet ou à un réseau de communication ainsi que des services d'hébergement (voir, en ce sens, arrêts du 24 novembre 2011, Scarlet Extended, C-70/10, EU:C:2011:771, point 40; du 16 février 2012, SABAM, C-360/10, EU:C:2012:85, point 34; du 15 septembre 2016, Mc Fadden, C-484/14, EU:C:2016:689, point 55, ainsi que du 7 aout 2018, SNB-REACT, C-521/17, EU:C:2018:639, point 42 et jurisprudence citée).

199. Toutefois, l'article 1, paragraphe 5, de la directive 2000/31 dispose que celle-ci n'est pas applicable aux questions relatives aux services de la société de l'information qui sont couvertes par les directives 95/46 et 97/66. À cet égard, il ressort des considérants 14 et 15 de la directive 2000/31 que la protection de la confidentialité des communications ainsi que des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information est uniquement régie par les directives 95/46 et 97/66, cette dernière interdisant, à son article 5, aux fins de la protection de la confidentialité des communications, toute forme d'interception ou de surveillance des communications.

200. Ainsi, des questions liées à la protection de la confidentialité des communications et des données à caractère personnel doivent être appréciées à l'aune de la directive 2002/58 et du règlement 2016/679, ceux-ci ayant remplacé respectivement la directive 97/66 et la directive 95/46, étant précisé que la protection que vise à assurer la directive 2000/31 ne peut en tout état de cause pas porter atteinte aux exigences résultant de la directive 2002/58 et du règlement 2016/679 (voir, en

voornaam, hun bijbehorende postadressen, hun bijbehorende e-mail- of accountadressen, hun wachtwoorden en, wanneer het ondertekenen van het contract of het aanmaken van het account plaatsvindt tegen betaling, de gebruikte betaalsoort, de betalingsreferentie, het bedrag en de datum en het tijdstip van de transactie.

196. Tot de te bewaren gegevens behoren ook de identificatoren van de abonnees, van de verbindingen en van de gebruikte eindapparatuur, de aan de inhoud toegekende identificatoren, de datum en het tijdstip van het begin en het einde van de verbindingen en verrichtingen, en de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud. De bewaartermijn voor die gegevens bedraagt één jaar en er kan om toegang tot die gegevens worden verzocht in het kader van strafrechtelijke en civielrechtelijke procedures, om de regels inzake civielrechtelijke of strafrechtelijke aansprakelijkheid te doen naleven, en in het kader van maatregelen voor het inwinnen van inlichtingen waarop artikel L. 851-1 CSI van toepassing is.

197. In dit verband moet worden opgemerkt dat richtlijn 2000/31 volgens artikel 1, lid 2, bepaalde nationale bepalingen nader tot elkaar brengt die van toepassing zijn op de diensten van de informatiemaatschappij in de zin van artikel 2, onder a).

198. Tot die diensten behoren onder meer die welke op individueel verzoek van een afnemer van diensten en gewoonlijk tegen vergoeding worden verricht via elektronische apparatuur voor de verwerking en de opslag van gegevens op afstand, zoals diensten waarbij toegang wordt verschaft tot het internet of tot een communicatienetwerk, en opslagdiensten (zie in die zin arresten van 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punt 40; 16 februari 2012, SABAM, C-360/10, EU:C:2012:85, punt 34; 15 september 2016, Mc Fadden, C-484/14, EU:C:2016:689, punt 55, en 7 augustus 2018, SNB-REACT, C-521/17, EU:C:2018:639, punt 42 en aldaar aangehaalde rechtspraak).

199. Artikel 1, lid 5, van richtlijn 2000/31 bepaalt evenwel dat deze richtlijn niet van toepassing is op kwesties in verband met diensten van de informatiemaatschappij die onder richtlijnen 95/46 en 97/66 vallen. Dienaangaande blijkt uit de overwegingen 14 en 15 van richtlijn 2000/31 dat de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij uitsluitend wordt beheerst door richtlijnen 95/46 en 97/66. Laatstgenoemde richtlijn stelt ter waarborging van de vertrouwelijkheid van communicatie in artikel 5 een verbod op iedere vorm van onderschepping of bewaking van berichten.

200. Vragen die verband houden met de bescherming van het vertrouwelijke karakter van communicatie en van persoonsgegevens moeten derhalve worden beoordeeld aan de hand van richtlijn 2002/58 en verordening 2016/679, die in de plaats zijn gekomen van, respectievelijk, richtlijn 97/66 en richtlijn 95/46, waarbij moet worden aangetekend dat de bescherming die richtlijn 2000/31 beoogt te verzekeren, hoe dan ook geen afbreuk mag doen aan de vereisten die

ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 57).

201. L'obligation imposée par la réglementation nationale visée au point 195 du présent arrêt aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement de conserver des données à caractère personnel afférentes à ces services doit donc, comme l'a relevé en substance M. l'avocat général au point 141 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), être appréciée à l'aune de la directive 2002/58 ou du règlement 2016/679.

202. Ainsi, selon que la fourniture des services couverts par cette réglementation nationale relève ou non de la directive 2002/58, elle sera régie soit par cette dernière directive, en particulier par l'article 15, paragraphe 1, de celle-ci, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, soit par le règlement 2016/679, en particulier par l'article 23, paragraphe 1, dudit règlement, lu à la lumière des mêmes dispositions de la Charte.

203. En l'occurrence, il ne saurait être exclu, comme l'a relevé la Commission européenne dans ses observations écrites, que certains des services auxquels s'applique la réglementation nationale visée au point 195 du présent arrêt constituent des services de communications électroniques, au sens de la directive 2002/58, ce qu'il appartient à la juridiction de renvoi de vérifier.

204. À cet égard, il convient de relever que la directive 2002/58 couvre les services de communications électroniques qui remplissent les conditions énoncées à l'article 2, sous c), de la directive 2002/21, auquel renvoie l'article 2 de la directive 2002/58 et qui définit le service de communications électroniques comme étant 'le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion'. S'agissant des services de la société de l'information, tels que visés aux points 197 et 198 du présent arrêt et couverts par la directive 2000/31, ceux-ci constituent des services de communications électroniques dès lors qu'ils consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, points 47 et 48)

205. Ainsi, les services d'accès à Internet, lesquels paraissent être couverts par la réglementation nationale visée au point 195 du présent arrêt, constituent, comme le confirme le considérant 10 de la directive 2002/21, des services de communications électroniques, au sens de cette directive (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, point 37). Tel est également le cas des services de messageries sur Internet, dont il ne semble pas exclu qu'ils relèvent également de cette réglementation nationale, dès lors que, sur le plan technique, ils impliquent

voortvloeien uit richtlijn 2002/58 en verordening 2016/679 (zie in die zin arrest van 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punt 57).

201. De bewaarplicht die de in punt 195 van het onderhavige arrest bedoelde nationale regeling oplegt aan aanbieders die het publiek online toegang geven tot communicatiediensten en aanbieders van opslagdiensten, en die betrekking heeft op de met die diensten verband houdende persoonsgegevens, moet dus worden getoetst aan richtlijn 2002/58 of verordening 2016/679, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 141 van zijn conclusie in de gevoegde zaken La Quadrature du Net e.a. (C-511/18 en C-512/18, EU:C:2020:6).

202. Afhankelijk van de vraag of de levering van de diensten waarop die nationale regeling betrekking heeft, al dan niet onder richtlijn 2002/58 valt, zal die levering derhalve ofwel worden beheerst door deze richtlijn, in het bijzonder door artikel 15, lid 1, ervan, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, ofwel door verordening 2016/679, in het bijzonder door artikel 23, lid 1, van deze verordening, gelezen in het licht van dezelfde bepalingen van het Handvest.

203. Zoals de Europese Commissie in haar schriftelijke opmerkingen heeft gesteld, valt *in casu* niet uit te sluiten dat sommige van de diensten waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling betrekking heeft, elektronischecommunicatiediensten in de zin van richtlijn 2002/58 zijn, hetgeen de verwijzende rechter dient na te gaan.

204. In dit verband moet worden opgemerkt dat richtlijn 2002/58 van toepassing is op elektronischecommunicatiediensten die voldoen aan de voorwaarden die vermeld staan in artikel 2, onder c), van richtlijn 2002/21, waarnaar artikel 2 van richtlijn 2002/58 verwijst en waarin een elektronischecommunicatiedienst wordt gedefinieerd als 'een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt'. Wat de door richtlijn 2000/31 bestreken diensten van de informatiemaatschappij als bedoeld in de punten 197 en 198 van het onderhavige arrest betreft, deze diensten zijn elektronischecommunicatiediensten indien zij geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken. (zie in die zin arrest van 5 juni 2019, Skype Communications, C-142/18, EU:C:2019:460, punten 47 en 48).

205. Internettoegangsdiensten, waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling van toepassing lijkt te zijn, zijn derhalve elektronischecommunicatiediensten in de zin van richtlijn 2002/21, zoals in overweging 10 van deze richtlijn wordt bevestigd (zie in die zin arrest van 5 juni 2019, Skype Communications, C-142/18, EU:C:2019:460, punt 37). Dit geldt ook voor webgebaseerde e-maildiensten, die mogelijk eveneens onder die nationale regeling vallen, aangezien die diensten technisch gezien kunnen worden beschouwd als diensten die geheel of hoofdzakelijk bestaan

entièrement ou principalement la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 13 juin 2019, Google, C-193/18, EU:C:2019:498, points 35 et 38).

206. S'agissant des exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, il convient de renvoyer à l'ensemble des constatations et des appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18.

207. Quant aux exigences découlant du règlement 2016/679, il convient de rappeler que celui-ci vise, notamment, ainsi qu'il ressort de son considérant 10, à assurer un niveau élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 101).

208. À cette fin, tout traitement de données à caractère personnel doit, sous réserve des dérogations admises à l'article 23 du règlement 2016/679, respecter les principes régissant les traitements des données à caractère personnel ainsi que les droits de la personne concernée énoncés respectivement dans les chapitres II et III de ce règlement. En particulier, tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes énoncés à l'article 5 dudit règlement et, d'autre part, satisfaire aux conditions de licéité énumérées à l'article 6 de ce même règlement (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 30 mai 2013, Worten, C-342/12, EU:C:2013:355, point 33 et jurisprudence citée).

209. Pour ce qui est, plus particulièrement, de l'article 23, paragraphe 1, du règlement 2016/679, il y a lieu de relever que celui-ci, à l'instar de ce qui est prévu à l'article 15, paragraphe 1, de la directive 2002/58, permet aux États membres de limiter, au regard des finalités qu'il prévoit et au moyen de mesures législatives, la portée des obligations et des droits qui y sont visés "lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir" la finalité poursuivie. Toute mesure législative prise sur ce fondement doit, en particulier, respecter les exigences spécifiques posées à l'article 23, paragraphe 2, de ce règlement.

210. Ainsi, l'article 23, paragraphes 1 et 2, du règlement 2016/679 ne saurait être interprété comme pouvant conférer aux États membres le pouvoir de porter atteinte au respect de la vie privée, en méconnaissance de l'article 7 de la Charte, tout comme aux autres garanties prévues par celle-ci (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-38/01 et C-139/01, EU:C:2003:294, point 91). En particulier, à l'instar

in het overbrengen van signalen via elektronischecommunicatienetwerken (zie in die zin arrest van 13 juni 2019, Google, C-193/18, EU:C:2019:498, punten 35 en 38).

206. Wat de vereisten betreft die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zij verwezen naar alle vaststellingen en beoordelingen in het kader van de beantwoording van de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18.

207. Wat de uit verordening 2016/679 voortvloeiende vereisten betreft, zij eraan herinnerd dat deze verordening, zoals blijkt uit overweging 10 ervan, met name een consistent en hoog niveau van bescherming van natuurlijke personen binnen de Unie beoogt te waarborgen en daartoe een coherente en homogene toepassing van de regels inzake bescherming van de grondrechten van deze personen in verband met de verwerking van persoonsgegevens binnen de gehele Unie wil verzekeren (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 101).

208. Daartoe moeten bij elke verwerking van persoonsgegevens, behoudens de op grond van artikel 23 van verordening 2016/679 toegestane uitzonderingen, de in hoofdstuk II van deze verordening neergelegde beginselen inzake verwerking van persoonsgegevens en de in hoofdstuk III van deze verordening geregelde rechten van de betrokkene worden geëerbiedigd. In het bijzonder moet elke verwerking van persoonsgegevens ten eerste in overeenstemming zijn met de in artikel 5 van verordening 2016/679 geformuleerde beginselen, en ten tweede voldoen aan de in artikel 6 van deze verordening opgesomde rechtmatigheidsvoorwaarden (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 30 mei 2013, Worten, C-342/12, EU:C:2013:355, punt 33 en aldaar aangehaalde rechtspraak).

209. Wat meer bepaald artikel 23, lid 1, van verordening 2016/679 betreft, moet worden opgemerkt dat deze bepaling – net als artikel 15, lid 1, van richtlijn 2002/58 – de lidstaten de mogelijkheid biedt om met het oog op de erin genoemde doelstellingen via wetgevingsmaatregelen de reikwijdte van de erin bedoelde verplichtingen en rechten te beperken, "op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van" het nagestreefde doel. Elke op die grondslag vastgestelde wettelijke maatregel moet met name voldoen aan de specifieke vereisten die zijn geformuleerd in artikel 23, lid 2, van verordening 2016/679.

210. Artikel 23, leden 1 en 2, van verordening 2016/679 kan derhalve niet aldus worden uitgelegd dat het de lidstaten de bevoegdheid kan verlenen om afbreuk te doen aan de eerbiediging van de persoonlijke levenssfeer, in strijd met artikel 7 van het Handvest, of aan de andere door het Handvest geboden waarborgen (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 20 mei 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 en C-139/01, EU:C:2003:294, punt 91).

de ce qui vaut pour l'article 15, paragraphe 1, de la directive 2002/58, le pouvoir que confère l'article 23, paragraphe 1, du règlement 2016/679 aux États membres ne saurait être exercé que dans le respect de l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire (voir, par analogie, s'agissant de la directive 95/46, arrêt du 7 novembre 2013, IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

211. Il s'ensuit que les constatations et les appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 s'appliquent *mutatis mutandis* à l'article 23 du règlement 2016/679".

Pour conclure, la Cour de Justice a dit pour droit:

"La directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ('directive sur le commerce électronique'), doit être interprétée en ce sens qu'elle n'est pas applicable en matière de protection de la confidentialité des communications et des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information, cette protection étant, selon le cas, régie par la directive 2002/58, telle que modifiée par la directive 2009/136, ou par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46. L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services".

6. Enfin, il convient d'avoir particulièrement égard à l'invitation formulée par la Cour constitutionnelle dans son arrêt n° 57/2021.

Pour rappel, la Cour constitutionnelle a considéré que:

– Un changement de perspective s'impose par rapport au choix que le législateur a effectué: l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle.

– La réglementation prévoyant une telle obligation doit être soumise à des règles claires et précises concernant la

Net zoals geldt voor artikel 15, lid 1, van richtlijn 2002/58, is het met name zo dat de bevoegdheid die artikel 23, lid 1, van verordening 2016/679 de lidstaten verleent, slechts kan worden uitgeoefend in overeenstemming met het evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 7 november 2013, IPI, C-473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).

211. Bijgevolg gelden de vaststellingen die zijn gedaan in het kader van de beantwoording van de eerste vraag in de zaken C-511/18 en C-512/18 en van de eerste en de tweede vraag in zaak C-520/18, en de beoordelingen die in dat kader zijn verricht, *mutatis mutandis* voor artikel 23 van verordening 2016/679."

Concluderend heeft het Hof van Justitie voor recht verklaard:

"richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000, betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel') moet aldus worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, of door verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming). Artikel 23, lid 1, van verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd."

6. Tot slot dient bijzondere aandacht besteed te worden aan het verzoek dat het Grondwettelijk Hof in arrest 57/2021 geformuleerd heeft.

Er wordt aan herinnerd dat het Grondwettelijk Hof het volgende heeft geoordeeld:

– Er is een verandering van gezichtspunt vereist ten opzichte van de keuze die de wetgever heeft gemaakt: de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel.

– De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke

portée et l'application de la mesure en cause et imposant des exigences minimales.

– Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours "répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi".

Dans ce but, il appartient au législateur d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire.

I.2. La jurisprudence de la cour européenne des droits de l'homme

De manière plus générale, il convient également d'avoir égard au droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par l'article 22 de la Constitution[13].

De la jurisprudence de la Cour européenne des droits de l'homme[14], s'agissant spécialement de la surveillance secrète et de l'interception de masse des communications et des données y afférentes, il y a lieu de retenir, en substance, les principes suivants:

– 1° la surveillance secrète des citoyens n'est admissible que dans la mesure où elle est strictement nécessaire à la sauvegarde des institutions démocratiques. Des dispositions législatives qui accordent des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications sont, devant une situation exceptionnelle telle la menace par des formes complexes d'espionnage et par le terrorisme, nécessaires dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales;

– 2° L'organisation d'un tel régime doit toutefois être "prévu par la loi" et "nécessaire"; dans ce cadre, la Cour européenne des droits de l'homme examine si le cadre juridique national définit clairement:

1. Les motifs pour lesquels l'interception en masse peut être autorisée;

[13] Voir e.a., L. TASSONE, *"La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme"* in "Enjeux européens et mondiaux de la protection des données personnelles", ouvrage collectif sous la direction d'A. Grosjean, Larcier, coll. Création Information Communication, p. 53 et s. , et les références citées; concernant les services de renseignement et de sécurité, voir e.a. l'avis n° 42.178/2.

[14] Voir notamment, pour un arrêt de principe, Cour.eur.D.H, arrêt *Klass et autres c. Allemagne*, 9 septembre 1978. Pour un rappel récent de la jurisprudence en la matière et des principes en la matière tels qu'ils résultent de celle-ci, voir Cour.eur.D.H, arrêt *Big Brother watch et autre c. Royaume-Uni*, 25 mai 2021, 322 à 364.

en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd.

– Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds "beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel".

Daartoe staat het aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

I.2. De rechtspraak van het Europees Hof voor de Rechten van de Mens

Meer in het algemeen dient ook rekening gehouden te worden met het recht op eerbiediging van het privéleven, dat gewaarborgd wordt bij artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en bij artikel 22 van de Grondwet.[13]

Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens[14], meer in het bijzonder wat betreft het geheim toezicht op en de massale onderschepping van communicatie en de daarmee verband houdende gegevens, moet in wezen met de volgende beginselen rekening gehouden worden:

– 1° geheim toezicht op burgers kan slechts aanvaard worden voor zover het strikt noodzakelijk is voor de bescherming van de democratische instellingen. Wetsbepalingen waarbij bevoegdheden verleend worden inzake geheim toezicht op correspondentie, postzendingen en telecommunicatie, zijn, in een uitzonderlijke situatie zoals de bedreiging door complexe vormen van spionage en terrorisme, in een democratische samenleving noodzakelijk voor de nationale veiligheid en/of de bescherming van de openbare orde en het voorkomen van strafbare feiten;

– 2° de invoering van een dergelijke regeling moet echter "bij wet voorzien" en "noodzakelijk" zijn; in dit kader onderzoekt het Europees Hof voor de Rechten van de Mens of het nationaal juridisch kader een duidelijke definitie bevat van:

1. de redenen waarom massale onderschepping toegestaan kan worden;

[13] Zie onder meer L. TASSONE, "*La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme*" in Enjeux européens et mondiaux de la protection des données personnelles, A. Grosjean (ed.), Larcier, coll. Création Information Communication, 53 e.v., en de verwijzingen aldaar; over de inlichtingen- en veiligheidsdiensten zie onder meer advies 42.178/2.

[14] Zie onder meer het principearrest, EHRM, arrest-*Klass e.a. t. Duitsland*, 9 september 1978. Zie EHRM, arrest *Big Brother watch en anderen t. Verenigd Koninkrijk*, 25 mei 2021, 322 tot 364 voor een recente herinnering aan de rechtspraak ter zake en de beginselen die daaruit voortvloeien.

2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées;

3. La procédure d'octroi d'une autorisation;

4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés;

5. Les précautions à prendre pour la communication de ces éléments à d'autres parties;

6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits;

7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement;

8. Les procédures de contrôle indépendant à posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

Le processus doit ainsi être encadré par des "garanties de bout en bout", qui permettent de s'assurer que la nécessité et la proportionnalité des mesures prises est appréciée à chaque étape du processus de la surveillance, spécialement de l'interception des données; ces garanties impliquent[15] notamment que

– les activités d'interception, à tout le moins de masse, doivent être soumises à l'autorisation d'une autorité indépendante dès le départ, à savoir lors de la définition de l'objet et de l'étendue de l'activité;

– les activités doivent faire l'objet d'une supervision et d'un contrôle indépendant opéré à posteriori[16].

2. de omstandigheden waarin de communicatie van een persoon onderschept mag worden;

3. De procedure voor het verlenen van een machtiging;

4. De procedure die gevolgd moet worden voor de selectie, het onderzoek en het gebruik van de onderschepte gegevens.

5. De voorzorgen die genomen moeten worden voor het mededelen van die gegevens aan andere partijen.

6. De beperkingen die gelden voor de duur van de onderschepping en voor de termijn waarin de onderschepte gegevens bewaard mogen worden, alsook de omstandigheden waarin die gegevens gewist of vernietigd moeten worden.

7. De procedures en nadere regels met betrekking tot het toezicht, door een onafhankelijke instantie, op de naleving van de hierboven vermelde waarborgen en de bevoegdheden van die instantie in geval van niet-naleving;

8. De procedures voor het onafhankelijk toezicht achteraf op de naleving van de waarborgen en de bevoegdheden die aan de bevoegde instantie verleend worden voor het behandelen van gevallen van niet-naleving.

Het proces moet derhalve afgebakend worden met "end-to-end-waarborgen", die het mogelijk maken zich ervan te vergewissen dat de noodzaak en de proportionaliteit van de genomen maatregelen in elke fase van het toezichtproces beoordeeld worden, inzonderheid bij het onderscheppen van gegevens; die waarborgen[15] houden onder andere in dat

– voor onderscheppingsactiviteiten, althans voor massale onderscheppingsactiviteiten , van meet af aan, d.w.z. bij de omschrijving van de bedoeling en de omvang van de activiteit, een vergunning verleend moet zijn door een onafhankelijke instantie;

– de activiteiten moeten worden onderworpen aan een onafhankelijk toezicht en aan een onafhankelijke controle die achteraf uitgevoerd wordt.[16]

---

15 Voir à ce propos, e.a., Cour.eur.D.H, arrêt *Big Brother watch et autre c. Royaume-Uni* , 25 mai 2021, 350.

16 La Cour européenne des droits de l'homme considère "qu'en ce qui concerne l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications". Elle considère en tout cas que l'exigence d'une autorisation indépendante vaut pour ces deux catégories (voir à ce propos, e.a., Cour.eur.D.H, arrêt *Big Brother watch et autre c. Royaume-Uni*, 25 mai 2021, 363 et 364, et 417 et 418).

15 Zie in dat verband onder meer EHRM, *arrest Big brother watch e. a. t. Verenigd Koninkrijk*, 25 mei 2021, 350.

16 Het Europees Hof voor de Rechten van de Mens heeft in dat verband het volgende geoordeeld: "(…) qu'en ce qui concerne l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications". Het Hof is hoe dan ook van mening dat het vereiste van een onafhankelijke vergunning voor beide categorieën geldt (zie in dit verband onder andere EHRM, *Big Brother watch e.a. t. Verenigd Koninkrijk*, 25 mei 2021, 363 en 364, en 417 en 418).

Examen de l'avant-projet

Observation Préalable

Avant toute autre observation, il échet de rappeler que dans son arrêt n° 57/2021, faisant suite à l'arrêt *La Quadrature du Net*, la Cour constitutionnelle a invité le législateur à opérer un changement de perspective dans la conservation des données concernées, de sorte que celle-ci demeure l'exception et non la règle, et qu'elle soit organisée par des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales de telle sorte que l'ingérence se limite au strict nécessaire et réponde à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. La Cour constitutionnelle a suggéré que, dans ce but, le législateur opère les distinctions qui s'imposent entre les différents types de données soumises à conservation.

L'avant-projet à l'examen se donne pour objet de répondre clairement à cet arrêt, en s'inscrivant dans les balises ainsi posées par la Cour constitutionnelle.

L'avant-projet appelle toutefois différentes observations générales, au regard, notamment, de la limitation au strict nécessaire des différents régimes de conservation organisés par catégories de données et de finalités, de la clarté et de la précision des régimes en projet, et de leur conformité au principe de légalité inscrit à l'article 22 de la Constitution, ce outre les observations particulières qui seront formulées ensuite.

Observations générales

Le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue d'assurer la sécurité nationale, dans des situations où l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible

1. Pour rappel, selon l'enseignement de l'arrêt *La Quadrature du Net*, est admissible une législation qui permet qu'une injonction soit donnée aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue d'assurer la sécurité nationale, dans des situations où l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible.

Il faut toutefois que la décision emportant cette injonction puisse faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des

Onderzoek van het voorontwerp

Voorafgaande opmerking

Voordat enige andere opmerking gemaakt wordt, dient eraan herinnerd te worden dat het Grondwettelijk Hof in arrest nr. 57/2021, dat volgt op het arrest *La Quadrature du Net*, de wetgever verzocht heeft om van gezichtspunt te veranderen wat de bewaring van de desbetreffende gegevens betreft opdat die de uitzondering zou blijven en niet de regel zou worden, en dat voor die bewaring duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel zouden gelden en dat daarbij een minimum aan regels opgelegd zou worden, zodat de inmenging tot het strikt noodzakelijke beperkt wordt en beantwoordt aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel. Het Grondwettelijk Hof heeft gesuggereerd dat de wetgever daartoe tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid zou maken dat geboden is.

Voorliggend voorontwerp strekt ertoe duidelijk tegemoet te komen aan dat arrest, door binnen de bakens te blijven die aldus door het Grondwettelijk Hof uitgezet zijn.

Het voorontwerp geeft echter aanleiding tot verscheidene algemene opmerkingen, met name op het stuk van de beperking tot het strikt noodzakelijke voor alle ontworpen regelingen inzake bewaring die opgezet worden per categorie van gegevens en per doeleinde, de duidelijkheid en de nauwkeurigheid van de ontworpen regelingen en hun verenigbaarheid met het legaliteitsbeginsel dat in artikel 22 van de Grondwet verankerd is, naast de bijzondere opmerkingen die vervolgens geformuleerd zullen worden.

Algemene opmerkingen

Het opleggen, aan de aanbieders van elektronischecommunicatiediensten, van een bevel tot een algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens ter bescherming van de nationale veiligheid, in situaties waarin de Staat geconfronteerd wordt met een ernstige bedreiging van de nationale veiligheid die werkelijk en actueel of voorzienbaar blijkt

1. Er zij aan herinnerd dat volgens de lering van het arrest *La Quadrature du Net* ingestemd kan worden met een wettelijke regeling die het mogelijk maakt om aan de aanbieders van elektronische communicatiediensten een bevel te geven tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ter bescherming van de nationale veiligheid in situaties waarin de Staat geconfronteerd wordt met een ernstige bedreiging van de nationale veiligheid die werkelijk en actueel of voorzienbaar blijkt.

De beslissing waarbij een dergelijk bevel opgelegd wordt, dient evenwel effectief getoetst te kunnen worden door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing erin bestaat na te gaan of een van die situaties zich

conditions et des garanties devant être prévues. Par ailleurs, cette injonction ne peut être émise que pour une période temporellement limitée au strict nécessaire, mais elle peut être renouvelée en cas de persistance de cette menace.

2.1.1. L'article 31 de l'avant-projet à l'examen entend insérer, dans la loi du 30 novembre 1998 'organique des services de renseignements et de sécurité' un article 18/17/1, rédigé comme suit:

"Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux.

La réquisition est effectuée par écrit par le dirigeant du service et mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné visée à l'article 18/10 § 3, alinéa 3, selon le cas.

L'autorisation du dirigeant du service est transmise au ministre compétent.

Le service de renseignement et de sécurité concerné peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques pour transmettre la réquisition à tous les opérateurs concernés.

Le dirigeant du service peut requérir, par une décision écrite, des personnes dont il présume qu'elles ont une expertise technique utile de prêter leur concours à la mise en œuvre de cette méthode. Cette réquisition mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.

Toute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à vingt mille euros.

La méthode est autorisée pour une durée ne pouvant excéder 6 mois sans préjudice de la procédure visée à l'article 18/10, § 5.

Le service de renseignement et de sécurité concerné fait rapport à la commission tous les deux mois sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

Le Roi peut déterminer, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les

voordoet en of voldaan is aan de voorwaarden en waarborgen waarin voorzien moet worden. Bovendien mag dat bevel slechts opgelegd worden voor een periode die niet langer is dan strikt noodzakelijk, maar die verlengd kan worden indien die bedreiging voortduurt.

2.1.1. Artikel 31 van voorliggend voorontwerp strekt ertoe in de wet van 30 november 1998 'houdende regeling van de inlichtingen– en veiligheidsdiensten', een artikel 18/17/1 in te voegen, luidende:

"De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid, de medewerking vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt.

De vordering wordt schriftelijk gedaan door het diensthoofd en vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister bedoeld in artikel 18/10, § 3, derde lid.

De machtiging van het diensthoofd wordt overgemaakt aan de bevoegde minister.

De betrokken inlichtingen- en veiligheidsdienst kan de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, om de vordering aan alle betrokken operatoren over te maken.

Het diensthoofd kan bij schriftelijke beslissing vorderen dat personen van wie hij veronderstelt dat zij over de nodige technische deskundigheid beschikken, medewerking verlenen bij de tenuitvoerlegging van deze methode. De vordering vermeldt, naargelang het geval, de aard van de instemming van de commissie, de aard van de instemming van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.

Eenieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

De methode wordt toegestaan voor een periode die niet langer mag zijn dan 6 maanden onverminderd de procedure bedoeld in artikel 18/10, § 5.

De betrokken inlichtingen– en veiligheidsdienst brengt om de twee maanden bij de Commissie verslag uit over de evolutie van de dreiging. In dit verslag worden de elementen belicht die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen.

De Koning kan, op voorstel van de minister van Justitie, de minister van Defensie en de minister bevoegd voor de

communications électroniques dans ses attributions, des modalités de collaboration des opérateurs".

2.1.2. Il y a lieu de constater que la disposition en projet répond aux exigences de droit européen dans la mesure où elle limite la possibilité d'injonction aux opérateurs à la seule fin de garantir la sécurité nationale, dans des situations où l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible.

2.1.3. Quant à la durée de l'opération – laquelle doit être limitée au strict nécessaire – le système mis en place prévoit qu'

– elle est limitée à six mois maximum, étant entendu que le service de renseignement et de sécurité concerné fait rapport à la Commission[17] tous les deux mois sur l'évolution de la menace, rapport qui a pour objet de mettre en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

– elle peut être prolongée aux conditions strictes de l'article 18/10, § 5, de la loi du 30 novembre 1998[18].

Ce système, qui résulte de la combinaison de l'article 18/10, en vigueur, et de l'article 18/17/1, en projet, de la loi du 30 novembre 1998, apparait ainsi de nature à répondre aux exigences résultant du droit européen sur ce point.

elektronische communicatie, nadere regels voor de samenwerking met de operatoren bepalen."

2.1.2. Er dient vastgesteld te worden dat de ontworpen bepaling tegemoetkomt aan de vereisten van het Europees recht voor zover de mogelijkheid om aan de operatoren een bevel te geven daarbij alleen geboden wordt ter bescherming van de nationale veiligheid in situaties waarin de Staat geconfronteerd wordt met een ernstige bedreiging van de nationale veiligheid die reëel en actueel of voorzienbaar blijkt.

2.1.3. Met betrekking tot de duur van de operatie – die tot het strikt noodzakelijke beperkt moet worden – wordt in de in te voeren regeling bepaald dat:

– die duur beperkt wordt tot maximaal zes maanden, met dien verstande dat de betrokken inlichtingen- en veiligheidsdienst om de twee maanden bij de Commissie[17] een verslag aangaande de evolutie van de dreiging moet indienen waarvan het de bedoeling is dat daarin de elementen belicht worden die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen.

– die duur verlengd kan worden onder de strikte voorwaarden bepaald in artikel 18/10, § 5, van de wet van 30 november 1998.[18]

Met die regeling, die voortvloeit uit het in onderlinge samenhang lezen van het thans geldende artikel 18/10 en het ontworpen artikel 18/17/1 van de wet van 30 november 1998, kan aldus blijkbaar voldaan worden aan de vereisten die voortvloeien uit het Europees recht op dat punt.

---

17 Il s'agit de la Commission instituée par l'article 43/1 de la loi du 30 novembre 1998.

18 Selon cette disposition:
"Le dirigeant du service peut, sur avis conforme préalable de la commission, autoriser la prolongation de la méthode exceptionnelle de recueil de données pour une nouvelle période ne pouvant excéder deux mois à compter de l'échéance de la méthode en cours, sans préjudice de l'obligation qui lui est faite de mettre fin à la méthode dès que la menace potentielle qui la justifie a disparu, que la méthode n'est plus utile à la finalité pour laquelle elle a été décidée ou qu'il constate une illégalité. Dans ce cas, le dirigeant du service concerné porte à la connaissance de la commission sa décision motivée de mettre fin à la méthode exceptionnelle.
Une seconde prolongation et toute nouvelle prolongation de la méthode exceptionnelle de recueil de données n'est possible qu'en présence de circonstances particulières nécessitant de prolonger l'utilisation de cette méthode. Ces motifs particuliers sont indiqués dans la décision. Si ces circonstances particulières font défaut, il doit être mis fin à la méthode.

Les conditions prévues aux paragraphes 1er à 3 sont applicables aux modalités de prolongation de la méthode exceptionnelle de recueil de données qui sont prévues dans le présent paragraphe".
Il convient par ailleurs de relever que, selon l'article 18/10, § 1er, de la loi du 30 novembre 1998, "[l]e dirigeant du service met fin à la méthode exceptionnelle lorsque la menace potentielle grave qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dès que possible la [c]ommission de sa décision".

17 Het gaat om de Commissie ingesteld bij artikel 43/1 van de wet van 30 november 1998.

18 Die bepaling luidt als volgt:
"Het diensthoofd kan, op voorafgaand eensluidend advies van de commissie, de verlenging van de uitzonderlijke methode voor het verzamelen van gegevens machtigen voor een nieuwe termijn die niet langer mag zijn dan twee maanden te rekenen vanaf het verstrijken van de lopende methode, onverminderd zijn verplichting om de methode te beëindigen zodra de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd beslist of wanneer hij een onwettigheid vaststelt. In dat geval brengt het diensthoofd van de betrokken dienst zijn met redenen omklede beslissing om de methode te beëindigen ter kennis van de commissie.
Een tweede en elke volgende verlenging van de uitzonderlijke methode voor het verzamelen van gegevens is slechts mogelijk indien er bijzondere omstandigheden aanwezig zijn, die de verlenging van het gebruik van deze methode noodzaken. Deze bijzondere redenen worden in de beslissing opgenomen. Indien deze bijzondere omstandigheden niet voorhanden zijn, dient de methode te worden beëindigd.
De voorwaarden bepaald in de paragrafen 1 tot 3 zijn toepasselijk op de in deze paragraaf bepaalde wijzen van verlenging van de uitzonderlijke methode voor het verzamelen van gegevens."
Bovendien moet opgemerkt worden dat luidens artikel 18/10, § 1, van de wet van 30 november 1998 "[h]et diensthoofd (…) de uitzonderlijke methode [beëindigt] wanneer de ernstige potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie."

2.1.4.1. Par contre, des difficultés se posent à propos de la question de savoir si l'opération envisagée est soumise:

– à "l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération" – selon les termes de la jurisprudence de la Cour européenne des droits de l'homme, spécialement l'arrêt *Big Brother watch*[19];

– à "un contrôle effectif", soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues" – selon les termes de la jurisprudence de la Cour de Justice.

2.1.4.2. Concernant l'arrêt *Big Brother watch*, comme mentionné précédemment, la Cour européenne des droits de l'homme considère que

"l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications".

Elle considère en tout cas que l'exigence d'une autorisation indépendante vaut pour ces deux catégories.

Interrogé à ce propos, les délégués du ministre ont répondu ce qui suit, concernant la portée de la notion de "l'interception et la conservation des données de communication associées":

"Door deze niet afzonderlijk te benoemen, impliceert het Hof volgens […] dat haar conclusie enkel van toepassing is wanneer ook de bulk interceptie van de inhoud van communicatie georganiseerd wordt. Het Hof spreekt zich niet uit over de bewaring van enkel de meta-data, waarbij verondersteld mag worden dat deze maatregel minder intrusief is dan het bewaren van de inhoud van de communicatie.

Minder intrusief, maar nog steeds intrusief. Daarom voorzien we de waarborg van de BIM-commissie die voorafgaandelijk toestemming moet geven in het geval van een ernstige dreiging tegen de nationale veiligheid, of een mechanisme dat in de wet beschreven staat dat ook betrekking heeft op de nationale veiligheid".

Au regard des explications ainsi communiquées, il y a effectivement lieu de constater que l'arrêt *Big Brother watch* ne se prononce pas sur un système qui aurait pour seul objet la conservation de données associées à des contenus de communications électroniques, mais sur un système qui englobait

[19] Voir à ce propos, e.a., Cour.eur.D.H., arrêt *Big Brother watch et autre c. Royaume-Uni*, 25 mai 2021, 350.

2.1.4.1. Er doen zich evenwel moeilijkheden voor in verband met de vraag of de voorgenomen operatie onderworpen is aan:

– "de instemming vanwege een onafhankelijke autoriteit vanaf het begin - zodra de bedoeling en de reikwijdte van de operatie bepaald zijn" – overeenkomstig de rechtspraak van het Europees Hof voor de Rechten van de Mens, in het bijzonder het arrest *Big Brother watch*[19];

– "een effectieve toetsing", hetzij door een rechterlijke instantie, hetzij door een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien" – volgens de bewoordingen van de rechtspraak van het Hof van Justitie.

2.1.4.2. Wat het arrest *Big Brother watch* betreft, heeft het Europees Hof voor de Rechten van de Mens, zoals eerder vermeld, het volgende geoordeeld:

"(…) que l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications."

Het Hof gaat er hoe dan ook van uit dat het vereiste van een onafhankelijke machtiging voor die beide categorieën geldt.

Op een vraag in dat verband hebben de gemachtigden van de minister het volgende geantwoord met betrekking tot de strekking van het begrip "l'interception et la conservation des données de communication associées":

"Door deze niet afzonderlijk te benoemen, impliceert het Hof volgens (…) dat haar conclusie enkel van toepassing is wanneer ook de bulk interceptie van de inhoud van communicatie georganiseerd wordt. Het Hof spreekt zich niet uit over de bewaring van enkel de meta-data, waarbij verondersteld mag worden dat deze maatregel minder intrusief is dan het bewaren van de inhoud van de communicatie.

Minder intrusief, maar nog steeds intrusief. Daarom voorzien we de waarborg van de BIM-commissie die voorafgaandelijk toestemming moet geven in het geval van een ernstige dreiging tegen de nationale veiligheid, of een mechanisme dat in de wet beschreven staat dat ook betrekking heeft op de nationale veiligheid."

In het licht van de aldus verstrekte toelichtingen dient inderdaad vastgesteld te worden dat in het arrest *Big Brother watch* geen uitspraak gedaan wordt over een regeling die louter betrekking zou hebben op de bewaring van gegevens die verband houden met de inhoud van elektronische

[19] Zie in dat verband, onder meer, EHRM, arrest *Big Brother watch e. a. t. Verenigd Koninkrijk*, 25 mei 2021, 350.

l'interception des contenus, des métadonnées, interception qui ne visait pas uniquement le stockage, la conservation de ces données, mais également l'accès à celles-ci et leur analyse[20].

Il apparait donc délicat d'étendre l'enseignement de cet arrêt, spécialement les exigences en matière de contrôle préalable par une juridiction ou un organisme indépendant, au mécanisme de conservation généralisée et indifférenciée envisagée par le texte en projet.

Si toutefois tel devait être le cas, il conviendrait alors de relever qu'il ressort de l'article 18/10, § 1er, de la loi du 30 novembre 1998 que l'avis conforme de la commission sera requis préalablement à la décision du dirigeant du service. La commission vérifiera ainsi "si les dispositions légales relatives à l'utilisation de la méthode exceptionnelle pour le recueil de données, ainsi que les principes de subsidiarité et de proportionnalité prévus à l'article 18/9 § § 2 et 3, sont respectés et qui contrôle les mentions prescrites par le § 2".

Cette commission, dont l'article 43/1, § 1er de la loi du 30 novembre 1998 prévoit qu'elle est composée de magistrats et effectue sa tâche de contrôle en toute indépendance répond à la notion d'"autorité administrative indépendante au sens des jurisprudences rappelées ci-avant. Son avis conforme est contraignant: en vertu de l'article 18/10, § 3, alinéa 2, lorsque son avis est négatif, l'opération envisagée ne peut pas être mise en œuvre.

Il reste que, selon l'article 18/10, § 3, alinéa 3, de la loi du 30 novembre 1998,

"Si la commission ne rend pas d'avis dans le délai de quatre jours ou informe le service concerné qu'elle est dans l'impossibilité de délibérer dans ce délai conformément à l'article 43, paragraphe 1er, alinéa 7, le service concerné peut saisir le ministre compétent, qui autorisera ou n'autorisera pas la mise en œuvre dans les plus brefs délais de la méthode envisagée. Le ministre communique sa décision aux présidents de la commission et du Comité permanent R".

Dans les deux hypothèses énoncées, à défaut d'intervention de la commission, c'est le ministre qui prend la décision d'autoriser l'opération. Or, le ministre ne constitue pas une "autorité administrative indépendante" dont l'intervention serait requise[21].

2.1.4.3. Au regard des missions confiées au Comité permanent R par les articles 43/2 et suivants de la loi du 30 novembre 1998, le système mis en place ne parait pas poser de difficulté par rapport aux exigences de contrôle énoncées par la Cour de Justice.

[20] Voir, sur le système examiné par la Cour européenne des droits de l'homme, les paragraphes 15 à 17 de l'arrêt.

[21] Cour eur. D.H. arrêt du 25 mai 2021, *Big Brother watch et autre c. Royaume-Uni* , 377.

communicaties, maar wel over een regeling betreffende zowel het onderscheppen van de inhoud als de metagegevens, waarbij dat onderscheppen niet alleen betrekking had op de opslag en de bewaring van die gegevens, maar ook op de toegang tot en de analyse van die gegevens.[20]

Het lijkt dan ook een hachelijke zaak de lering van dat arrest, in het bijzonder de vereisten inzake de voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke instelling, ook te laten gelden voor het mechanisme van de algemene en ongedifferentieerde bewaring dat in de ontworpen tekst in het vooruitzicht gesteld wordt.

Indien dat toch het geval zou zijn, dan zou erop gewezen moeten worden dat uit artikel 18/10, § 1, van de wet van 30 november 1998 blijkt dat het diensthoofd zijn beslissing slechts kan nemen op eensluidend advies van de commissie. Zo moet de commissie onderzoeken "of de wettelijke bepalingen voor het aanwenden van de uitzonderlijke methode voor het verzamelen van gegevens, alsook de in artikel 18/9 §§ 2 en 3, bepaalde principes van proportionaliteit en subsidiariteit, zijn nageleefd en (…) de door § 2 voorgeschreven vermeldingen" controleren.

Die commissie, waarvan in artikel 43/1, § 1 van de wet van 30 november 1998 bepaald wordt dat ze samengesteld is uit magistraten en in de uitoefening van haar controleopdrachten volledig onafhankelijk handelt, beantwoordt aan het begrip "onafhankelijke bestuurlijke autoriteit" in de zin van de hiervoor aangehaalde rechtspraak. Haar eensluidend advies is bindend: krachtens artikel 18/10, § 3, tweede lid, mag de geplande operatie niet verricht worden indien haar advies negatief is.

Niettemin luidt artikel 18/10, § 3, derde lid, van de wet van 30 november 1998 als volgt:

"Indien de commissie geen advies uitbrengt binnen de termijn van vier dagen of zij de betrokken dienst meedeelt dat zij niet kan beraadslagen binnen die termijn overeenkomstig artikel 43, § 1, zevende lid, kan de betrokken dienst de bevoegde minister aanzoeken, die al dan niet toelating geeft om zo spoedig mogelijk de beoogde methode uit te voeren. De minister deelt zijn beslissing mee aan de voorzitters van de commissie en van het Vast Comité I."

In beide genoemde gevallen wordt de beslissing om de operatie toe te staan door de minister genomen indien de commissie geen advies uitbrengt. De minister is evenwel geen "onafhankelijke bestuurlijke autoriteit" waarvan de medewerking vereist zou zijn.[21]

2.1.4.3. In het licht van de opdrachten die bij de artikelen 43/2 en volgende van de wet van 30 november 1998 aan het Vast Comité I toevertrouwd worden, lijkt de in te voeren regeling geen moeilijkheden op te leveren in het licht van de door het Hof van Justitie vermelde controlevereisten.

[20] Zie met betrekking tot de door het Europees Hof voor de Rechten van de Mens onderzochte regeling de punten 15 tot en met 17 van dat arrest.

[21] Zie EHRM, arrest van 25 mei 2021, *Big Brother watch e.a. t. Verenigd Koninkrijk*, 377.

2.2. Le dispositif en projet appelle toutefois une observation fondamentale au regard du droit constitutionnel.

La conservation “généralisée et indifférenciée” organisée par l’article 18/17/1, en projet suppose ainsi qu’une injonction soit donnée à tous les opérateurs fournissant des services de communications électroniques. Même si seuls certains opérateurs préalablement identifiés étaient requis de procéder à cette conservation, il n’en reste pas moins qu’un ordre leur serait ainsi donné de conserver les données de trafic et de localisation de manière généralisée et indifférenciée.

Aussi, cette “injonction”, fût-elle limitée dans le temps ne constitue pas un acte administratif à portée individuelle, revêt-elle un caractère général et abstrait, dont les opérateurs sont le medium. Par conséquent, la décision d’imposer cette conservation “généralisée et indifférenciée” est de nature réglementaire.

Concernant l’attribution d’un pouvoir réglementaire à une autorité qui n’est pas responsable politiquement devant les assemblées législatives concernées – c’est-à-dire, à une autorité autre que le Roi agissant sous le contreseing d’un ministre, ou qu’un ministre –, la section de législation a déjà observé à de nombreuses reprises que l’attribution d’une compétence réglementaire à des agents ou à des organismes publics ou à leurs organes est difficilement compatible avec les principes généraux du droit public belge (article 33 et 108 de la Constitution), en ce qu’elle porte atteinte au principe de l’unité du pouvoir réglementaire et échappe à tout contrôle parlementaire direct. Les actes réglementaires de ce type sont en outre dépourvus des garanties dont est assortie la réglementation classique, telles que celles en matière de publication. Si dans le passé, la section de législation a déjà jugé admissibles certaines exceptions à l’interdiction de déléguer une compétence réglementaire à des agents ou des organismes publics, il s’agissait généralement de délégations de portée limitée ou accessoire et d’une technicité telle qu’il pouvait être considéré que les organismes qui devaient appliquer la réglementation concernée, étaient également les mieux placés pour l’élaborer[22].

La décision de principe d’imposer la conservation généralisée et indifférenciée des données de trafics et de localisation de moyens de communications électroniques ne revêt d’évidence pas un caractère limité ou accessoire et n’est pas d’une technicité telle qu’elle pourrait justifier qu’elle soit déléguée aux agents des services de renseignement et de sécurité.

[22] Voir entre autres, à ce propos, l’avis n° 69.160/4 donné le 6 mai 2021 sur un avant-projet de loi “introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G” et l’avis n° 69.166/4 donné le 10 juin 2021 sur un avant-projet de loi “portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques”.

2.2. Het ontworpen dispositief geeft in het licht van het grondwettelijk recht evenwel aanleiding tot een fundamentele opmerking.

Zo veronderstelt de “algemene en ongedifferentieerde” bewaring waarin het ontworpen artikel 18/17/1 voorziet, dat een bevel gegeven wordt aan alle operatoren die diensten voor elektronische communicatie leveren. Zelfs indien slechts bepaalde vooraf aangewezen operatoren verplicht zouden zijn om de gegevens in kwestie te bewaren, zou hen aldus niettemin het bevel gegeven worden om de verkeers- en locatiegegevens op een algemene en ongedifferentieerde wijze te bewaren.

Zelfs indien het om een in de tijd beperkt bevel zou gaan, vormt dergelijk bevel geen bestuurshandeling met individuele strekking, maar is het algemeen en abstract van aard, terwijl het aan de operatoren gericht is. Bijgevolg is de beslissing waarbij die “algemene en ongedifferentieerde” bewaring opgelegd wordt van verordenende aard.

Met betrekking tot het toekennen van een bevoegdheid van verordenende aard aan een overheid die geen politieke verantwoording verschuldigd is aan de betrokken wetgevende vergaderingen – dat wil zeggen aan een andere overheid dan de Koning die handelt met medeondertekening van een minister, of dan een minister – heeft de afdeling Wetgeving in het verleden er al meermaals op gewezen dat het toekennen van een reglementaire bevoegdheid aan ambtenaren of aan openbare instellingen of organen ervan, moeilijk in overeenstemming te brengen valt met de algemene principes van het Belgisch publiekrecht (artikelen 33 en 108 van de Grondwet), aangezien daardoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en ter zake iedere rechtstreekse parlementaire controle ontbreekt. Verordeningen van die aard ontberen daarenboven de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake bekendmaking. Als er in het verleden al uitzonderingen op het delegatieverbod van reglementaire bevoegdheid aan openbare instellingen aanvaardbaar geacht zijn door de afdeling Wetgeving, betrof het doorgaans delegaties met een beperkte draagwijdte of betreffende nevenaspecten en van een zodanig technische aard dat ervan uitgegaan mocht worden dat de instellingen die de betrokken reglementering dienden toe te passen, ook het best geplaatst waren om die reglementering uit te werken.[22]

De principiële beslissing om de algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens van de elektronische communicatiemiddelen op te leggen, is uiteraard geen beslissing met een beperkte draagwijdte of betreffende nevenaspecten en ze is evenmin van een zodanig technische aard dat ze er gegrond redenen bestaan om de bevoegdheid daartoe op te dragen aan personeelsleden van de inlichtingen- en veiligheidsdiensten.

[22] Zie in dat verband, onder andere, advies 69.160/4 d.d. 6 mei 2021 over een voorontwerp van wet ‘tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten’ en advies 69.166/4 d.d. 10 juni 2021 over voorontwerp van wet ‘houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie’.

Sous réserve de l'observation 2.1.4.2 et 2.1.4.3, c'est au Roi qu'il appartient, *in fine*, de prendre une telle décision à portée générale et abstraite.

Le texte en projet sera revu à la lumière de cette observation.

2.3. Le système mis en place par l'avant-projet à l'examen est susceptible d'engendrer une autre hypothèse dans laquelle une conservation généralisée et indifférenciée des métadonnées serait opérée.

Il s'agit du cas prévu à l'article 126/1, § 3, alinéa 1er, 2°, en projet, de la loi du 13 juin 2005, qui permet la conservation des données de communications électroniques, visées au paragraphe 2 du même article, dans toutes les zones dont le niveau de menace, déterminé en vertu de la loi du 10 juillet 2006 'relative à l'analyse de la menace' est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 'portant exécution de la loi 10 juillet 2006 relative à l'analyse de la menace', et aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones.

Cette hypothèse est ainsi réglée, dans l'intention des auteurs de l'avant-projet, non pas au titre des cas de conservation généralisée et indifférenciée des données, mais au titre des situations de conservation ciblée de celles-ci.

Or, le passé récent a montré que le niveau 3 de menace était susceptible d'être atteint sur l'ensemble du territoire national, et ce, le cas échéant, pour une période relativement longue.

Dans l'hypothèse où le niveau 3 de menace serait atteint sur l'ensemble du territoire, le système aboutirait ainsi à une conservation généralisée et indifférenciée des métadonnées. La prudence impose donc de considérer que, pour cette situation spécifique, ce sont les principes relatifs à la conservation généralisée et indifférenciée qui trouvent à s'appliquer, et non ceux relatifs à la conservation ciblée.

Dans la mesure de cette hypothèse spécifique, le système en projet parait répondre aux exigences énoncées plus haut, quant aux finalités de la conservation[23] et à sa limitation dans le temps[24].

Onder voorbehoud van de opmerkingen 2.1.4.2 en 2.1.4.3 staat het uiteindelijk aan de Koning om een dergelijke algemene en abstracte beslissing te nemen.

De ontworpen tekst moet in het licht van deze opmerking herzien worden.

2.3. Het systeem dat bij voorliggend voorontwerp ingevoerd wordt, kan leiden tot een ander geval waarin tot een algemene en ongedifferentieerde bewaring van metagegevens beslist zou worden.

Het gaat om het geval bedoeld in het ontworpen artikel 126/1, § 3, eerste lid, 2°, van de wet van 13 juni 2005, dat voorziet in de bewaring van de gegevens inzake elektronische communicatie, bedoeld in paragraaf 2 van datzelfde artikel, in alle zones waar het algemeen dreigingsniveau, vastgesteld op basis van de wet van 10 juli 2006 'betreffende de analyse van de dreiging', ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang niveau 3 of 4 geldt.

Dat geval wordt aldus, overeenkomstig de bedoeling van de stellers van het voorontwerp, bepaald in het licht van de situaties waarin de gegevens op een gerichte wijze bewaard moeten worden en niet van situaties waarin een algemene en ongedifferentieerde bewaring van gegevens vereist wordt.

Uit het recent verleden is evenwel gebleken dat dreigingsniveau 3 voor het volledige grondgebied van het Rijk kan gelden en dat, in voorkomend geval, zelfs voor een relatief lange periode.

In het geval waarbij dreigingsniveau 3 voor het volledige grondgebied zou gelden, zou dat systeem dus neerkomen op een algemene en ongedifferentieerde bewaring van de metagegevens. Voorzichtigheidshalve moet er dus van uitgegaan worden dat voor deze specifieke situatie de beginselen betreffende de algemene en ongedifferentieerde bewaring toepassing vinden en niet die betreffende de gerichte bewaring.

Wat dat specifieke geval betreft, lijkt de ontworpen regeling te voldoen aan de eerder genoemde vereisten inzake het doel van de gegevensbewaring[23] en de beperking ervan in de tijd.[24]

---

[23] Le dispositif mis en place par la loi du 10 juillet 2006 et par l'arrêté royal du 28 novembre 2006 a vocation à s'appliquer, en première intention, à des menaces qui ont trait à des activités de terrorisme et d'extrémisme (voir l'article 3 de la loi du 10 juillet 2006 et l'article 8, 1°, b) et c) de la loi du 30 novembre 1998). Le niveau 3 de menace correspond à une menace grave, c'est-à-dire "possible et vraisemblable", le niveau 4 de menace correspond à une menace "très grave", c'est-à-dire "sérieuse et imminente", conformément à l'article 11, § 6, de l'arrêté royal du 28 novembre 2006.

[24] Les zones concernées ne font l'objet de l'opération de conservation qu'aussi longtemps qu'elles se trouvent à un niveau 3 ou 4 de menace.

[23] De regeling die bij de wet van 10 juli 2006 en het koninklijk besluit van 28 november 2006 ingevoerd is, is in de eerste plaats bedoeld om te gelden voor bedreigingen die verband houden met terrorisme en extremisme (zie artikel 3 van de wet van 10 juli 2006 en artikel 8, 1°, b) en c) van de wet van 30 november 1998). Overeenkomstig artikel 11, § 6, van het koninklijk besluit van 28 november 2006 stemt dreigingsniveau3 stemt overeen met een "ernstige" bedreiging, namelijk een bedreiging die "mogelijk en waarschijnlijk" is, terwijl dreigingsniveau 4 overeenkomt met een "zeer ernstige" bedreiging, namelijk een bedreiging die "ernstig en zeer nabij" is.

[24] In de betrokken zones is de gegevensbewaring van toepassing zolang daar dreigingsniveau 3 of 4 van kracht is.

Par contre, se pose la question de savoir comment il sera satisfait à l'exigence de "contrôle effectif" au sens des jurisprudences rappelées ci-avant.

Le dispositif en projet sera revu et complété à la lumière de cette observation.

La conservation ciblée des données relatives au trafic et des données de localisation délimitée, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique

1. Pour rappel, selon l'enseignement de l'arrêt *La Quadrature du Net*, est admissible la conservation ciblée des données relatives au trafic et des données de localisation délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique.

2. L'avant-projet à l'examen entend organiser le régime d'une telle conservation par l'insertion d'un article 126/1 nouveau dans la loi du 13 juin 2005.

En substance, cette disposition envisage la conservation de trois catégories de données de trafic et de localisation énumérées en son paragraphe 2 (données d'accès et de connexion, données de communications, données des appels infructueux). Le Roi est chargé de fixer les données à conserver, dans ces trois catégories, ainsi que les exigences auxquelles elles doivent répondre.

3. La conservation a pour finalité, selon la paragraphe 1er, alinéa 3, en projet, la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave, la prévention de menaces graves contre la sécurité publique et la sauvegarde des intérêts vitaux d'une personne physique.

Ces finalités correspondent formellement à celles mentionnées par l'arrêt *La Quadrature du Net*, à l'exception de "la sauvegarde des intérêts vitaux d'une personne physique". Toutefois, concernant cette finalité, il y a lieu de constater qu'elle relève d'un autre contexte que celui des questions préjudicielles auxquelles la Cour de Justice a répondu dans son arrêt *La Quadrature du Net*.

En tout état de cause, une telle finalité peut, à priori, être considérée comme relevant de la sauvegarde de la sécurité publique et des obligations positives incombant à ce titre aux États membres, en vue de garantir la vie et la sécurité des personnes.

Au regard des finalités de conservation, l'article 126/1 en projet n'apparait dès lors pas poser des difficultés au

De vraag rijst evenwel op welke manier voldaan zal worden aan het vereiste van de "effectieve toetsing" in de zin van de hiervoor aangehaalde rechtspraak.

De ontworpen tekst moet in het licht van die opmerking herzien en aangevuld worden.

De afgebakende en gerichte bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid

1. Er wordt aan herinnerd dat volgens de lering van het arrest *La Quadrature du Net* een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren afgebakend wordt aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die verlengd kan worden, aanvaard kan worden ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid.

2. Voorliggend voorontwerp strekt ertoe een dergelijke bewaring te regelen door in de wet van 13 juni 2005 een nieuw artikel 126/1 in te voegen.

In essentie voorziet die bepaling in de bewaring van drie categorieën verkeers- en locatiegegevens die opgesomd worden in paragraaf 2 (de gegevens met betrekking tot de toegang en de verbinding, de communicatiegegevens en de gegevens van oproeppogingen zonder resultaat). De Koning wordt ermee belast te bepalen welke gegevens van die drie categorieën bewaard moeten worden en aan welke vereisten die gegevens moeten beantwoorden.

3. Naar luid van de ontworpen paragraaf 1, derde lid, van dat artikel worden die gegevens bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

Die doeleinden stemmen uitdrukkelijk overeen met die vermeld in het arrest *La Quadrature du Net*, met uitzondering van "de bescherming van de vitale belangen van een natuurlijke persoon". Wat dat doeleinde betreft, valt evenwel op te merken dat het deel uitmaakt van een andere context dan die van de prejudiciële vragen waarop het Hof van Justitie geantwoord heeft in zijn arrest *La Quadrature du Net*.

Een dergelijk doeleinde kan hoe dan ook *a priori* geacht worden te vallen onder de bescherming van de openbare veiligheid en onder de positieve verplichtingen die in dat verband op de lidstaten rusten ter bescherming van het leven en de veiligheid van personen.

Wat het doeleinde van de bewaring betreft, lijkt het ontworpen artikel 126/1 derhalve geen moeilijkheden op te leveren

regard de la jurisprudence de la Cour de Justice et de la Cour constitutionnelle.

4.1.1. Le ciblage de la conservation concernée repose sur l'établissement de différentes catégories de zones géographiques, qui sont énumérées par le paragraphe 3 de la disposition en projet, à savoir:

1° les arrondissements judiciaires dans lesquels au moins trois infractions par mille habitants, parmi celles énumérées à l'article 90*ter* du Code d'instruction criminelle, ont été constatées durant l'année, sur une moyenne des trois années précédant celle en cours, ainsi que les zones de police présentant les mêmes caractéristiques et situées dans les arrondissements judiciaires qui ne répondent pas aux conditions précitées;

2° les zones dont le niveau de la menace, déterminé en vertu de la loi du 10 juillet 2006 est au moins de niveau 3, et aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones;

3° les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave; sont mentionnés dans cette catégorie les ports, les gares, les stations de métro et de pré-métro, les bâtiments affectés à différents services comme la justice, la police locale et fédérale, les douanes et accises; sont également visés les communes dans lesquelles se trouvent des domaines militaires, les prisons et les maisons de transition, les armuriers et stands de tir, les établissements visés par la réglementation en matière de protection contre les radiations ionisantes, les établissements "Seveso", les communes comportant une ou plusieurs infrastructures critiques, le réseau ASTRID, ainsi que les réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de services essentiels;

4° les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population; sont mentionnés à ce titre les zones neutres et les cabinets ministériels, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et de la Défense et approuvée par le Conseil national de sécurité, les autoroutes et les parkings publics attenant, les assemblées législatives, les maisons communales et les hôtels de ville, les sièges des conseils provinciaux, le palais royal, les domaines royaux, les bâtiments affectés à différents services comme la justice, la police locale et fédérale, la sûreté de l'État; sont également visés les communes dans lesquelles se trouvent des domaines militaires, et les communes frontalières, les hôpitaux et la Banque Nationale de Belgique;

5° les zones où il y a une menace grave potentielle pour les intérêts des institutions internationales; sont mentionnés à ce titre les ambassades et représentations diplomatiques, les bâtiments affectés à l'Union européenne, et à l'OTAN, les

in het licht van de rechtspraak van het Hof van Justitie en het Grondwettelijk Hof.

4.1.1. Het richten van de betrokken bewaring steunt op het bepalen van verschillende categorieën van geografische zones die opgesomd worden in paragraaf 3 van het ontworpen artikel, namelijk:

1° de gerechtelijke arrondissementen waar gemiddeld minstens drie strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per duizend inwoners per jaar vastgesteld zijn tijdens de drie jaren voorafgaand aan het lopende jaar, alsook de politiezones die dezelfde kenmerken vertonen maar gelegen zijn in een gerechtelijk arrondissement dat niet aan de voormelde voorwaarden voldoet;

2° de zones waar het dreigingsniveau, vastgesteld krachtens de wet van 10 juli 2006 ten minste niveau 3 is, en zolang in die zones ten minste dreigingsniveau 3 blijft bestaan;

3° de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit; als tot die categorie behorend worden vermeld de havens, de spoorwegstations, de metro– en de pre-metrostations, de gebouwen bestemd voor allerlei diensten, zoals justitie, de lokale en de federale politie en douane en accijnzen; eveneens vermeld worden de gemeenten waar zich militaire domeinen bevinden, de gevangenissen en de transitiehuizen, de wapenkamers en schietstanden, de faciliteiten bedoeld in de regelgeving inzake de bescherming tegen ioniserende stralingen, de SEVESO-inrichtingen, de gemeenten waar zich kritieke infrastructuren bevinden, het ASTRID-netwerk, alsook de informatienetwerken en – systemen ter ondersteuning van het verlenen van essentiële diensten door operatoren van essentiële diensten;

4° de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking; in dat verband worden vermeld de neutrale zones en de ministeriële kabinetten, de gebouwen die bestemd zijn voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden en die opgenomen zijn in een lijst die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst opgesteld wordt op voorstel van de minister van Justitie en Defensie en door de Nationale Veiligheidsraad goedgekeurd wordt, de autosnelwegen en de bijhorende openbare parkeerterreinen, de wetgevende vergaderingen, de gemeentehuizen, de zetels van de provincieraden, het koninklijk paleis, de koninklijke domeinen, de gebouwen bestemd voor allerlei diensten zoals justitie, de lokale en de federale politie, alsook voor de Veiligheid van de Staat; eveneens vermeld worden de gemeenten waar zich militaire domeinen bevinden, de grensgemeenten, de ziekenhuizen en de Nationale Bank van België;

5° de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de internationale instellingen; in dat verband wordt melding gemaakt van de ambassades en diplomatieke vertegenwoordigingen, de gebouwen bestemd

bureaux des institutions de l'Espace économique européen et les bureaux des Nations-Unies.

Les autorités compétentes dans l'une des matières en relation avec l'objet de la zone sont chargées de transmettre chaque année, à la date et au service déterminés par le Roi, les informations nécessaires à la détermination concrète des zones géographiques. Elles sont également tenues d'informer sans délai ce service lorsqu'une zone ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation. La liste des zones est mise à jour chaque année, et mise à la disposition, selon le cas, du Comité permanent R par les services de renseignement et de sécurité, ou de l'Organe de contrôle de l'information policière.

4.1.2. Pour les zones relevant des catégories citées aux points 3°, 4° et 5°, ci-avant, il est prévu que, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre en charge des communications électroniques, et après avis des Autorités de protection des données compétentes et de l'Institut belge des services postaux et des télécommunications (ci-après "l'Institut"), le Roi peut fixer d'autres zones, par un arrêté qui doit être renouvelé tous les trois ans. À défaut de renouvellement, l'obligation de conservation dans les zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'une éventuel nouvel arrêté royal.

Il est également prévu que

"Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves".

4.1.3. Par ailleurs, le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre en charge de communications électroniques, et après avis des Autorités de protection des données compétentes et de l'Institut, les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées, la liste des différentes autorités compétentes dans les matières concernées, les modalités de communication des informations par les autorités compétentes vers le service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation pour la zone concernée.

voor de Europese Unie en voor de NAVO, de kantoren van de instellingen van de Europese Economische Ruimte en de kantoren van de Verenigde Naties.

De autoriteiten die bevoegd zijn voor een van de aangelegenheden in verband met de bestemming van de zone worden ermee belast jaarlijks op de door de Koning vastgestelde datum aan de door de Koning aangewezen dienst de gegevens mee te delen die nodig zijn voor de concrete vaststelling van de geografische zones. Wanneer een geografische zone niet langer aan bedoeld criterium voldoet, zijn die autoriteiten er tevens toe gehouden deze dienst daarvan onverwijld in kennis stellen, zodat de verplichting tot bewaring zo spoedig mogelijk beëindigd kan worden. De lijst van de zones wordt elk jaar bijgewerkt en naar gelang van het geval ter beschikking gesteld van het Vast Comité I, door de inlichtingen- en veiligheidsdiensten, of van het Controleorgaan van de politionele informatie.

4.1.2. Voor de zones die behoren tot een van de categorieën die vermeld worden in de hiervoor geciteerde punten 3°, 4° en 5° wordt bepaald dat, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister bevoegd voor de elektronische communicatie, na raadpleging van de bevoegde gegevensbeschermingsautoriteiten en van het Belgisch Instituut voor postdiensten en telecommunicatie (hierna "het Instituut"), door de Koning bijkomende zones bepaald kunnen worden, met dien verstande dat dit besluit om de drie jaar hernieuwd moet worden. Indien dat besluit binnen die termijn niet hernieuwd wordt, vervalt de verplichting tot bewaring wat de bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.

Voorts wordt nog het volgende bepaald:

"Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit."

4.1.3. Bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister bevoegd voor elektronische communicatie, na raadpleging van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, kan de Koning bovendien bepalen welke technische parameters en gegevens de operatoren dienen te gebruiken om de gegevensopslag tot de bedoelde zones te beperken, de lijst opstellen van de verschillende autoriteiten die bevoegd zijn voor de aangelegenheden in kwestie, de procedures bepalen voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst en de procedures voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de bewaring voor de betrokken zone ten uitvoer leggen.

4.1.4. Un rapport d'évaluation annuel est établi, qui est adressé à la Chambre des représentants et à l'Organe de contrôle de l'information policière. Par contre, s'agissant de la transparence administrative et de l'information du public, l'article 126/1, § 3, dernier alinéa, en projet, prévoit:

"La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 aout 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1er, point 1°".

4.1.5. De manière concrète, les opérateurs seront tenus de conserver les données pour toutes les communications effectuées à partir de l'une des zones précitées, ou vers cette zone. Les seules données d'un utilisateur final qui seront conservées sont celles traitées ou générées lorsqu'il se trouve dans la zone concernée.

Toutefois, il est prévu que

"[l]orsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques".

4.2.1. Le système ainsi mis en place pose question sur différents points.

4.2.2. Tout d'abord, comme le relève le commentaire de l'article, dans son arrêt *La Quadrature du net*, la Cour de Justice a considéré que la conservation ciblée de données pouvait se fonder sur des critères géographiques

"lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave.[…] Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages"[25].

Il y a lieu de constater que les auteurs de l'avant-projet se sont efforcés, dans le choix des zones retenues, de se limiter à la mise en œuvre des critères mentionnés par la Cour de Justice.

Il faut également constater que le commentaire de l'article entend justifier les raisons pour lesquelles, au regard des

[25] Paragraphe 150 de l'arrêt.

4.1.4. Dienaangaande wordt jaarlijks een evaluatieverslag opgesteld dat gericht wordt aan de Kamer van volksvertegenwoordigers en aan het Controleorgaan op de politionele informatie. Met betrekking tot de administratieve transparantie en de informatie van het publiek wordt in het ontworpen artikel 126/1, § 3, laatste lid, daarentegen het volgende bepaald:

"De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°."

4.1.5. Concreet zullen de operatoren gehouden zijn tot het bewaren van de gegevens voor alle communicaties die vanuit of naar een van de voornoemde zones gevoerd worden. Van een eindgebruiker zullen alleen die gegevens bewaard worden die verwerkt of gegenereerd zijn wanneer hij zich in de betrokken zone bevond.

Hoe dan ook wordt in dat verband het volgende bepaald:

"Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden."

4.2.1. Het aldus ingevoerde systeem doet op een aantal punten vragen rijzen.

4.2.2. In de eerste plaats heeft het Hof van Justitie, zoals in de bespreking van dit artikel gesteld wordt, in zijn arrest *La Quadrature du Net* geoordeeld dat voor de gerichte bewaring van gegevens gesteund kan worden op geografische criteria

"wanneer de bevoegde nationale autoriteiten op basis van objectieve [en niet- discriminatoire] factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (…). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones."[25]

Op te merken valt dat de stellers van het voorontwerp bij de keuze van de in aanmerking genomen zones getracht hebben om zich te beperken tot de tenuitvoerlegging van de criteria die door het Hof van Justitie vermeld zijn.

Tevens moet opgemerkt worden dat in de bespreking van dit artikel getracht wordt de redenen op te geven waarom, in het

[25] Randnummer 150 van dat arrest.

critères ainsi mis en œuvre, chaque type de zone pouvait et devait être inclus dans l'énumération retenue.

Il reste toutefois que, d'une part, le nombre et la variété des zones ainsi énumérées sont considérables, et que, d'autre part, leur addition aboutit à couvrir une partie assez importante du territoire.

Pour certaines zones, la qualification de "lieu caractérisé par un nombre élevé d'actes de criminalité grave", ou de "lieu particulièrement exposés à la commission d'actes de criminalité grave, en tant que fréquenté par un nombre très élevé de personnes", ou encore de "lieu stratégique", n'apparait pas évidente.

Il en va ainsi, à titre d'exemples, des maisons de transition visées à la loi du 17 mai 2006 'relative au statut juridique externe des personnes condamnées à une peine privative de liberté et aux droits reconnus à la victime dans le cadre des modalités d'exécution de la peine', des autoroutes dans leur ensemble, des maisons communales et hôtels de ville ou encore des sièges des conseils provinciaux.

Aussi, la section de législation ne peut-elle que prendre acte des justifications déjà données, et inviter les auteurs de l'avant-projet à justifier plus avant encore le choix des zones retenues. À défaut de justification claire, précise et spécifique pour chaque type de zone, le texte en projet sera entaché d'un aléa lié à la question de savoir si le régime de conservation envisagé se limite effectivement au "strict nécessaire".

L'énumération des zones envisagées sera réexaminée en conséquence.

4.2.3. La question se pose de savoir par quelle autorité le périmètre de chaque zone sera délimité, étant entendu que la précision de ce périmètre et sa limitation au strict nécessaire sont requises au regard de l'arrêt *La Quadrature du Net*.

Ainsi, dans le système prévu par le texte en projet, l'autorité compétente dans la matière en rapport avec l'objet de la zone sera chargée de transmettre chaque année au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques. Elle devra également informer sans délai le même service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis un terme le plus rapidement possible à la conservation des données[26].

[26] La section de législation suppose qu'il s'agit, par exemple, d'hypothèses où des arrondissements judiciaires ou des zones de police ne présenteraient plus lors d'une nouvelle année, le taux de criminalité minimum requis pour être classés comme zone de conservation, ou bien lorsqu'un bâtiment affecté à un usage qui justifie son classement dans une zone de conservation serait affecté à un autre usage qui ne le justifierait plus.

licht van de aldus ten uitvoer gelegde criteria, elk type zone in uiteindelijke opsomming opgenomen kon en moest worden.

Zulks neemt evenwel niet weg dat aldus een aanzienlijk aantal en een aanzienlijke verscheidenheid aan zones opgesomd worden, enerzijds, en dat, anderzijds, als men die zaken samen beschouwt, een vrij groot deel van het grondgebied gedekt wordt.

Voor bepaalde zones lijkt het niet voor de hand te liggen of ze al dan niet bestempeld kunnen worden als "plek waar veel zware criminaliteit plaatsvindt", als "plaats waar er een verhoogd risico is op zware misdrijven, doordat ze regelmatig door een zeer groot aantal personen bezocht worden", of nog als "strategische plek".

Dat is het geval met, bijvoorbeeld, de transitiehuizen bedoeld in de wet van 17 mei 2006 'betreffende de externe rechtspositie van de veroordeelden tot een vrijheidsstraf en de aan het slachtoffer toegekende rechten in het raam van de strafuitvoeringsmodaliteiten', de autosnelwegen in hun geheel, de gemeentehuizen of nog de zetels van de provincieraden.

De afdeling Wetgeving kan bijgevolg alleen maar akte nemen van de redenen die reeds opgegeven zijn en de stellers van het voorontwerp verzoeken de keuze van de betrokken zones nog nader te motiveren. Indien er voor elk type zone geen duidelijke, precieze en specifieke redenen opgegeven worden, zal met betrekking tot de ontworpen tekst onzekerheid blijven bestaan over de vraag of de voorgenomen regeling inzake bewaring tot het "strikt noodzakelijke" beperkt blijft.

De lijst van de betrokken zones moet bijgevolg opnieuw onderzocht worden.

4.2.3. De vraag rijst welke autoriteit verantwoordelijk is voor de afbakening van de omvang van elke zone, aangezien die omvang nauwkeurig bepaald en tot het strikt noodzakelijke ingeperkt moet worden in het licht van het arrest *La Quadrature du Net*.

Zo zal, volgens het systeem waarin de ontworpen tekst voorziet, de autoriteit bevoegd voor de aangelegenheid die verband houdt met de bestemming van de zone ermee belast worden jaarlijks aan de door de Koning aangewezen dienst de gegevens mee te delen die nodig zijn voor de concrete bepaling van de geografische zones. Wanneer een geografische zone niet langer aan bedoeld criterium voldoet, zal die autoriteit die dienst daarvan eveneens onverwijld in kennis moeten stellen, zodat de verplichting tot bewaring van de gegevens zo spoedig mogelijk beëindigd kan worden.[26]

[26] De afdeling Wetgeving gaat ervan uit dat het daarbij bijvoorbeeld gaat om gevallen waarbij in gerechtelijke arrondissementen of politiezones bij aanvang van een nieuw jaar niet meer de minimale criminaliteitscijfers gehaald zouden worden die vereist zijn om als bewaringszone beschouwd te worden, of gevallen waarin een gebouw bestemd voor een welbepaald gebruik op grond waarvan het beschouwd wordt als een bewaringszone, bestemd wordt voor een ander gebruik waardoor de reden om het aldus te beschouwen zou komen te vervallen.

Par ailleurs, il est prévu que chaque année, et chaque fois qu'il est informé d'une modification, le service désigné par le Roi met à jour la liste des zones géographiques de conservation.

Le dispositif en projet reste toutefois en défaut de définir les critères concrets et techniques à prendre en compte pour définir le périmètre de la zone, de manière telle que les zones relevant d'une même catégorie soient définies selon la même méthodologie[27]. La section de législation n'aperçoit pas non plus quelle autorité sera chargée de la définition du périmètre proprement dit, ou de sa modification. Il est uniquement prévu, à cet égard, que le service désigné par le Roi met à jour la liste des zones, annuellement et "chaque fois qu'il est informé d'une modification", ce qui suppose, s'agissant de la modification de la liste, que le pouvoir de décision revient aux autorités compétentes en la matière concernée par la zone, autorités dont le Roi peut arrêter la liste, sans y être toutefois tenu.

Or, dès lors que la définition des périmètres des zones ainsi que leur inscription sur la liste ou leur retrait de celle-ci, conditionnent l'obligation imposée aux opérateurs de conserver les données y afférentes, l'ensemble de ces décisions doivent être adoptées ou à tout le moins approuvées par une autorité unique, aux fins d'assurer le respect du principe d'égalité, spécialement entre les personnes susceptibles de voir leurs données conservées. Par ailleurs, ces actes constituent des actes à portée générale et abstraite dans leurs effets; ils sont donc de nature réglementaire et ne peuvent être adoptés que par une autorité responsable politiquement devant le Parlement, à savoir, s'agissant de l'autorité fédérale, le Roi[28-29].

4.2.4. L'article 126/1, § 5, en projet, habilite le Roi, pour les trois catégories de zones prévues à l'article 126/1, § 3, alinéa 1er, 3°, 4° et 5°, en projet, à fixer des "zones additionnelles".

Les critères qui doivent être en mis en œuvre par le Roi ne sont pas précisés.

Certes, le paragraphe 6 en projet prévoit:

"Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et

Voorts wordt bepaald dat de door de Koning aangewezen dienst elk jaar en telkens wanneer hij van een wijziging in kennis gesteld wordt, de lijst bijwerkt van de geografische gebieden waar de gegevens bewaard moeten worden.

In het ontworpen dispositief wordt evenwel niets voorgeschreven inzake de concrete en technische criteria die in aanmerking genomen moeten worden om de omvang van de zone te bepalen opdat de zones die tot eenzelfde categorie behoren volgens dezelfde methodologie bepaald zouden worden.[27] Het is de afdeling Wetgeving evenmin duidelijk welke overheid bevoegd is voor het bepalen van de omvang op zich of voor de wijziging ervan. In dat verband wordt alleen bepaald dat de door de Koning aangewezen dienst de lijst van de zones elk jaar en "telkens wanneer hij van een wijziging in kennis wordt gesteld" bijwerkt, wat veronderstelt dat inzake de wijziging van de lijst de beslissingsbevoegdheid toekomt aan de instanties die bevoegd zijn voor de aangelegenheid waarvoor die zone bestemd is, terwijl de Koning de lijst van die instanties kan vaststellen, maar Hij daartoe niet verplicht is.

Doordat het bepalen van de omvang van de zones en het opnemen van zones op de lijst of het schrappen van zones van de lijst van doorslaggevend belang zijn voor de verplichting die aan de operatoren opgelegd wordt om de daarmee verband houdende gegevens te bewaren, moeten al die beslissingen dan ook genomen, of op zijn minst goedgekeurd worden door één enkele overheid, om ervoor te zorgen dat het gelijkheidsbeginsel in acht genomen wordt, in het bijzonder wat betreft de personen wier gegevens bewaard zouden kunnen worden. Het gaat daarbij bovendien om handelingen met een algemene strekking en abstracte gevolgen; het gaat dus om verordenende handelingen die alleen gesteld mogen worden door een overheid die politieke verantwoording verschuldigd is aan het Parlement, namelijk de Koning, aangezien het *in casu* om de federale overheid gaat.[28-29]

4.2.4. Bij het ontworpen artikel 126/1, § 5, wordt de Koning ertoe gemachtigd met betrekking tot de drie categorieën van zones waarvan in het ontworpen artikel 126/1, § 3, eerste lid, 3°, 4° en 5°, sprake is de "bijkomende geografische zones" te bepalen.

Er wordt evenwel niet nader bepaald aan welke criteria de Koning daarbij uitvoering dient te geven.

De ontworpen paragraaf 6 luidt weliswaar als volgt:

"De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité voor Inlichtingen

27 Ainsi, il ne serait pas admissible, à titre d'exemple, que la zone contenant une maison communale, une ambassade ou un hôpital, comporte également les abords directs du bâtiment, alors que la zone contenant un autre maison communale, une autre ambassade ou un autre hôpital se limiterait strictement au bâtiment concerné.

28 Le cas échéant, à condition que la méthode de calcul ait été préalablement fixée par le législateur ou par le Roi, il pourrait être envisager de charger un ou plusieurs ministres de cette détermination.

29 Voir, en un sens similaire, l'avis n° 69.160/4 donné le 6 mai 2021.

27 Zo zou bijvoorbeeld niet aanvaard kunnen worden dat in de ene zone waarin een gemeentehuis, een ambassade of een ziekenhuis gelegen is ook de onmiddellijke omgeving tot die zone gerekend worden, terwijl in een andere zone waarin een gemeentehuis, een ambassade of een ziekenhuis gelegen is alleen het betrokken gebouw daartoe gerekend zou worden.

28 In voorkomend geval en mits de berekeningsmethode vooraf door de wetgever of door de koning vastgesteld is, zouden één of meer ministers ermee belast kunnen worden die zones vast te stellen.

29 Zie in dezelfde zin, advies 69.160/4, gegeven op 6 mei 2021.

de la Sécurité, et de l'Institut et des autorités de protection des données compétentes, un rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 5, afin de vérifier si des dispositions doivent être adaptées.

Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 5 répondent toujours aux critères visés au paragraphe 3, alinéa 1er, points 3° à 5° et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.

Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.

[…]".

La portée des principes définis par l'alinéa 3 de cette disposition n'apparait toutefois pas clairement.

La section de législation se demande ainsi si ces principes s'appliqueront de manière contraignante au Roi, lors de la mise en œuvre de l'habilitation qui Lui est conférée en vue d'ajouter des types de zones dans les trois catégories précitées, ou s'il s'agit d'une invitation faite au législateur futur, invitation qui, par hypothèse ne saurait le contraindre.

En tout état de cause, le principe de légalité attaché à l'article 22 de la Constitution impose que l'habilitation conférée au Roi soit encadrée de manière suffisante et que, par conséquent, le texte en projet soit rédigé de manière telle que les principes énoncés à l'article 126/1, § 6, alinéa 3, en projet s'imposent à Lui sans ambiguïté.

À cet égard, il ressort des explications communiquées par les délégués du ministre que, lorsque le Roi mettra en œuvre l'habilitation concernée, Il sera tenu de s'inscrire dans les critères énoncés *in limine* des dispositions qui prévoient les trois catégories de zones concernées. Ainsi, à titre d'exemple, s'il est envisagé d'ajouter une zone à la catégorie prévue au paragraphe 3, alinéa 1er, 5°, en projet, le Roi devra être en mesure de justifier l'ajout au regard de l'existence d' "une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national". Ce mécanisme a ainsi vocation à encadrer l'habilitation conférée au Roi.

4.2.5. Le dernier alinéa du paragraphe 3 de la disposition en projet est rédigé comme suit:

"La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 aout 2006 relative à l'accès du public

en Veiligheid, en van het Instituut en de bevoegde gegevensbeschermingsautoriteiten, jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 5 bedoelde Koninklijk Besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 5, bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in paragraaf 3, eerste lid, punten 3° tot 5° of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit.

(…)."

De strekking van de beginselen die vastgelegd worden in het derde lid van die bepaling is evenwel niet helemaal duidelijk.

Zo vraagt de afdeling Wetgeving zich af of die beginselen voor de Koning bindend zullen zijn, wanneer uitvoering gegeven wordt aan de machtiging die aan Hem verleend wordt met het oog op de toevoeging van bepaalde types zones aan de drie voornoemde categorieën, dan wel of het gaat om een aan de toekomstige wetgever gericht verzoek, dat per definitie voor Hem niet bindend zou kunnen zijn.

Hoe dan ook impliceert het legaliteitsbeginsel dat verbonden is aan artikel 22 van de Grondwet, dat de machtiging die aan de Koning verleend wordt nauwkeurig genoeg afgebakend moet worden en dat de ontworpen tekst bijgevolg aldus gesteld moet worden dat de beginselen die in het ontworpen artikel 126/1, § 6, derde lid, vervat zijn op ondubbelzinnige wijze voor Hem gelden.

In dat verband volgt uit de uitleg van de gemachtigden van de minister dat, wanneer de Koning aan de betrokken machtiging uitvoering zal geven, Hij de criteria in acht zal moeten nemen die vermeld worden *in limine* van de bepalingen die in de drie betrokken categorieën zones voorzien. Zo zal, bij wijze van voorbeeld, wanneer overwogen wordt om een zone toe te voegen aan de categorie waarvan in de ontworpen paragraaf 3, eerste lid, 5°, sprake is, de Koning die toevoeging moeten kunnen verantwoorden in het licht van het bestaan van "een mogelijk ernstige bedreiging (…) voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen". Deze regeling is aldus bedoeld om de aan de Koning verleende machtiging af te bakenen.

4.2.5. Het laatste lid van paragraaf 3 van de ontworpen artikel luidt als volgt:

"De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de

à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1er point 1°".

4.2.5.1. La disposition en projet rend ainsi inapplicable la loi du 11 avril 1994 'relative à la publicité de l'administration', et ce, de manière extrêmement générale, aux "informations, documents ou données, sous quelque forme que ce soit, visés [à l'article 126/1, en projet]".

Sur ce point[30], il y a lieu d'avoir égard à l'article 32 de la Constitution qui dispose:

"Chacun a le droit de consulter chaque document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134".

Si l'article 32 de la Constitution habilite le législateur concerné à prévoir des cas dans lesquels le droit de consulter chaque document administratif et de s'en faire remettre copie ne s'applique pas, les exceptions ainsi mises en place doivent, dans le respect des principes d'égalité et de non-discrimination, poursuivre un but légitime et demeurer proportionnées au but légitime poursuivi.

La loi du 11 avril 1994, qui organise le régime général d'accès aux documents administratifs, prévoit déjà des exceptions à l'accès à certains documents. Ainsi, l'article 6, § 1er, de cette loi dispose que l'autorité administrative rejette la demande de consultation, d'explication ou de communication sous la forme de copie d'un document administratif si elle a constaté que l'intérêt de la publicité ne l'emporte pas notamment sur la protection de la sécurité de la population ou de l'ordre public, ou encore, la sûreté ou la défense nationales. Cette disposition organise un système de refus au cas par cas de l'accès à un document administratif ou de la communication d'une copie de ce document, sans instituer un régime général d'interdiction à priori d'accès à une catégorie spécifique de documents ou de limitation à priori de l'accès d'un document déterminé à telles catégories de personnes.

Un tel système de décision individuelle à posteriori permet de garantir la protection de la sécurité publique, de l'ordre public, et de la sureté et de la défense nationales.

Un tel régime d'actes à portée individuelle susceptibles de recours, *in fine*, auprès de la section du contentieux administratif du Conseil d'État, est ainsi de nature à garantir la proportionnalité des restrictions apportées au droit d'accès aux documents administratifs.

[30] Pour des observations similaires, voir, *mutatis mutandis*, l'avis n° 69.160/4.

toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°."

4.2.5.1. Bij de ontworpen bepaling wordt de wet van 11 april 1994 'betreffende de openbaarheid van bestuur' aldus op uiterst algemene wijze niet-toepasselijk verklaard op "de informatie, documenten of gegevens, in welke vorm ook, bedoeld in [het ontworpen artikel 126/1]".

In dat verband[30] dient rekening gehouden te worden met artikel 32 van de Grondwet, dat als volgt luidt:

"Ieder heeft het recht elk bestuursdocument te raadplegen en er een afschrift van te krijgen, behoudens in de gevallen en onder de voorwaarden bepaald door de wet, het decreet of de regel bedoeld in artikel 134."

Hoewel de betrokken wetgever er bij artikel 32 van de Grondwet toe gemachtigd wordt te bepalen in welke gevallen het recht om elk bestuursdocument te raadplegen en daarvan een afschrift te krijgen niet geldt, moet met de uitzonderingen die aldus gemaakt worden, met inachtneming van het gelijkheidsbeginsel en het beginsel van niet-discriminatie een legitiem doel nagestreefd worden en moeten ze proportioneel blijven ten opzichte van het legitiem doel dat aldus nagestreefd wordt.

De wet van 11 april 1994 die de algemene regeling inzake de toegang tot bestuursdocumenten bevat, voorziet reeds in uitzonderingen op de toegang tot bepaalde documenten. Zo wordt in artikel 6, § 1, van die wet bepaald dat de administratieve overheid de vraag om inzage in, uitleg over of mededeling van een afschrift van een bestuursdocument afwijst, wanneer zij vastgesteld heeft dat het belang van de openbaarheid niet opweegt tegen de bescherming van onder andere de veiligheid van de bevolking of de openbare orde, of nog de veiligheid of de verdediging van het land. Bij die bepaling wordt een systeem ingesteld in het kader waarvan de toegang tot een bestuursdocument of de afgifte van een afschrift van dat document geval per geval geweigerd kan worden, maar wordt geen algemene regeling ingevoerd volgens welke het *a priori* verboden zou zijn toegang te verlenen tot een specifieke categorie documenten of volgens welke de toegang tot een welbepaald document *a priori* tot deze of gene categorie personen beperkt zou kunnen worden.

Met een dergelijk systeem van *a posteriori* te nemen individuele beslissingen kan ervoor gezorgd worden dat de openbare veiligheid, de openbare orde en de veiligheid en de verdediging van het land beschermd worden.

Een degelijke regeling, in het kader waarvan handelingen met individuele strekking gesteld kunnen worden waartegen in laatste instantie bij de afdeling Bestuursrechtspraak van de Raad van State beroep ingesteld kan worden, is aldus van dien aard dat daarmee de proportionaliteit gegarandeerd kan worden van de beperkingen die aan het recht op toegang tot bestuursdocumenten opgelegd worden.

[30] Voor soortgelijke opmerkingen zie, *mutatis mutandis*, advies 69.160/4.

Pour sa part, le texte en projet restreint de manière radicale le droit à la transparence administrative en ce qui concerne, de manière tout-à-fait générale, tous les “informations, documents ou données, sous quelque forme que ce soit, visés [à l’article 126/1, en projet]”.

Il appartient aux auteurs de l’avant-projet d’être en mesure de démontrer que la différence de traitement qu’institue le dispositif à l’examen entre les personnes qui se trouvent à priori exclues de toute possibilité de prendre connaissance de la liste des zones sensibles, et les personnes qui souhaitent prendre connaissance d’autres documents administratifs sensibles sur le plan de la sécurité publique, de l’ordre public, et de la sûreté et de la défense nationales, auxquelles s’applique le système mis en place par la loi du 11 avril 1994, spécialement son article 6, repose sur une justification objective et raisonnable rendant cette différence de traitement conforme aux principes d’égalité et de non-discrimination[31].

En tout état de cause, il convient que le régime en projet demeure conforme au principe de proportionnalité. À ce propos, l’exclusion du champ d’application de la loi du 11 avril 1994 de tous les “informations, documents ou données, sous quelque forme que ce soit, visés [à l’article 126/1, en projet], à l’exception des statistiques de criminalité visées à l’alinéa 1er point 1°, de l’article” apparait excessive dans la généralité de ses termes. Il conviendrait ainsi de limiter l’exclusion envisagée aux catégories d’informations, documents ou données pour lesquelles le régime dérogatoire se justifie effectivement.

4.2.5.2. Dans la mesure où elle entend déroger à la loi du 5 aout 2006 ‘relative à l’accès du public à l’information en matière d’environnement’, la disposition en projet appellerait en principe, *mutatis mutandis*, les mêmes observations que celles formulées au point précédent.

Toutefois, il convient de ne pas perdre de vue que cette loi a pour objet la transposition de la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 ‘concernant l’accès du public à l’information en matière d’environnement et abrogeant la directive 90/313/CEE du Conseil’.

Au regard du système organisé par les articles 3 et 4 de la directive, qui ne s’applique certes qu’aux informations environnementales, telles que définies en son article 2, 1°, seules des dérogations au cas par cas à l’obligation de communication, sont admissibles. Ces dérogations peuvent reposer notamment sur la nécessité de garantir la sécurité publique ou la défense nationale[32], mais aucun régime général d’exclusion à priori ne peut être organisé. La disposition à l’examen ne peut dès lors être admise dans la mesure où elle prévoit que la loi du 5 aout 2006 est inapplicable aux informations, documents et données concernées qui constituent des informations environnementales au sens de la directive.

4.2.5.3. La disposition à l’examen sera revue à la lumière des observations qui précèdent.

31 Voir C.C., 19 décembre 2013, n° 169/2013.
32 Article 4, paragraphe 2, de la directive.

De ontworpen tekst beperkt, daarentegen, op radicale wijze het recht op bestuurlijke transparantie met betrekking tot werkelijk alle “de informatie, documenten of gegevens, in welke vorm ook, bedoeld in [het ontworpen artikel 126/1]”.

De stellers van het voorontwerp moeten kunnen aantonen dat de verschillende behandeling die bij voorliggend dispositief ingevoerd wordt tussen degenen voor wie het *a priori* volstrekt niet mogelijk is om van de lijst met de gevoelige zones kennis te nemen en degenen die kennis wensen te nemen van andere gevoelige bestuursdocumenten op het stuk van de openbare veiligheid, de openbare orde en de veiligheid en de verdediging van het land, die vallen onder de regeling die ingevoerd is bij de wet van 11 april 1994, en in het bijzonder bij de artikel 6 van die wet, op een redelijke en objectieve verantwoording berust zodat die verschillende behandeling conform het gelijkheidsbeginsel en het niet-discriminatiebeginsel is.[31]

Hoe dan ook dient de ontworpen regeling in overeenstemming te blijven met het evenredigheidsbeginsel. Het feit dat de wet van 11 april 1994 niet van toepassing is op “de informatie, documenten of gegevens, in welke vorm ook, bedoeld in [het ontworpen artikel 126/1], met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°” van dat artikel, lijkt overdreven wegens de zeer algemene bewoordingen waarin die bepaling gesteld is. Het verdient derhalve aanbeveling om de voorgenomen uitsluiting te beperken tot de categorieën van informatie, documenten of gegevens waarvoor die afwijkende regeling daadwerkelijk verantwoord is.

4.2.5.2. Voor zover de ontworpen bepaling voorziet in een afwijking van de wet van 5 augustus 2006 ‘betreffende de toegang van het publiek tot milieu-informatie’ dienen in dat verband in principe, *mutatis mutandis*, dezelfde opmerkingen geformuleerd te worden als die welke in het vorige punt gemaakt zijn.

Er mag evenwel niet uit het oog verloren worden dat die wet strekt tot omzetting van richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 ‘inzake de toegang van het publiek tot milieu-informatie en tot intrekking van richtlijn 90/313/EEG van de Raad’.

In het licht van het systeem dat ingevoerd is bij de artikelen 3 en 4 van die richtlijn, dat weliswaar alleen geldt voor “milieu-informatie”, zoals gedefinieerd in artikel 2, 1°, van die richtlijn, kunnen afwijkingen van de mededelingsplicht alleen aanvaard worden als ze geval per geval toegestaan worden. Die afwijkingen kunnen inzonderheid ingegeven zijn door de noodzaak om de openbare veiligheid of nationale defensie[32] te garanderen, maar in een algemene regeling van voorafgaande uitsluiting mag niet voorzien worden.

4.2.5.3. De voorliggende bepaling moet in het licht van de voorgaande opmerkingen worden herzien.

31 Zie GwH 19 december 2013, nr. 169/2013.
32 Artikel 4, lid 2, van de richtlijn.

4.3.1. Comme mentionné ci-avant, la disposition en projet prévoit:

"Chaque autorité compétente dans l'une des matières visées aux paragraphe 3, alinéa 1er, 1° à 5°, transmet chaque année à la date déterminée par le Roi et au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques".

Par ailleurs, ces autorités sont tenues d'informer sans délai ce service "lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée au paragraphe 1er dans cette zone".

Enfin le Roi peut – sans donc y être tenu – établir la liste des différentes autorités concernées.

Dans la mesure où l'objet de zones de conservation relèverait de matières qui sont de la compétences des Communautés et des Régions[33], cette disposition présente une difficulté: elle impose de manière unilatérale des obligations à ces niveaux de pouvoir, qui sont soumis ainsi à ces obligations, non pas uniquement au titre d'une matière qui relève de la compétence fédérale, mais précisément, en raison de leurs compétences propres dans leurs matières[34-35].

Un mécanisme de collaboration qui implique l'intervention des Communautés et des Régions, ou d'organes relevant de celles-ci, en raison de leurs compétences propres, doit faire l'objet d'une coopération au sens de l'article 92*bis*, de la loi spéciale du 8 aout 1980 'de réformes institutionnelles'. Un autre biais pourrait consister à créer un organe de décision ou consultatif au sein duquel les Communautés et les Régions seraient représentées, conformément à l'article 92*ter* de la même loi spéciale.

À ce propos, s'il est vrai que dans la matière des communications électroniques, la Cour constitutionnelle et la section de législation ont déjà admis que d'autres formes de coopération, tel un accord du comité de concertation sur la

33 À titre d'exemple, il en va ainsi, fût-ce en partie, des ports, aéroports, stations de métro et pré-métro, communes, et conseils provinciaux et des hôpitaux.

34 Ainsi, le mécanisme prévu par la disposition en projet ne peut être comparé, par exemple, à la situation dans laquelle se trouve l'administration d'une Communauté ou d'une Région, qui est tenue au respect de la législation fédérale en matière de bien-être au travail, ce en sa qualité d'employeur.

35 *Mutatis mutandis*, dans son avis n° 37.295/4 donné le 28 juin 2004 sur un avant-projet devenu la loi du 13 juin 2005 'relative aux communications électroniques', *http://www.raadvst-consetat.be/dbx/avis/37295.pdf*, la section de législation a observé:

"L'autonomie respective des communautés et des régions s'oppose en effet à ce que l'État fédéral ou une entité fédérée décide unilatéralement d'associer les autorités d'autres entités fédérale ou fédérées à l'exercice de ses propres compétences. Seule une loi adoptée à la majorité spéciale ou un accord de coopération pourrait imposer une telle concertation".

4.3.1. Zoals hierboven is aangegeven, stelt de ontworpen bepaling het volgende:

"Elke autoriteit die bevoegd is voor een van de in de punten 1 tot en met 5 bedoelde aangelegenheden deelt jaarlijks op de door de Koning vastgestelde datum aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de operationele tenuitvoerlegging van dit lid."

Die autoriteiten zijn voorts gehouden die dienst onverwijld in te lichten "wanneer een geografische zone niet langer aan het bedoelde criterium voldoet, (…) zodat de verplichting tot bewaring bedoeld in paragraaf 1 in deze zone zo spoedig mogelijk kan worden beëindigd".

Ten slotte kan de Koning – maar hij is daartoe dus niet verplicht – een lijst opstellen van de verschillende autoriteiten in kwestie.

In zoverre in zones gegevens worden bewaard die inhoudelijk aangelegenheden zouden betreffen waarvoor de gemeenschappen en de gewesten bevoegd zijn,[33] is deze bepaling problematisch: ze legt eenzijdig verplichtingen op aan die bevoegdheidsniveaus, voor wie die verplichtingen dus gelden, niet alleen in het kader van een aangelegenheid die onder federale bevoegdheid valt, maar precies op grond van hun eigen bevoegdheden inzake hun aangelegenheden.[34-35]

Een samenwerkingsregeling die inhoudt dat de gemeenschappen en de gewesten, of organen die daaronder ressorteren, op grond van hun eigen bevoegdheden optreden, moet het voorwerp uitmaken van een samenwerking in de zin van artikel 92*bis* van de bijzondere wet van 8 augustus 1980 'tot hervorming der instellingen'. Een andere werkwijze zou erin kunnen bestaan dat een beslissings- of raadgevend orgaan wordt opgericht waarin de gemeenschappen en de gewesten vertegenwoordigd zouden zijn, overeenkomstig artikel 92*ter* van dezelfde bijzondere wet.

Weliswaar hebben het Grondwettelijk Hof en de afdeling Wetgeving inzake elektronische communicatie reeds andere vormen van samenwerking toelaatbaar geacht, zoals een overeenkomst van het overlegcomité betreffende de wetgeving

33 Dat geldt bijvoorbeeld, zij het gedeeltelijk, voor de havens, luchthavens, metro- en pre-metrostations, gemeenten, provincieraden en ziekenhuizen.

34 Zo kan de regeling waarin de ontworpen bepaling voorziet, niet worden vergeleken met bijvoorbeeld de situatie waarin de administratie van een gemeenschap of een gewest zich bevindt, die als werkgever de federale wetgeving inzake welzijn op het werk dient na te leven.

35 *Mutatis mutandis* heeft de afdeling Wetgeving het volgende opgemerkt in advies 37.295/4, op 28 juni 2004 gegeven over een voorontwerp dat heeft geleid tot de wet van 13 juni 2005 'betreffende de elektronische communicatie', *http://www.raadvst-consetat.be/dbx/adviezen/37295.pdf*:
"De autonomie van respectievelijk de gemeenschappen en de gewesten staat er immers aan in de weg dat de Federale Staat of een deelentiteit eenzijdig zouden beslissen de instanties van andere deelentiteiten of van de Federale Staat te betrekken bij de uitoefening van zijn of haar bevoegdheden. Alleen een wet aangenomen met een bijzondere meerderheid of een samenwerkingsakkoord zou zulk een overleg kunnen opleggen."

législation concernée, pouvaient être admises, ce n'est que dans la mesure où, compte tenu des compétences résiduelles de l'autorité fédérale en matière de communications électroniques et des compétences d'attribution des Communautés en matière d'aspects de contenu et techniques des services de médias audiovisuels et sonores, il convenait que les infrastructures concernées soient "réglées en coopération entre l'État fédéral et les Communautés, afin de faire en sorte que ces autorités harmonisent leurs normes respectives et pour éviter que cette infrastructure et ces services soient soumis à des dispositions contradictoires"[36-37].

Tel n'est pas le cas de l'avant-projet à l'examen: il ne s'agit pas d'éviter des contradictions entre deux législations relevant chacune de la compétence de niveaux de pouvoir différents, mais, le cas échéant, pour l'autorité fédérale d'imposer, au titre de ses compétences propres, des obligations à d'autres niveaux de pouvoir, en raison de leurs compétences propres.

Par conséquent, il ne peut être garanti que l'accord du Comité de concertation sur le texte en projet s'avère suffisant, en l'espèce, au titre de mécanisme de coopération.

En tout état de cause, il ressort du dossier communiqué à la section de législation que, concernant l'avant-projet à l'examen, la concertation organisée a eu lieu sur la base de l'accord de coopération du 17 novembre 2006 entre l'État fédéral, la Communauté flamande, la Communauté française et la Communauté germanophone 'relatif à la consultation mutuelle lors de l'élaboration d'une législation en matière de réseaux de communications électroniques, lors de l'échange d'informations et lors de l'exercice des compétences en matière de réseaux de communications électroniques par les autorités de régulation en charge des télécommunications ou de la radiodiffusion et la télévision'. Les Régions n'ont dès lors pas participé à celle-ci.

5. Quant à la durée de conservation, l'article 126/1, § 1er, en projet, prévoit que les données visées au paragraphe 2 doivent être conservées pendant douze mois à partir de la communication, sauf si une autre durée est fixée dans le même article.

in kwestie. Maar gelet op de residuaire bevoegdheden van de federale overheid inzake elektronische communicatie en gelet op de toegewezen bevoegdheden van de gemeenschappen inzake inhoudelijke en technische aspecten van de audiovisuele en auditieve mediadiensten, geldt dit enkel in zoverre de betrokken infrastructuren "in samenwerking tussen de Federale Staat en de gemeenschappen moe[s]ten worden geregeld, teneinde te bewerkstelligen dat die overheden hun respectieve normen op elkaar afstemmen en om te vermijden dat die infrastructuur en die diensten aan tegenstrijdige bepalingen worden onderworpen".[36-37]

Dat is niet het geval met het voorliggende voorontwerp: het gaat niet om het voorkomen van tegenstrijdigheden tussen twee wetgevingen die elk tot een ander bevoegdheidsniveau behoren, maar, in voorkomend geval, om het feit dat de federale overheid, op basis van haar eigen bevoegdheden, verplichtingen voorschrijft aan andere bevoegdheidsniveaus op grond van hun eigen bevoegdheden.

Bijgevolg kan niet worden gegarandeerd dat de instemming van het overlegcomité met de ontworpen tekst *in casu* toereikend is als samenwerkingsregeling.

Hoe dan ook volgt uit het dossier dat aan de afdeling Wetgeving is bezorgd, dat het georganiseerde overleg in verband met het voorliggende voorontwerp heeft plaatsgehad op basis van het samenwerkingsakkoord van 17 november 2006 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franstalige Gemeenschap en de Duitstalige Gemeenschap 'betreffende het wederzijds consulteren bij het opstellen van regelgeving inzake elektronische communicatienetwerken, het uitwisselen van informatie en de uitoefening van de bevoegdheden met betrekking tot elektronische communicatienetwerken door de regulerende instanties bevoegd voor telecommunicatie of radio-omroep en televisie'. De gewesten waren bijgevolg geen partij bij dat samenwerkingsakkoord.

5. Wat betreft de duur van de bewaring bepaalt het ontworpen artikel 126/1, § 1, dat de in paragraaf 2 bedoelde gegevens gedurende twaalf maanden moeten worden bewaard, te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in hetzelfde artikel.

---

36 C.C. , 8 novembre 2006, n° 163/2006, B.4; voir également C.C. , 14 juillet 2004, n° 132/2004, B.6.1., rédigé en ces termes:
"Sur la base de l'article 92*bis* de la loi spéciale du 8 aout 1980 de réformes institutionnelles, l'État, les communautés et les régions peuvent conclure des accords de coopération qui portent notamment sur la création et la gestion conjointes de services et institutions communs, sur l'exercice conjoint de compétences propres, ou sur le développement d'initiatives en commun. Ils disposent en outre d'autres instruments en vue de donner forme à leur coopération".

37 Voir spécialement l'avis n° 42.495/4 le 19 mars 2007 sur un avant-projet devenu le décret de la Communauté française du 2 juillet 2007 'remplaçant les articles 81 à 83 et 90 à 98 du décret du 27 février 2003 sur la radiodiffusion', annulés par la Cour constitutionnelle le 8 novembre 2006, *http://www.raadvst-consetat.be/dbx/avis/42495.pdf*.

36 GwH 8 november 2006, nr. 163/2006, B.4; zie ook GwH 14 juli 2004, nr. 132/2004,B.6.1., dat als volgt luidt:
"Op grond van artikel 92*bis* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen kunnen de Staat, de gemeenschappen en de gewesten samenwerkingsakkoorden sluiten die onder meer betrekking hebben op de gezamenlijke oprichting en het gezamenlijk beheer van gemeenschappelijke diensten en instellingen, op de gezamenlijke uitoefening van eigen bevoegdheden of op de gemeenschappelijke ontwikkeling van initiatieven. Daarnaast beschikken ze over andere instrumenten om hun samenwerking gestalte te geven."

37 Zie in het bijzonder advies 42.495/4, op 19 maart 2007 gegeven over een voorontwerp dat heeft geleid tot het decreet van de Franse Gemeenschap van 2 juli 2007 'tot vervanging van de artikelen 81 tot 83 en 90 tot 98 van het decreet van 27 februari 2003 betreffende de radio-omroep, vernietigd door het Arbitragehof op 8 november 2006', *http://www.raadvst-consetat.be/dbx/adviezen/42495.pdf*.

Les autres durées prévues à l'article 126/1, en projet, sont à l'exception de celles prévues au paragraphe 3, 1°, alinéa 2, c), et alinéa 3, c), toutes inférieures à douze mois. Il s'agit des durées de six et, neuf mois prévues au paragraphe 3, 1°, alinéa 2, a) et b), et alinéa 3, a) et b),en fonction du taux de criminalité décelé dans la zone concernée.

Il n'apparait pas, à priori, que ces durées de conservation poseraient des difficultés particulières, d'autant que celles prévues au paragraphe 3, 1°, alinéas 2 et 3, précité entendent garantir la proportionnalité de la conservation au regard de l'importance de la criminalité dans l'arrondissement judiciaire ou la zone de police considérés.

6.1. La dernière condition mise à l'opération de conservation ici envisagée, selon l'enseignement de l'arrêt *La Quadrature du Net*, réside dans le caractère temporellement limité au strict nécessaire, de l'opération.

Le point 151 de l'arrêt exprime plus clairement cette exigence en ces termes:

"Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation".

Semble ainsi visée non pas tant la durée de conservation des données, que la durée de la période au cours de laquelle les données doivent être stockées en vue de leur conservation[38].

6.2. Dans le système mis en place par l'article 126/1 en projet, il n'est pas prévu de limiter les opérations de conservation dans les différentes zones envisagées, moyennant une éventuelle prolongation.

La raison en est que la plupart des zones retenues se fondent sur la présence de bâtiments ou installations affectés à certaines fonctions dont les auteurs de l'avant-projet considèrent qu'ils présentent, en raison de la nature-même de ces fonctions, un risque spécifique au regard des objectifs poursuivis. En d'autres termes, dans l'intention des auteurs de l'avant-projet, aussi longtemps que les bâtiments et installations sont affectés à ces fonctions, la nécessité de la conservation des données se justifie. Le même raisonnement vaut pour les zones définies en fonction du niveau de menace, où les auteurs de l'avant-projet considèrent la conservation nécessaire aussi longtemps que la menace est au minimum de niveau 3. Il en va de même pour les zones définies en fonction du taux de criminalité, aussi longtemps que le taux est atteint.

[38] Comparer avec l'article 39*quinquies*, en projet, du Code d'instruction criminelle (article 17 de l'avant-projet).

De andere bewaringstermijnen waarin het ontworpen artikel 126/1 voorziet, zijn allemaal korter dan twaalf maanden, met uitzondering van de termijnen bepaald in paragraaf 3, 1°, tweede lid, c), en derde lid, c). Het gaat om termijnen van zes en negen maanden, bepaald in paragraaf 3, 1°, tweede lid, a) en b), en derde lid, a) en b), afhankelijk van het aantal strafbare feiten in de betreffende zone.

A priori lijken die bewaringstermijnen geen bijzondere moeilijkheden op te leveren, nog des te minder daar de termijnen bepaald in de voornoemde paragraaf 3, 1°, tweede en derde lid, de evenredigheid van de bewaring willen garanderen ten aanzien van de omvang van de criminaliteit in het gerechtelijk arrondissement of de politiezone in kwestie.

6.1. De laatste voorwaarde die volgens de lering van het arrest *La Quadrature du Net* voor de hier beoogde bewaringsverrichting wordt opgelegd, is dat die verrichting in de tijd wordt beperkt tot wat strikt noodzakelijk is.

Punt 151 van het arrest verwoordt dat vereiste duidelijker aldus:

"Om ervoor te zorgen dat de inmenging die in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan."

Hier lijkt niet zozeer de termijn van de gegevensbewaring te worden bedoeld, als wel de duur van de periode waarin de gegevens met het oog op hun bewaring moeten worden opgeslagen.[38]

6.2. In de regeling die bij het ontworpen artikel 126/1 wordt ingevoerd, wordt niet voorzien in een beperking van de bewaringsverrichtingen in de verschillende bedoelde zones, mits een eventuele verlenging van de maatregelen.

De reden daarvoor is dat de meeste zones in kwestie gebaseerd zijn op de aanwezigheid van gebouwen of installaties bestemd voor bepaalde functies, die volgens de stellers van het voorontwerp, vanwege de aard zelf van die functies, een specifiek risico inhouden ten aanzien van de nagestreefde doelstellingen. Met andere woorden: de stellers van het voorontwerp beogen te bepalen dat de noodzaak om de gegevens te bewaren gerechtvaardigd is zolang de gebouwen en installaties bestemd zijn voor die functies. Dezelfde redenering geldt voor de zones die zijn gedefinieerd op basis van het dreigingsniveau: daar beschouwen de stellers van het voorontwerp de bewaring als noodzakelijk zolang de dreiging ten minste op niveau 3 ligt. Hetzelfde geldt voor de zones die zijn gedefinieerd op basis van het aantal strafbare feiten, zolang dat aantal bereikt is.

[38] Vergelijk met het ontworpen artikel 39*quinquies* van het Wetboek van Strafvordering (artikel 17 van het voorontwerp).

Par ailleurs, aux fins de limiter les opérations de conservation au strict nécessaire, chaque autorité compétente pour la matière concernée par la zone est tenue d'informer sans délai le service désigné par le Roi de ce que la zone concernée ne répond plus au critère qui classe celle-ci dans les zones de conservation. Ce service est en outre chargé d'actualiser la liste des zones chaque année et chaque fois qu'il est informé d'une modification par l'une des autorités compétentes. Enfin, un rapport annuel est présenté à la Chambre des représentants, qui examine en particulier si les catégories de zones géographiques énumérées dans la loi ou l'arrêté visé au paragraphe 5 de la disposition en projet répondent toujours aux critères en lien avec les objectifs poursuivis et s'il est nécessaire de les maintenir ou si d'autres zones doivent être incluses.

Ces mécanismes visent à garantir qu'aucun périmètre initialement soumis au régime de l'article 126/1 en projet n'y sera maintenu que dans la mesure de ce qui est strictement nécessaire aux finalités concernées.

Si la section de législation comprend la logique du système mis en place, il ne peut toutefois être garanti que celui-ci répond intégralement à la condition exprimée au point 151 de l'arrêt *La Quadrature du Net*.

Ainsi, ce point laisse à penser qu'il est attendu que le mécanisme repose sur une limitation temporelle à priori, moyennant renouvellement éventuel, tandis que le mécanisme en projet se fonde lui sur une opération durable, non limitée dans le temps, à laquelle il est mis fin, en principe, dès que la nécessité ne la justifie plus.

7.1. Enfin, la disposition à l'examen appelle des observations plus ponctuelles.

7.2. Certaines des zones énumérées se concilient difficilement avec cette notion, qui implique la détermination d'un périmètre géographique. Il en va ainsi du réseau utilisé par ASTRID, et des réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de services essentiels, visés à l'article 126/1, § 3, 3°, o) et p), en projet.

Le texte en projet gagnerait à être complété aux fins de mieux cerner la définition géographique de ces réseaux.

De même, les zones "dont le niveau de la menace, déterminé en vertu de la loi du 10 juillet 2006 relative à l'analyse de la menace est au moins de niveau 3, et aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones" sont délicates à déterminer. En effet, selon l'article 11, § 6, de l'arrêté royal du 28 novembre 2006, le niveau de menace est déterminé au regard d'une personne, d'un groupement, ou d'un événement: dès lors qu'elle concerne une personne ou un groupement limité, la définition du niveau de menace ne se prête pas nécessairement à une localisation géographique. La section

Om de bewaringsverrichtingen tot het strikt noodzakelijke te beperken, is elke overheid die voor de betreffende aangelegenheid bevoegd is, voorts verplicht de door de Koning aangewezen dienst er onverwijld van in kennis te stellen dat de zone in kwestie niet meer beantwoordt aan het criterium dat haar tot een zone maakt waar gegevens worden bewaard. Die dienst is bovendien belast met het bijwerken van de lijst van de zones, wat ze jaarlijks, alsook telkens wanneer een bevoegde overheid haar in kennis stelt van een wijziging, moet doen. Ten slotte moet een jaarverslag aan de Kamer van volksvertegenwoordigers worden voorgelegd, waarin met name wordt onderzocht of de categorieën van geografische zones die worden opgesomd in de wet of in het besluit waarvan in paragraaf 5 van de ontworpen bepaling sprake is, nog altijd beantwoorden aan de criteria in verband met de nagestreefde doelstellingen, en of die categorieën moeten worden gehandhaafd dan wel of er andere zones in moeten worden opgenomen.

Met die regelingen wil men garanderen dat geen enkele perimeter die aanvankelijk onder het bepaalde van het ontworpen artikel 126/1 viel, als dusdanig wordt gehandhaafd indien dat niet strikt noodzakelijk is voor de betreffende doelstellingen.

De afdeling Wetgeving begrijpt weliswaar de logica van de ingevoerde regeling, maar toch kan niet worden gegarandeerd dat die regeling volledig in overeenstemming is met de voorwaarde die in punt 151 van het arrest *La Quadrature du Net* wordt gesteld.

Zo wekt dat punt 151 de indruk dat de regeling berust op een beperking in de tijd *a priori*, met eventueel een verlenging, terwijl de ontworpen regeling van haar kant op een duurzame verrichting zonder tijdsbeperking steunt, waaraan in principe een einde wordt gemaakt zodra die regeling niet meer door enige noodzaak wordt gerechtvaardigd.

7.1. Ten slotte dienen over de voorliggende bepaling de volgende specifieke opmerkingen te worden gemaakt.

7.2. Sommige vermelde zones zijn moeilijk verenigbaar met het begrip "zone", dat de vaststelling van een geografische perimeter inhoudt. Dat geldt bijvoorbeeld voor het netwerk waarvan ASTRID gebruikmaakt en voor de informatienetwerken en -systemen die de verlening van essentiële diensten van operatoren van essentiële diensten ondersteunen, bedoeld in het ontworpen artikel 126/1, § 3, 3°, o) en p).

De ontworpen tekst zou beter worden aangevuld zodat die netwerken geografisch duidelijker worden afgebakend.

Evenzo valt moeilijk te bepalen welke de zones zijn "waar het algemene dreigingsniveau, vastgesteld [krachtens] de wet van 10 juli 2006 betreffende de dreigingsanalyse, ten minste niveau 3 bedraagt, (…) en zolang niveau 3 blijft bestaan". Volgens artikel 11, § 6, van het koninklijk besluit van 28 november 2006 wordt het dreigingsniveau immers vastgesteld ten aanzien van een persoon, groepering of gebeurtenis: in zoverre de vaststelling van het dreigingsniveau betrekking heeft op een persoon of een beperkte groepering, kan ze niet altijd geografisch worden gelokaliseerd. De afdeling Wetgeving

de législation suppose dès lors que le système en projet ne concerne que les cas où la menace est localisable au sein d'une aire géographique, ce que le texte en projet devrait prévoit expressément.

7.3. Les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du titre III de la Constitution, les communes dans lesquelles se trouvent les domaines militaires et les bâtiments affectés à la police fédérale ou à la police locale sont repris au titre de zones de conservation, d'une part, au paragraphe 3, 3°, respectivement e), h) et f), en projet, comme zones "particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave") et, d'autre part, au 4°, d), respectivement vi), vii) et viii), en projet, "pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, décrets ou les ordonnances".

La section de législation n'aperçoit pas la logique et l'utilité qu'il y a à inclure ces types de zones dans deux catégories différentes, ce qui prête par ailleurs à confusion. La question se pose de savoir si ce doublon ne trouve pas sa cause dans une erreur.

7.4. La disposition en projet n'envisage pas et ne règle pas la situation, qui ne saurait être exclue, dans laquelle, en raison des matières pour lesquelles elles sont compétentes, plusieurs autorités au sens des paragraphes 3 et 5, de la disposition en projet, seraient compétentes pour un même type de zone.

7.5. Dans la catégorie des zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, figurent "les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la [Sécurité] sur proposition du ministre de la Justice et de la Défense et approuvée par le Conseil national de sécurité".

Selon le commentaire de l'article, ce type de zone renvoie en réalité, d'une part, aux missions du service de la Sûreté de l'État, qui, selon l'article 7, 1°, de la loi du 30 novembre 1998, a pour mission, notamment

"de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace […] le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité".

D'autre part, il est renvoyé à l'article 11, § 1er, 1°, c), de la même loi, qui confie au Service Général du Renseignement et de la Sécurité notamment la mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer

veronderstelt dan ook dat de ontworpen regeling alleen gaat over de gevallen waarin de dreiging lokaliseerbaar is in een geografisch gebied; dat zou expliciet moeten worden bepaald in de ontworpen tekst.

7.3. De gebouwen bestemd voor de instellingen bedoeld in de hoofdstukken 5 tot 7 van titel III van de Grondwet, de gemeenten waarin zich militaire domeinen bevinden en de gebouwen bestemd voor de federale of de lokale politie, worden opgenomen in de lijst van zones waarbinnen gegevens worden bewaard, enerzijds in de ontworpen paragraaf 3, 3°, respectievelijk e), h) en f), als zones "die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit", en anderzijds in het ontworpen punt 4°, d), respectievelijk vi), vii) en viii, "voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties".

De afdeling Wetgeving begrijpt de logica noch het nut van het feit dat die types van zones in die twee verschillende categorieën worden ondergebracht; dat leidt trouwens tot onduidelijkheid. De vraag rijst of die overlapping niet aan een vergissing te wijten is.

7.4. Het valt niet uit te sluiten dat zich een situatie voordoet waarin verschillende overheden in de zin van de paragrafen 3 en 5 van de ontworpen bepaling, op grond van de aangelegenheden waarvoor ze bevoegd zijn, voor eenzelfde soort zone bevoegd zouden zijn. Die situatie komt in het ontwerp niet ter sprake en wordt er niet in geregeld.

7.5. In de categorie van zones waar een mogelijke ernstige bedreiging bestaat voor de vitale belangen van de natie of voor de essentiële behoeften van de bevolking, bevinden zich "de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden die zijn opgenomen in een lijst die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst wordt opgesteld op voorstel van de minister van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad".

Volgens de commentaar op dat artikel verwijst dat soort zone in werkelijkheid enerzijds naar de opdrachten van de Veiligheid van de Staat, die volgens artikel 7, 1°, van de wet van 30 november 1998 onder meer de volgende opdracht heeft:

"het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die (…) het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen."

Anderzijds wordt verwezen naar artikel 11, § 1, 1°, c), van dezelfde wet, dat de Algemene Dienst Inlichting en Veiligheid met name opdraagt inlichtingen in te winnen, te analyseren en te verwerken die betrekking hebben op elke activiteit die een bedreiging vormt of zou kunnen vormen voor

"le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense".

Au regard de cette précision, la section de législation constate que la disposition à l'examen mentionne une liste "établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et de la Défense et approuvée par le Conseil national de sécurité". S'agissant de l'atteinte au potentiel économique et scientifique, l'article 7, 1°, de la loi du 30 novembre 1998, qui a trait à la Sûreté de l'État, ne prévoit pas l'établissement d'une telle liste par ce service, tandis que l'article 11, § 1er, 1°, c), de la même loi, prévoit que le Service Général du Renseignement et de la Sécurité établira, lui, une liste, dans des conditions similaires à celles prévues par la disposition à l'examen, mais qui ne visent que les secteurs économiques et industriels liés à la Défense.

Aux fins d'éviter l'élaboration de plusieurs listes, qui le cas échéant, pourraient comporter des doublons ou se contredire, il appartient aux auteurs de l'avant-projet de revoir l'ensemble des dispositions précitées aux fins d'assurer la cohérence entre celles-ci, dans la mesure où elles concernent la protection du potentiel économique et scientifique sur le territoire national et l'élaboration de liste(s) y relative(s).

7.6. L'article 126/1, § 3, en projet, mentionne, à de multiples reprises, "les infractions visées à l'article 90*ter*, du Code d'instruction criminelle". Dans un souci de transparence et de sécurité juridique, il s'indiquerait de renvoyer de manière plus précise à celles des subdivisions de l'article concerné qui mentionnent les infractions dont question.

8. En conclusion, l'article 126/1 en projet sera réexaminé et revu à la lumière des observations qui précèdent.

La conservation généralisée et indifférenciée des adresses IP attribuées à la source aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique

1. L'article 7 de l'avant-projet entend remplacer la totalité de l'article 126 de la loi du 13 juin 2005, de sorte qu'il disposerait comme suit:

"§ 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données de souscription de l'abonné ainsi que les données techniques qui sont nécessaires pour

"het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst."

In het licht van die precisering stelt de afdeling Wetgeving vast dat de voorliggende bepaling melding maakt van een lijst "die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst wordt opgesteld op voorstel van de minister van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad". In verband met de aantasting van het economische en wetenschappelijke potentieel bepaalt artikel 7, 1°, van de wet van 30 november 1998, dat over de Veiligheid van de Staat gaat, niet dat die dienst een dergelijke lijst moet opstellen, terwijl artikel 11, § 1, 1°, c), van dezelfde wet bepaalt dat de Algemene Dienst Inlichting en Veiligheid van zijn kant een lijst opstelt, in soortgelijke omstandigheden als die waarin de voorliggende bepaling voorziet, maar die alleen betrekking hebben op de economische en industriële sectoren die met Defensie verband houden.

De stellers van het voorontwerp dienen alle voornoemde bepalingen te herzien om te voorkomen dat verschillende lijsten worden gemaakt, die in voorkomend geval elkaar zouden kunnen overlappen of tegenspreken, en om die bepalingen samenhangend te maken in zoverre ze betrekking hebben op de bescherming van het economische en wetenschappelijke potentieel op het nationale grondgebied en over de uitwerking van de daarmee verband houdende lijst(en).

7.6. In het ontworpen artikel 126/1, § 3, wordt meermalen melding gemaakt van "inbreuken (…) zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering". Omwille van de transparantie en de rechtszekerheid zou nauwkeuriger moeten worden verwezen naar de onderverdelingen van het betreffende artikel waarin van de "inbreuken" in kwestie sprake is.

8. Als besluit kan worden gesteld dat het ontworpen artikel 126/1 in het licht van de voorgaande opmerkingen opnieuw moet worden onderzocht en moet worden herzien.

Algemene en ongedifferentieerde bewaring van IP-adressen die zijn toegewezen aan de bron, ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid

1. Artikel 7 van het voorontwerp beoogt heel artikel 126 van de wet van 13 juni 2005 te vervangen, zodat dat als volgt zou luiden:

"§ 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken leveren, de abonnementsgegevens van de abonnee alsook de technische gegevens die noodzakelijk zijn om de

identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, pour autant qu'ils traitent ou génèrent ces données dans le cadre de la fourniture des réseaux ou services de communications concernés.

Le présent article ne porte pas sur le contenu des communications.

Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1.

Les données visées au présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Par dérogation à l'alinéa 3, les adresses IP dynamiques, autres que celle qui a été utilisée pour souscrire au service, sont conservées jusqu'à douze mois après la fin de la session.

§ 2. Le Roi fixe après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver ainsi que les exigences auxquelles ces données doivent répondre".

Le commentaire de l'article justifie cette disposition comme suit:

"Pour mettre en œuvre l'arrêt de la Cour constitutionnelle du 22 avril 2021 et l'arrêt Quadrature du Net de la Cour de Justice de l'Union européenne, ne sont plus visées par l'obligation de conservation que les données de souscription et les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique (tels que l'identifiant créé pour chaque communication). Le présent article est applicable lorsqu'un service de communications électroniques est fourni en Belgique.

La durée de conservation de 12 mois a été maintenue, dès lors que cette durée correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave.

Une distinction est effectuée entre l'adresse IP utilisée pour souscrire au service et les autres adresses IP. En effet, l'adresse IP utilisée pour souscrire au service est une donnée qui doit être conservée par l'opérateur dans le cadre de l'article 127, afin de pouvoir établir ou vérifier l'identité de l'abonné.

Les données de souscription comprennent entre autres le numéro de téléphone, l'adresse email, le numéro d'abonné, la date de début et de fin de la souscription. Le Conseil d'État français, qui a été amené à examiner la législation française en matière de conservation de données de trafic pour les

eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, op voorwaarde dat ze deze gegevens in het kader van de verstrekking van de communicatienetwerken of -diensten in kwestie verwerken of genereren.

Dit artikel heeft geen betrekking op de inhoud van de communicatie.

Deze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1.

De in dit artikel beoogde gegevens worden bewaard vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is.

In afwijking van het derde lid worden de andere dynamische IP-adressen dan diegene die is gebruikt om in te tekenen op de dienst, tot twaalf maanden na het einde van de sessie bewaard.

§ 2. De Koning bepaalt, na advies van de bevoegde Gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens alsook de vereisten waaraan deze gegevens moeten beantwoorden."

Die bepaling wort in de commentaar op het artikel als volgt verantwoord:

"Voor de tenuitvoerlegging van het arrest van het Grondwettelijk Hof van 22 april 2021 en het arrest-Quadrature du Net van het Europees Hof van Justitie worden voor de bewaringsplicht enkel nog de abonnementsgegevens en technische gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst beoogd, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie (zoals de identificatiecode die wordt gecreëerd voor elke communicatie). Dit artikel is van toepassing wanneer elektronische-communicatiedienst in België wordt verstrekt.

De bewaringstermijn van 12 maanden werd behouden, aangezien deze termijn overeenstemt met de strikt noodzakelijke bewaringstermijn om de autoriteiten in staat te stellen om hun onderzoeken tot een goed einde te brengen, in het bijzonder op het stuk van de strijd tegen de zware criminaliteit.

Er wordt een onderscheid gemaakt tussen het IP-adres dat gebruikt is om op de dienst in te tekenen en de overige IP-adressen. Het IP-adres dat gebruikt is om in te tekenen op de dienst is immers een gegeven dat door de operatoren moet worden bewaard in het kader van artikel 127, om de identiteit van de abonnee te kunnen vaststellen of nagaan.

De abonnementsgegevens omvatten onder andere het telefoonnummer, het e-mailadres, het nummer van de abonnee, de start- en einddatum van het abonnement. De Franse Conseil d'État, die de Franse wetgeving betreffende bewaring van verkeersgegevens voor de autoriteiten moest onderzoeken

autorités (arrêt du 21/04/2021 n^{os} 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), a considéré à cet égard ce qui suit: "il résulte clairement de la directive du 12 juillet 2002 et du RGPD qu'ils ne s'opposent pas à une obligation de conservation généralisée et indifférenciée, pour une durée d'un an, des informations autres que celles relatives à l'identité civile fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, d'une part, et des données relatives aux paiements, d'autre part, mentionnées respectivement aux 3° et 4°, de l'article 1er du décret du 25 février 2011 (point 36)

Les identifiants techniques qui ne sont pas rattachés à une communication déterminée mais qui servent principalement à identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé comprennent entre autres l'adresse IP source, l'IMEI (*International Mobile Equipment Identity*), l'IMSI (International Mobile Subscriber Identity), l'ICCID (*Integrated Circuit Card Identifier*), l'adresse MAC, le MSISDN (*Mobile Station Integrated Services Digital Network*), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées. À ce jour, la Cour de justice de l'Union européenne ne s'est prononcée que sur l'adresse IP source mais pas sur les autres données techniques précitées, dont la conservation est également nécessaire à des fins d'identification.

Les données nécessaires pour identifier l'utilisateur final, l'équipement ou le service de communications électroniques peuvent inclure des données de trafic. A titre d'exemple, la conservation de certaines données de trafic sera nécessaire pour relier l'adresse IP à une personne spécifique ou pour retrouver le numéro de téléphone utilisé ou le numéro MSISDN ("*Mobile Subscriber Integrated Services Digital Network*", à savoir le numéro de téléphone avec le préfixe international) servi.

Comme l'indique la Cour de Justice dans son arrêt *Quadrature du Net* du 6/10/2020, l'adresse IP source est le seul moyen susceptible de permettre l'identification de l'auteur d'une infraction en ligne (point 154 de l'arrêt).

Dans l'arrêt de la Cour de Justice *Ministerio Fiscal* (C-207/16, point 20), a été considérée comme ne constituant pas une ingérence grave aux droits fondamentaux (vie privée et protection des données à caractère personnel), la demande de la police judiciaire, pour les besoins d'une enquête pénale, de se voir transmettre les numéros de téléphone activés, pendant une période de douze jours, avec le code relatif à l'identité internationale d'équipement mobile (ci-après le "code IMEI") du téléphone mobile volé ainsi que les données à caractère personnel relatives à l'identité civile des titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code.

Au vu de l'utilité que représentent ces données techniques afin de permettre l'identification d'auteurs d'infractions en

(arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), heeft daarover het volgende gesteld: 'uit de richtlijn van 12 juli 2002 en van de AVG blijkt duidelijk dat zij niet gekant zijn tegen een verplichting tot algemene en ongedifferentieerde bewaring, voor de duur van een jaar, van andere inlichtingen dan die in verband met de burgerlijke identiteit die verstrekt zijn bij het sluiten van een contract door een gebruiker of bij het aanmaken van een account enerzijds, en van de gegevens met betrekking tot de betalingen anderzijds, respectievelijk vermeld in de bepalingen onder 3° en 4° van artikel 1 van het decreet van 25 februari 2011' (punt 36) (vrij vertaald).

De technische identificatiecodes die niet gelinkt zijn aan een specifieke communicatie maar die hoofdzakelijk dienen om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, omvatten onder andere het IP-bronadres, de IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), ICCID (Integrated Circuit Card Identifier), het MAC-adres, het MSISDN (Mobile Station Integrated Services Digital Network), of andere identificatiecodes die zullen worden ontwikkeld in het kader van 5G of afhankelijk van de evolutie van de gebruikte technologieën. Tot op heden heeft het Hof van Justitie van de Europese Unie zich enkel uitgesproken over het IP-adres aan de bron, maar niet over de voormelde andere technische gegevens, waarvan de bewaring eveneens noodzakelijk is voor identificatiedoeleinden.

De gegevens die noodzakelijk zijn om de eindgebruiker, de apparatuur of de elektronische-communicatiedienst te identificeren, kunnen verkeersgegevens omvatten. Zo zullen bijvoorbeeld bepaalde verkeersgegevens moeten bewaard worden om het IP-adres aan een specifieke persoon te linken of om het gebruikte telefoonnummer of MSISDN-nummer ('Mobile Subscriber Integrated Services Digital Network', met name het telefoonnummer met het internationale prefix) terug te vinden.

Zoals aangegeven in het arrest La Quadrature du Net van het HvJ-EU van 6/10/2020, is het IP-bronadres het enige middel aan de hand waarvan de dader van een online-inbreuk kan worden geïdentificeerd (punt 154 van het arrest).

In het arrest van het HvJ-EU van 2 oktober 2018, Ministerio Fiscal (C207/16, punt 20), werd beschouwd dat het volgende geen ernstige inmenging vormt in de grondrechten (persoonlijke levenssfeer en bescherming van de persoonsgebonden gegevens): het verzoek van de gerechtelijke politie, ten behoeve van een strafrechtelijk onderzoek, om de telefoonnummers te krijgen die gedurende een periode van twaalf dagen werden geactiveerd aan de hand van de code voor de internationale identiteit van het mobiele toestel (hierna de 'IMEI-code') van de gestolen mobiele telefoon alsook de persoonsgebonden gegevens met betrekking tot de burgerlijke identiteit van de houders of van de gebruikers van de telefoonnummers die overeenstemmen met de via deze code geactiveerde simkaarten.

In het licht van het nut dat deze technische gegevens vertegenwoordigen voor de identificatie van daders van

ligne ou hors ligne, la mesure de conservation prévue est proportionnée"[39].

2. L'article 126 en projet, doit être mis en rapport avec l'arrêt *La Quadrature du Net*, ainsi qu'avec l'arrêt n° 57/2021 de la Cour constitutionnelle.

Pour rappel, dans le dispositif de son arrêt *La Quadrature du Net*, la Cour de Justice a dit en effet pour droit que l'article 15, paragraphe 1, de la directive 2002/58/CE lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, ne s'oppose pas à des mesures législatives:

"[…]

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques,

[…]".

La Cour de Justice opère ainsi une distinction entre:

– d'une part, la conservation généralisée et indifférenciée des adresse IP attribuées à une source de connexion, laquelle peut être imposée aux opérateurs par la législation uniquement aux fins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, et ce pour une période temporellement limitée au strict nécessaire, et,

– d'autre part, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, laquelle peut être imposée aux opérateurs par la législation à des fins plus larges, à savoir la sauvegarde de la sécurité nationale, la lutte contre la criminalité, que celle-ci soit grave ou non, et la sauvegarde de la sécurité publique, même lorsque cette sécurité ne fait pas l'objet de menaces graves, et ce sans que ces données doivent être conservées pour une "période temporelle limitée au strict nécessaire".

3. La disposition à l'examen vise quant à elle:

– les données de souscription de l'abonné, qui ne sont pas définies, mais à propos desquelles le commentaire de l'article précise qu'elles "comprennent entre autres le numéro

[39] Exposé des motifs, pp 30-32.

overtredingen online en offline, is de geplande bewaringsmaatregel evenredig."[39]

2. Het ontworpen artikel 126 moet in verband worden gebracht met het arrest *La Quadrature du Net* en met arrest nr. 57/2021 van het Grondwettelijk Hof.

Pro memorie zij gesteld dat het Hof van Justitie in het dictum van zijn arrest *La Quadrature du Net* inderdaad voor recht heeft verklaard dat artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 en van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, geen wetgevende maatregelen verhindert

"(…)

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen,

(…)."

Het Hof van Justitie maakt aldus een onderscheid tussen:

– enerzijds de algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, die de wetgeving aan de operatoren enkel kan opleggen ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid, en dit voor een periode die niet langer is dan strikt noodzakelijk,

– en anderzijds algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, die de wetgeving aan de operatoren kan opleggen met het oog op ruimere doelstellingen, namelijk de bescherming van de nationale veiligheid, de bestrijding van criminaliteit, ongeacht of het al dan niet om zware criminaliteit gaat, en de bescherming van de openbare veiligheid, zelfs wanneer die niet ernstig wordt bedreigd, en dit zonder dat de bewaring van die gegevens beperkt is tot "periode die niet langer is dan strikt noodzakelijk".

3. Harerzijds heeft de voorliggende bepaling betrekking op het volgende:

– de abonnementsgegevens van de abonnee, die niet worden gedefinieerd maar waarover in de commentaar op het artikel wordt gezegd dat ze "onder andere het telefoonnummer,

[39] Memorie van toelichting, 30-32.

de téléphone, l'adresse email, le numéro d'abonné, la date de début et de fin de la souscription", et

– les données qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, qui, elles non plus, ne sont pas définies mais dont le commentaire de l'article mentionne qu'elles "comprennent entre autres l'adresse IP source, l'IMEI (*International Mobile Equipment Identity*), l'IMSI *(International Mobile Subscriber Identity*), l'ICCID (*Integrated Circuit Card Identifier*), l'adresse MAC, le MSISDN (*Mobile Station Integrated Services Digital Network*), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées".

S'agissant des données visées par la disposition en projet qui ne constitueraient pas des données uniquement relatives à "l'identité civile des utilisateurs de moyens de communications électroniques" mais sont des adresses IP source, ou des données dont la conservation est susceptible d'entrainer des risques similaires à ceux que présentent la conservation et l'accès à des données IP source[40], il y a lieu de constater que rien, dans la disposition en projet, ne limite la conservation de ces données à des fins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique.

Certes, l'article 126, § 1er, alinéa 3, en projet, prévoit-il que "ces données sont conservées pour les autorités et les finalités visées à l'article 127/1". Cependant, dans l'article 127/1, en projet, s'agissant spécialement des 1° et 2° de son paragraphe 1er, les finalités sont exprimées de manière générale et

40 Dans son arrêt *La Quadrature du Net*, la Cour de Justice a relevé, à propos des adresses IP source, ce qui suit:
"152. Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.
153.Toutefois, les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt". C'est la gravité de l'ingérence ainsi considérée qui a amené la Cour de Justice à réserver à cette catégorie de données un traitement plus sévère que celui réservé aux données relatives à l'identité civile des utilisateurs.

het e-mailadres, het nummer van de abonnee, de start- en einddatum van het abonnement [omvatten]", en

– de gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst, die al evenmin worden gedefinieerd maar waarover de commentaar op het artikel stelt dat ze "onder andere het IP-bronadres, de IMEI (*International Mobile Equipment Identity),* IMSI *(International Mobile Subscriber Identity*), ICCID (*Integrated Circuit Card Identifier*), het MAC-adres, het MSISDN (*Mobile Station Integrated Services Digital Network*), of andere identificatiecodes die zullen worden ontwikkeld in het kader van 5G of afhankelijk van de evolutie van de gebruikte technologieën [omvatten]".

In verband met de in de ontworpen bepaling vermelde gegevens die niet uitsluitend betrekking zouden hebben op de "burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen", maar IP-bronadressen zijn, of in verband met de gegevens waarvan de bewaring soortgelijke risico's kan meebrengen als die waartoe de bewaring van en de toegang tot IP-brongegevens aanleiding geven,[40] dient te worden opgemerkt dat de bewaring van die gegevens in de ontworpen bepaling geenszins wordt beperkt tot doeleinden van bescherming van de nationale veiligheid, bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen van de openbare veiligheid.

Het ontworpen artikel 126, § 1, derde lid, bepaalt weliswaar dat "[d]eze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1", maar in het ontworpen artikel 127/1, meer bepaald in § 1, 1° en 2°, worden die doeleinden op algemene wijze geformuleerd en worden ze

40 Het Hof van Justitie heeft in zijn arrest *La Quadrature du Net* het volgende opgemerkt over de IP-bronadressen:
"152. Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronische communicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.

153. Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben". De ernst van de aldus beschouwde inmenging heeft het Hof van Justitie ertoe gebracht die categorie van gegevens strenger te behandelen dan de gegevens betreffende de burgerlijke identiteit van de gebruikers.

ne sont pas limitées à “la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique”.

4. Il en résulte que le système mis en place par l’article 126 en projet, combiné avec l’article 127/1 en projet n’est pas de nature à garantir le respect de l’article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière de l’enseignement de l’arrêt *La Quadrature du Net*, en ce qui concerne la conservation générale et non différenciée des adresses IP source, et par analogie, de toutes les données assimilables, dont la conservation présente des risques similaires à ceux qui sont attachés à la conservation des adresses IP source, tels que relevés par la Cour de Justice.

Le dispositif en projet sera revu et complété à la lumière de cette observation.

5. Enfin, la disposition à l’examen prévoit que les données qu’elle vise sont conservées “à partir de la date d’activation du service jusqu’à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l’aide du service utilisé”. Pour les adresses IP dynamiques, autres que celles qui sont utilisées pour souscrire au service, il est prévu qu’elles sont conservées jusqu’à douze mois après la fin de la session.

De tels délais peuvent paraitre relativement longs au regard des exigences résultant de l’enseignement de l’arrêt *La quadrature du Net*.

Le commentaire de l’article précise à ce propos:

“La durée de conservation de 12 mois a été maintenue, dès lors que cette durée correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave”.

Cette justification revêt un caractère très général, et relève de l’affirmation de principe.

Les auteurs de l’avant-projet doivent être en mesure de mieux justifier les délais retenus, ce sur la base d’éléments concrets et probants.

La disposition à l’examen sera réexaminée à la lumière de cette observation.

La conservation généralisée et indifférenciée, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, des données relatives à l’identité civile des utilisateurs de moyens de communications électroniques

1. Selon l’enseignement de l’arrêt *La Quadrature du Net*, est admissible une législation permettant aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation

niet beperkt tot “de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid”.

4. Daaruit vloeit voort dat de in het ontworpen artikel 126 ingevoerde regeling in combinatie met het ontworpen artikel 127/1 niet de inachtneming kan garanderen van artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van de lering van het arrest *La Quadrature du Net*, wat betreft de algemene en ongedifferentieerde bewaring van IP-bronadressen, en bij analogie van alle vergelijkbare gegevens, waarvan de bewaring soortgelijke risico’s inhoudt als die welke verbonden zijn aan de bewaring van de IP-bronadressen, zoals naar voren gebracht door het Hof van Justitie.

Het ontworpen dispositief moet in het licht van deze opmerking worden herzien en aangevuld.

5. Ten slotte stelt de voorliggende bepaling dat de gegevens die ze vermeldt, bewaard worden “vanaf de datum van activering van de dienst tot twaalf maanden na de datum vanaf wanneer communicatie voor het laatst mogelijk is aan de hand van de gebruikte dienst”. Voor andere dynamische IP-adressen dan die welke worden gebruikt om in te tekenen op de dienst, wordt bepaald dat ze tot twaalf maanden na het einde van de sessie worden bewaard.

Dergelijke termijnen kunnen relatief lang lijken ten aanzien van de vereisten die voortvloeien uit de lering van het arrest *La Quadrature du Net*.

In de commentaar op het artikel wordt dienaangaande het volgende gepreciseerd:

“De bewaringstermijn van 12 maanden werd behouden, aangezien deze termijn overeenstemt met de strikt noodzakelijke bewaringstermijn om de autoriteiten in staat te stellen om hun onderzoeken tot een goed einde te brengen, in het bijzonder op het stuk van de strijd tegen de zware criminaliteit.”

Dat is een heel algemene verantwoording die meer weg heeft van een beginselverklaring.

De stellers van het voorontwerp moeten de vastgestelde termijnen beter kunnen verantwoorden met concrete en afdoende gegevens.

De voorliggende bepaling moet in het licht van deze opmerking opnieuw worden onderzocht.

Algemene en ongedifferentieerde bewaring van gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de bescherming van de openbare veiligheid

1. Volgens de lering van het arrest *La Quadrature du Net* kan worden aanvaard dat een wetgeving een algemene en ongedifferentieerde bewaring van gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronische

généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques.

L'article 9 de l'avant-projet, qui entend remplacer l'article 127 de la loi du 13 juin 2005 vise à organiser une conservation ayant cet objet.

Au regard des exigences de droit international et européen rappelées ci-avant, sur le principe, cette disposition ne parait pas poser de difficulté.

Il n'en demeure pas moins que l'autorisation générale, donnée aux opérateurs par l'article 127, § 2, alinéa 2, en projet, de "réaliser, de manière automatique, une comparaison entre les paramètres biométriques sur la photo de la pièce d'identité de l'abonné et ceux du visage" peut paraitre disproportionnée par rapport à l'objectif poursuivi, compte tenu, spécialement, de ce que ces données pourraient être recueillies auprès de tous les abonnés personnes physiques, généralement quelconques, de tous les opérateurs, sans même que cette possibilité soit encadrée par le législateur et limitée à des cas spécifiques rendant la mesure nécessaire.

Interrogés sur ce point, les délégués du ministre ont toutefois expliqué que l'opération de comparaison biométrique envisagée interviendrait uniquement le temps nécessaire pour identifier la personne et n'impliquerait aucun stockage ni conservation subséquente de données. Dans ce contexte, la mesure envisagée ne parait pas disproportionnée.

Dans un autre ordre d'idées, et très subsidiairement, la section de législation n'aperçoit pas comment l'article 127, § 2, alinéa 2, en projet, est supposé s'articuler avec l'habilitation conférée au Roi par l'article 127, § 3, alinéa 1er, 1° et 2°, en projet, qui permet à Celui-ci de "déterminer si l'opérateur doit lui-même identifier ses abonnés ou s'il peut seulement rendre cette identification possible" et de "déterminer les méthodes d'identification que les opérateurs peuvent utiliser, y compris soumettre une méthode d'identification proposée par un opérateur à une autorisation préalable du ministre [en charge des communications électroniques] et du ministre de la Justice".

L'article 9 de l'avant-projet sera revu à la lumière de ces observations.

Le recours à une injonction faite aux fournisseurs de services de communications électroniques, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services aux fins de la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale

1. Pour rappel, il résulte de l'arrêt *La Quadrature du Net* qu'aux fins de la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale, est admissible une législation qui permet qu'une injonction soit donnée aux

communicatiemiddelen mogelijk maakt ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de bescherming van de openbare veiligheid.

Artikel 9 van het voorontwerp, dat strekt tot vervanging van artikel 127 van de wet van 13 juni 2005, wil een dergelijke bewaring regelen.

Ten aanzien van de vereisten van het internationaal en het Europees recht die hierboven zijn vermeld, lijkt deze bepaling in principe geen moeilijkheden op te leveren.

Dat neemt niet weg dat de algemene machtiging die het ontworpen artikel 127, § 2, tweede lid, aan de operatoren verleent om "automatisch een vergelijking uit [te] voeren tussen de biometrische gegevens op de foto van het identiteitsstuk van de abonnee en deze van zijn gezicht" buitensporig kan lijken ten aanzien van het nagestreefde doel, in het bijzonder gelet op het feit dat die gegevens zouden kunnen worden verzameld bij alle abonnees, zijnde om het even welke natuurlijke persoon van alle operatoren, zonder dat de wetgever die mogelijkheid ook maar afbakent en beperkt tot specifieke gevallen waarin de maatregel noodzakelijk is.

Naar aanleiding van een vraag daarover hebben de gemachtigden van de minister evenwel uitgelegd dat de beoogde biometrische vergelijking enkel zou worden verricht in de tijdspanne die nodig is om een persoon te identificeren, en geen enkele opslag noch vervolgens enige bewaring van de gegevens zou inhouden. In die context lijkt de beoogde maatregel niet buitensporig te zijn.

In een andere gedachtegang, en in zeer bijkomende orde, ziet de afdeling Wetgeving niet in hoe het ontworpen artikel 127, § 2, tweede lid, zich zou moeten verhouden tot de machtiging die bij het ontworpen artikel 127, § 3, eerste lid, 1° en 2°, aan de Koning wordt verleend. Die machtiging houdt in dat de Koning kan "bepalen of de operator zelf zijn abonnees moet identificeren of louter deze identificatie mogelijk moet kunnen maken" en dat hij "de methodes voor identificatie [kan] bepalen die de operatoren kunnen gebruiken, inclusief een door een operator voorgestelde identificatiemethode onderwerpen aan een voorafgaande machtiging van de minister [bevoegd voor de elektronische communicatie] en van de minister van Justitie".

Artikel 9 van het voorontwerp moet in het licht van deze opmerkingen worden herzien.

Gebruikmaken van een bevel aan de aanbieders van elektronischecommunicatiediensten tot spoedbewaring gedurende een bepaalde periode van de in hun handen zijnde verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid

1. Er wordt aan herinnerd dat uit het arrest *La Quadrature du Net* volgt dat ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid een wetgeving toelaatbaar is die het mogelijk maakt

fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

2.1. L'article 32 de l'avant-projet entend insérer un paragraphe 1er*bis*/1 dans l'article 84 de la loi du 2 aout 2002 'relative à la surveillance du secteur financier et aux services financiers', rédigé comme suit:

"Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1er, alinéa 2, de conserver les données visées au paragraphe 1er, alinéa 1er, qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.

Les paragraphes 1er, alinéas 4 et 5, et 3 s'appliquent par analogie à l'ordre visé à l'alinéa 1er.

Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

L'auditeur ou, en son absence, l'auditeur adjoint fait part au juge d'instruction de l'ordre visé à l'alinéa 1er au moment où il lui adresse sa demande d'autorisation préalable pour requérir la communication des données visées au paragraphe 1er, alinéa 1er. Si le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre ou s'il estime que l'ordre n'était pas légitime ou pas justifié, cet ordre s'éteint".

2.2.1. Eu égard à l'enseignement de l'arrêt *La Quadrature du Net*, cette disposition appelle deux observations.

2.2.2. Tout d'abord se pose la question de savoir si l'opération de "*quick freeze*" ainsi autorisée se limite bien à des faits qui relèvent de "la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale".

À ce propos, le commentaire de l'article mentionne ce qui suit:

"Cette possibilité de quick freeze n'est en outre prévue que pour les violations de l'interdiction d'abus de marché (articles 14 ou 15 du Règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché)), qui constituent une infraction grave. Leur impact sur l'intégrité des marchés financiers et sur la confiance des investisseurs est en effet important. Il s'agit, au sein du secteur financier, de l'une des infractions les plus graves, comme en témoignent notamment le fait que le règlement relatif aux abus de marché exige pour

om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

2.1. Artikel 32 van het voorontwerp strekt ertoe een paragraaf 1*bis*/1 in te voegen in artikel 84 van de wet van 2 augustus 2002 'betreffende het toezicht op de financiële sector en de financiële diensten'. Die paragraaf luidt als volgt:

"Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de in paragraaf 1, tweede lid, bedoelde actoren bevelen om de gegevens bedoeld in paragraaf 1, eerste lid, die riskeren te worden verwijderd of anoniem gemaakt, te bewaren totdat hij de toestemming van een onderzoeksrechter heeft bekomen.

Paragrafen 1, vierde en vijfde lid, en 3 zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.

De in paragraaf 1, tweede lid, bedoelde actoren zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, bezorgt het in het eerste lid bedoelde bevel aan de onderzoeksrechter gelijktijdig met zijn verzoek tot voorafgaande toestemming om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel betrekking heeft of oordeelt dat het bevel niet wettig of niet gerechtvaardigd was, vervalt het bevel."

2.2.1. Gelet op de lering van het arrest *La Quadrature du Net*, geeft die bepaling aanleiding tot twee opmerkingen.

2.2.2. Allereerst rijst de vraag of de "*quick freeze*", de snelle gegevensbewaring die op die manier toegestaan wordt, zich wel beperkt tot feiten die verband houden met "de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid".

De bespreking van het artikel vermeldt in dat verband het volgende:

"Bovendien wordt deze mogelijkheid tot quick freeze enkel voorzien voor inbreuken op het verbod op marktmisbruik (artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik)), wat een ernstig misdrijf uitmaakt. De impact daarvan op de integriteit van de financiële markten en het vertrouwen van de beleggers is immers groot. Binnen de financiële sector gaat het om één van de meest ernstige inbreuken, wat o.m. blijkt uit het feit dat de Verordening marktmisbruik voor deze inbreuken aanzienlijk

ces infractions des amendes maximales d'un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement et à la plupart des autres législations financières européennes, ainsi que le fait que la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché impose aux États membres de prévoir également des sanctions pénales pour les abus de marché (disposition transposée dans les articles 39 et 40 de la loi du 2 aout 2002). Dans le cadre des enquêtes généralement longues et complexes qui concernent les abus de marché, les données de communications électroniques jouent souvent un rôle important dans l'administration de la preuve, par exemple pour constater que des personnes ont, à un moment donné, été en contact l'une avec l'autre et qu'il existe une relation entre deux ou plusieurs personnes".

Certes, le règlement 596/2014, prévoit, en son article 30, à l'égard des manquements à ses articles 14 et 15, des sanctions qui apparaissent lourdes, dans l'absolu, et en tout cas plus lourdes que celles prévues pour d'autres infractions.

Ainsi, pour les personnes physiques, en son article 30, paragraphe 2, ce règlement impose aux États membres de faire en sorte que les autorités compétentes puissent imposer une sanction administrative pécuniaire d'un montant maximal d'au moins 5 000 000 EUR.

Pour les personnes morales, ce montant maximal est d'au moins 15 000 000 EUR ou 15 % du chiffre d'affaires annuel total de la personne morale tel qu'il ressort des derniers comptes disponibles approuvés par l'organe de direction de l'entreprise.

Il reste toutefois que ces sanctions constituent, selon le règlement lui-même, des sanctions pécuniaires administratives, et non pénales.

Par ailleurs, le règlement ne fixe pas de montant minimum pour ces sanctions, mais uniquement le plancher du montant maximum de la sanction.

Quant aux articles 39 et 40 de la loi du 2 aout 2002, auxquels renvoie le commentaire de l'article, les sanctions pénales minimales qu'ils prévoient sont respectivement:

– pour l'article 39, § 1er: un emprisonnement d'un mois et une amende de 300 euros;

– pour l'article 40, § 6: un emprisonnement de trois mois et une amende de 50 euros.

Dans ces contextes, il parait difficile de considérer que, dans l'absolu, toutes les infractions couvertes par ces différentes

hogere minimale maximumboetes vereist dan voor de inbreuken op andere bepalingen van de verordening en op de meeste andere Europese financiële wetgeving, alsook uit het feit dat richtlijn 2014/57/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende strafrechtelijke sancties voor marktmisbruik de lidstaten oplegt om voor marktmisbruik ook strafrechtelijke sancties te voorzien (uitgewerkt in de artikelen 39 en 40 van de wet van 2 augustus 2002). In het kader van de doorgaans complexe en tijdsintensieve onderzoeken inzake marktmisbruik spelen elektronische communicatiegegevens dikwijls een belangrijke rol in de bewijsvoering, bijvoorbeeld om vast te stellen dat personen op een bepaald moment met elkaar in contact zijn geweest en er tussen twee of meer personen een relatie bestaat."

Verordening 596/2014 voorziet in haar artikel 30 met betrekking tot de inbreuken op haar artikelen 14 en 15 weliswaar in sancties die in theorie zwaar lijken en die in elk geval zwaarder zijn dan de straffen bepaald voor andere strafbare feiten.

Zo schrijft artikel 30, lid 2, van die verordening met betrekking tot natuurlijke personen voor dat de lidstaten ervoor moeten zorgen dat de bevoegde autoriteiten een maximale administratieve financiële sanctie kunnen opleggen van ten minste 5 000 000 EUR.

Met betrekking tot rechtspersonen bedraagt dat maximumbedrag ten minste 15 000 000 EUR of 15 % van de totale jaaromzet van de rechtspersoon overeenkomstig de meest recente beschikbare en door het management goedgekeurde jaarrekeningen.

Dat neemt evenwel niet weg dat die sancties volgens de verordening zelf administratieve financiële sancties zijn en geen strafsancties.

Bovendien stelt de verordening geen minimumbedrag vast voor die sancties, maar enkel de onderste drempel van het maximumbedrag van de sanctie.

Wat de artikelen 39 en 40 van de wet van 2 augustus 2002 betreft waarnaar in de bespreking van het artikel verwezen wordt, wordt respectievelijk voorzien in de volgende minimale strafsancties:

– wat artikel 39, § 1, betreft: een gevangenisstraf van één maand en een geldboete van 300 euro;

– wat artikel 40, § 6, betreft: een gevangenisstraf van drie maanden en een geldboete van 50 euro.

In die omstandigheden lijkt het moeilijk aanneembaar dat in theorie alle strafbare feiten waarop die verschillende

dispositions participent, par nature, de la notion de “criminalité grave”[41].

Si la section de législation comprend la logique des justifications invoquées dans le commentaire des articles, il convient, aux fins d’assurer la conformité du dispositif en projet avec les principes dégagés par l’arrêt *La Quadrature du Net*, de limiter le pouvoir d’injonction envisagé aux faits dont le caractère de gravité est établi ou peut être présumé sur la base des éléments dont dispose l’auditeur ou l’auditeur adjoint.

2.2.3. Par ailleurs, le mécanisme en projet gagnerait à être complété aux fins de prévoir que la demande d’accès aux données formée auprès du juge d’instruction doit être concomitante à l’injonction de “*quick freeze*” adressée à ou aux opérateurs concernés, ou, à tout le moins, intervenir sans délai en suite de cette dernière.

Une telle simultanéité ou quasi simultanéité est en effet de nature à mieux garantir un contrôle juridictionnel effectif, comme requis par le droit européen.

2.2.4. L’article 32 de l’avant-projet sera revu à la lumière de ces observations.

3. L’article 24 de l’avant-projet envisage d’insérer un article 16/2/1, dans la loi du 30 novembre 1998.

Outre les observations particulières qu’appelle cette disposition compte tenu des ambiguïtés, imprécisions et autres difficultés dont elle est entachée, et qui sont abordées dans les observations particulières ci-après, la section de législation s’interroge sur la manière dont il sera satisfait à l’exigence de contrôle juridictionnel effectif, qui résulte de l’enseignement de l’arrêt *La Quadrature du Net*.

L’article 24 sera réexaminé à la lumière de cette observation.

Observations particulières

Arrêté de présentation

L’arrêté de présentation sera rédigé comme suit:

“Philippe I^er^, Roi des Belges,

À tous, présents et à venir, Salut.

[41] Comparer sur ce point avec l’article 39*quinquies*, en projet, du Code d’instruction criminel (article 17 de l’avant-projet) qui visent des infractions qui “peuvent donner lieu à un emprisonnement correctionnel principal d’un an ou à une peine plus lourde”.

bepalingen van toepassing zijn per definitie onder de noemer “zware criminaliteit” vallen.[41]

Hoewel de afdeling Wetgeving de logica begrijpt van de rechtvaardigingen die in de bespreking van de artikelen aangevoerd worden, dient, teneinde ervoor te zorgen dat het ontworpen dispositief in overeenstemming is met de beginselen voortvloeiend uit het arrest *La Quadrature du Net*, de injunctiebevoegdheid waarvan sprake is beperkt te worden tot de feiten waarvan de ernst aangetoond is of verondersteld kan worden op basis van de gegevens waarover de auditeur of de adjunct-auditeur beschikt.

2.2.3. Bovendien zou de ontworpen regeling beter aldus aangevuld worden dat daarin bepaald wordt dat de aan de onderzoeksrechter gerichte aanvraag tot toegang tot de gegevens met het aan de betrokken operator(en) gegeven bevel tot “*quick freeze*” moet samenvallen of daar op zijn minst onverwijld moet op volgen.

Dat samenvallen of het bijna samenvallen ervan biedt immers een grotere garantie op een effectieve rechterlijke toetsing, zoals wordt voorgeschreven door het Europees recht.

2.2.4. Artikel 32 van het voorontwerp moet in het licht van die opmerkingen herzien worden.

3. Artikel 24 van het voorontwerp strekt ertoe een artikel 16/2/1 in te voegen in de wet van 30 november 1998.

Afgezien van de bijzondere opmerkingen waartoe die bepaling aanleiding geeft, gelet op de dubbelzinnigheden, de onnauwkeurigheden en de andere moeilijkheden waarmee ze behept is en die in de bijzondere opmerkingen hierna aan bod komen, vraagt de afdeling Wetgeving zich af op welke wijze voldaan zal worden aan het vereiste van een effectieve rechterlijke toetsing dat voortvloeit uit de lering van het arrest *La Quadrature du Net*.

Artikel 24 moet in het licht van die opmerking opnieuw onderzocht worden.

Bijzondere opmerkingen

Indieningsbesluit

Het indieningsbesluit moet als volgt gesteld worden:

“Filip I, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

[41] Vergelijk op dat punt met het ontworpen artikel 39*quinquies* van het Wetboek van Strafvordering (artikel 17 van het voorontwerp) dat betrekking heeft op misdrijven “die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben”.

Sur la proposition du ministre de la ministre des Télécommunications, du ministre de la Justice et de la ministre de la Défense,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

La ministre des Télécommunications, le ministre de la Justice et la ministre de la Défense sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:"[42].

DISPOSITIF

Article 4

1. Le paragraphe 4, alinéa 3, en projet, de l'article 122 de la loi du 13 juin 2005 prévoit que les opérateurs sont tenus de conserver les données de localisation et les autres données de trafic nécessaires aux fins de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications, au minimum quatre mois.

Le commentaire de l'article mentionne à ce propos que:

"Le délai de quatre mois a été retenu pour l'application de l'alinéa 3, étant donné que la fraude peut avoir un impact sur la facturation de l'opérateur envers l'abonné (ou d'une entreprise envers l'abonné).

Le délai minimal de quatre mois de conservation tient compte d'un cycle complet de facturation (premier mois suivant la consommation du service), d'une durée de contestation minimale (de 15 jours à 1 mois, le deuxième mois suivant la consommation du service), d'une période de traitement de la contestation permettant un échange entre l'abonné et l'opérateur (le troisième mois suivant la contestation du service) et d'une période de retard possible dans ce traitement (le quatrième mois suivant la consommation).

Le délai de 4 mois permettra aussi de prendre en compte les évolutions en matière de fraude".

Si ces explications apparaissent, *prima facie*, comme pouvant justifier un délai de conservation de quatre mois, par contre, la disposition en projet devrait mieux encadrer la conservation des données concernées au-delà de ce délai, aux fins de prévoir un délai maximum et en tout cas limité au strict nécessaire compte tenu des finalités de la conservation, la lutte contre la fraude, d'une part, et celle, d'autre part, contre les appels malveillants qui constituent, par nature, deux finalités distinctes.

[42] *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet "Technique législative", recommandations n^os^ 226 et 227, formule F 5.

Op de voordracht van de minister van Telecommunicatie, de minister van Justitie en de minister van Defensie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Telecommunicatie, de minister van Justitie en de minister van Defensie zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:"[42]

DISPOSITIEF

Artikel 4

1. De ontworpen paragraaf 4, derde lid, van artikel 122 van de wet van 13 juni 2005 bepaalt dat de locatiegegevens en andere verkeersgegevens die nodig zijn om een vermoed geval van fraude of van moedwillig gebruik van een elektronische-communicatienetwerk op te sporen en te analyseren minstens vier maanden door de operatoren bewaard moeten worden.

De bespreking van het artikel vermeldt in dat verband het volgende:

"De termijn van vier maanden is in aanmerking genomen voor de toepassing van het derde lid, aangezien de fraude een impact kan hebben op de facturering van de operator tegenover de abonnee (of van een onderneming tegenover de abonnee).

De minimale termijn van vier maanden bewaring houdt rekening met een volledige factureringscyclus (eerste maand volgend op het verbruik van de dienst), met een minimale duur voor betwisting (van 15 dagen tot 1 maand, de tweede maand volgend op het verbruik van de dienst), met een periode voor de behandeling van de betwisting die een uitwisseling tussen de abonnee en de operator mogelijk maakt (de derde maand volgend op de betwisting van de dienst) en met een periode van mogelijke vertraging in die behandeling (de vierde maand volgend op het verbruik).

De termijn van 4 maanden zal het ook mogelijk maken om rekening te houden met de ontwikkelingen op het stuk van fraude."

Hoewel die toelichting *prima facie* blijkbaar een bewaartermijn van vier maanden kan rechtvaardigen, zou de bewaring van de betrokken gegevens buiten die termijn echter beter door de ontworpen bepaling afgebakend moeten worden, teneinde te voorzien in een maximumtermijn die zich tevens hoe dan ook tot het strikt noodzakelijke beperkt, gelet op de doeleinden van de bewaring, namelijk enerzijds de fraudebestrijding en anderzijds de bestrijding van kwaadwillige oproepen, die per definitie twee verschillende doeleinden zijn.

[42] *Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbevelingen 226 en 227, formule F 5.

2. Le paragraphe 4, alinéa 4, en projet, de l'article 122, de la loi du 13 juin 2005, est rédigé comme suit:

"Lorsqu'un opérateur a détecté une fraude potentielle ou avérée ou une utilisation malveillante potentielle ou avérée du réseau, il prend les mesures appropriées, compte tenu des possibilités techniques les plus récentes, pour éviter que l'utilisateur final ne subisse un préjudice ou ne soit importuné".

Telle qu'elle est rédigée, cette disposition peut être comprise comme imposant des obligations extrêmement larges aux opérateurs, obligations qui pourraient impliquer que ceux-ci soient tenus de procéder à des mesures en vue de protéger les intérêts d'un utilisateur, certes, mais qui interviendraient au détriment d'un autre, sur la base d'éléments non autrement établis par une autorité administrative ou un organe juridictionnel à la suite d'une instruction appropriée. De telles obligations sont sujettes à critiques au regard du droit au respect de la vie privée, de la liberté d'expression et du principe d'égalité et de non-discrimination.

Toutefois, le commentaire de l'article explique, à ce propos:

"Lorsque l'opérateur a détecté une fraude potentielle ou avérée envers son abonné, il lui revient de prendre les mesures les plus appropriées pour protéger son abonné. Une de ces mesures peut être l'information de ce dernier, par exemple l'information que l'appel pourrait être frauduleux.

Par ailleurs, les opérateurs doivent pouvoir contribuer à établir une utilisation malveillante du réseau (par exemple en confirmant qu'une certaine communication entrante a bien eu lieu dans le cadre d'une plainte d'harcèlement par téléphone).

En pratique, en cas de harcèlement par téléphone, la victime doit s'adresser au service de médiation pour les télécommunications.

Ce dernier, qui a pour mission l'aide aux victimes et n'est pas rattaché à un service de police, pourra alors obtenir via les opérateurs concernés les nom, prénom et adresse de l'auteur du harcèlement par téléphone et pourra fournir ces données à la victime de ce harcèlement (voir article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques). En pratique, un délai de conservation des données inférieur à 12 mois serait problématique, au vu des différentes étapes susmentionnés à suivre. Il convient également de souligner que le harcèlement par téléphone n'aura pas d'impact sur la facturation de l'opérateur à l'abonné, étant donné qu'il s'agit de communications entrantes".

Interrogés sur la portée de la disposition à l'examen, les délégués du ministre ont par ailleurs exposés, en substance, que

2. De ontworpen paragraaf 4, vierde lid, van artikel 122 van de wet van 13 juni 2005 luidt als volgt:

"Wanneer een operator een mogelijk of bewezen geval van fraude of een mogelijk of bewezen geval van kwaadwillig gebruik van het netwerk heeft opgespoord, neemt hij de gepaste maatregelen, rekening houdend met de meest recente technische mogelijkheden, om te vermijden dat de eindgebruiker schade ondervindt of wordt ontriefd."

Zoals die bepaling geredigeerd is, kan ze uitgelegd worden in die zin dat ze aan de operatoren uitzonderlijk grote verplichtingen oplegt welke zouden kunnen impliceren dat door hen maatregelen genomen moeten worden die er weliswaar op gericht zijn de belangen van een gebruiker te beschermen, maar die ten nadele van een andere gebruiker tot stand zouden komen op basis van elementen die na een adequaat onderzoek niet anderszins aangetoond worden door een administratieve overheid of een jurisdictioneel orgaan. Dergelijke verplichtingen zijn vatbaar voor kritiek in het licht van het recht op eerbiediging van het privéleven, de vrijheid van meningsuiting en het gelijkheids- en non-discriminatiebeginsel.

De bespreking van het artikel geeft in dat verband echter de volgende toelichting:

"Wanneer de operator een mogelijk of bewezen geval van fraude heeft opgespoord jegens zijn abonnee, dient hij de meest gepaste maatregelen te nemen om zijn abonnee te beschermen. Een van die maatregelen kan bestaan in het informeren van deze laatste, bijvoorbeeld hem melden dat de oproep frauduleus kan zijn.

Verder moeten de operatoren kunnen bijdragen tot het vaststellen van kwaadwillig gebruik van het netwerk (bijvoorbeeld door te bevestigen dat er wel degelijk een zekere communicatie is binnengekomen in het kader van een klacht in verband met telefonische pesterijen).

In geval van telefonische pesterijen moet het slachtoffer zich in de praktijk richten tot de Ombudsdienst voor telecommunicatie.

Deze laatste, die als opdracht heeft hulp te verlenen aan de slachtoffers en die niet onder een politiedienst valt, zal dan via de betrokken operatoren de naam, voornaam en het adres van de dader van de telefonische pesterijen kunnen krijgen en zal deze gegevens kunnen verstrekken aan het slachtoffer van die pesterijen (zie artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven). In de praktijk zou een termijn van gegevensbewaring van minder dan 12 maanden problematisch zijn gezien de verschillende voormelde stappen die moeten worden gevolgd. Er dient ook te worden benadrukt dat de telefonische pesterijen geen impact zullen hebben op de facturering van de operator aan de abonnee, aangezien het om binnenkomende communicatie gaat."

Op de vraag wat de draagwijdte is van de voorliggende bepaling hebben de gemachtigden van de minister voorts in hoofdzaak het volgende geantwoord:

– s'agissant des fraudes et utilisations malveillantes, les interventions ainsi attendues des opérateurs se limitent aux fraudes et utilisations malveillantes du réseau, qui revêtent un caractère manifeste et généralisé, comme des utilisations adressées à l'ensemble ou un groupe d'utilisateurs finaux en vue d'un but lucratif ou de nuire;

– pour le surplus, les utilisations malveillantes à l'égard de personnes déterminées, comme des comportements de harcèlement par le biais de réseaux de communications ne sont pas visées en tant que tels par les obligations générales imposées aux opérateurs, le système en projet n'ayant pas vocation à modifier le système existant qui implique l'intervention préalable du service de médiation.

De l'ensemble de ces éléments, il résulte que les obligations imposées aux opérateurs par l'alinéa reproduit ci-avant s'avèrent en réalité, dans l'intention des auteurs de l'avant-projet, d'une portée plus restreinte que la compréhension que l'on pourrait avoir de cette disposition, telle qu'elle est rédigée.

Il y a toutefois lieu d'avoir égard à l'alinéa 6 de l'article 122, § 4, en projet qui permet notamment au Roi de déterminer, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et des Autorités de protection des données compétentes, notamment "les actions que l'opérateur doit ou peut entreprendre lorsqu'il détecte une fraude présumée ou avérée ou une utilisation malveillante présumée ou avérée du réseau".

En vue de justifier que le Roi puisse – sans y être tenu – déterminer ces actions, le commentaire de l'article mentionne:

"L'adoption de cet arrêté royal n'est pas obligatoire, au vu des défis suivants. D'abord, les fraudes évoluent significativement avec le temps. Certains types de fraude peuvent disparaitre ou diminuer en importance alors que de nouveaux types de fraude peuvent voir le jour.

[…]

De plus, les actions que l'opérateur prend lorsqu'il détecte une fraude potentielle ou avérée peuvent être diverses en fonction du type de fraude et du degré de certitude que l'opérateur a par rapport au fait qu'il s'agit bien d'une fraude (seulement des indices ou une certitude à cet égard)".

Compte tenu de ces justifications, la question se pose de savoir si l'intention est effectivement de limiter les obligations imposées à l'opérateur aux nuisances (fraudes ou utilisations malveillantes) manifestes, ce qui serait de nature à mieux garantir la proportionnalité de la disposition envisagée au regard des droits et libertés évoqués plus haut, ou si telle n'est pas l'intention.

Par ailleurs, si la section de législation peut comprendre que l'évolution et la diversification rapides de ces nuisances requièrent certaines souplesse et forme de réactivité, les

– wat betreft fraude en kwaadwillig gebruik, beperken de aldus verwachte tussenkomsten van de operatoren zich tot de kennelijke en algemeen verbreide vormen van fraude en kwaadwillig gebruik van het net, zoals het gebruik dat op alle of op een groep van eindgebruikers gericht is met het doel winst te maken of schade te berokkenen;

– voor het overige hebben de algemene verplichtingen die aan de operatoren opgelegd worden als zodanig geen betrekking op het kwaadwillig gebruik ten aanzien van bepaalde personen, zoals pestgedrag via communicatienetwerken, aangezien de ontworpen regeling niet strekt tot wijziging van de bestaande regeling die een voorafgaande tussenkomst van de ombudsdienst impliceert.

Uit al die elementen volgt dat de verplichtingen die bij het hierboven weergegeven lid aan de operatoren opgelegd worden volgens de bedoeling van de stellers van het voorontwerp in feite een beperktere draagwijdte blijken te hebben dan die welke men uit de huidige redactie van die bepaling meent te kunnen afleiden.

Er moet evenwel rekening gehouden worden met het zesde lid van het ontworpen artikel 122, § 4, waarbij de Koning onder meer gemachtigd wordt om bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de bevoegde gegevensbeschermingsautoriteiten "de acties [te bepalen] die de operator moet of mag ondernemen wanneer hij een vermoed of bewezen geval van fraude of van kwaadwillig gebruik van het netwerk heeft opgespoord".

Ter rechtvaardiging van het feit dat de Koning die acties – zonder daartoe gehouden te zijn – zou kunnen bepalen, wordt in de bespreking van het artikel het volgende gesteld:

"De aanneming van dit koninklijk besluit is niet verplicht in het licht van de volgende uitdagingen. Ten eerste evolueert fraude aanzienlijk mettertijd. Bepaalde vormen van fraude kunnen verdwijnen of minder belangrijk worden terwijl nieuwe soorten van fraude kunnen opduiken.

(…)

Bovendien kunnen de acties die de operator onderneemt wanneer hij een mogelijk of bewezen geval van fraude heeft opgespoord, variëren naargelang van het type van fraude en van de graad van zekerheid die de operator heeft ten opzichte van het feit dat het wel degelijk om fraude gaat (enkel aanwijzingen of een zekerheid wat dat betreft)."

Gelet op die rechtvaardigingen rijst de vraag of het wel degelijk de bedoeling is om de verplichtingen die aan de operator opgelegd worden te beperken tot de kennelijke hinder (fraude of kwaadwillig gebruik), wat een grotere garantie zou bieden voor de proportionaliteit van de ontworpen bepaling in het licht van de hierboven besproken rechten en vrijheden, dan wel of dat niet de bedoeling is.

Hoewel de afdeling Wetgeving kan begrijpen dat de snelle evolutie en diversificatie van die hinder enige flexibiliteit en een vorm van reactiviteit vereisen, zouden de voornoemde

droits et libertés précités seraient mieux garantis si le Roi était tenu – et non simplement autorisé – à définir les actions, ou catégories d'actions à entreprendre par l'opérateur, en distinguant en outre l'hypothèse des nuisances manifestes ou "avérées" des autres hypothèses.

Enfin, les critères encadrant l'habilitation ainsi conférée au Roi doivent être précisés par le législateur, pour satisfaire au principe de légalité inscrit à l'article 22 de la Constitution.

3. Il ressort des explications communiquées par les délégués du ministre que l'établissement de la réalité d'une utilisation malveillante du réseau, telle que visée à l'article 122, § 4, alinéa 6, en projet, n'incombera pas à l'opérateur mais aux autorités compétentes en la matière, comme le service de médiation.

Le texte en projet sera revu et complété aux fins de le préciser.

4. La disposition à l'examen sera revue à la lumière de ces observations.

Article 5

1. L'article 5, 1°, entend remplacer l'article 123, § 1er, de la loi du 13 juin 2005, afin d'y traiter spécifiquement de la conservation des données de localisation autres que les données relatives au trafic.

Cette disposition transpose l'article 9 de la directive 2002/58/CE, qui dispose comme suit:

"1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et

rechten en vrijheden bovendien beter gewaarborgd worden indien de Koning gehouden – en niet gewoon gemachtigd – zou zijn een definitie te geven van de acties of de categorieën van acties die door de operator ondernomen moeten worden en hij daarbij het geval van kennelijke of "bewezen" hinder zou onderscheiden van de andere gevallen.

Ten slotte moeten de criteria ter afbakening van de aldus aan de Koning verleende machtiging door de wetgever gepreciseerd worden om te voldoen aan het legaliteitsbeginsel dat in artikel 22 van de Grondwet vervat is.

3. Uit de toelichtingen die de gemachtigden van de minister verstrekt hebben, blijkt dat het bestaan van een kwaadwillig gebruik van het netwerk, zoals bedoeld in het ontworpen artikel 122, § 4, zesde lid, niet door de operator aangetoond zal moeten worden maar door de ter zake bevoegde autoriteiten, zoals de ombudsdienst.

De ontworpen tekst moet herzien en aangevuld worden zodat dat nader bepaald wordt.

4. De voorliggende bepaling moet in het licht van die opmerkingen herzien worden.

Artikel 5

1. Artikel 5, 1°, strekt tot vervanging van artikel 123, § 1, van de wet van 13 juni 2005, om daarin specifiek te voorzien in een regeling met betrekking tot de bewaring van de andere locatiegegevens dan de verkeersgegevens.

Die bepaling zet artikel 9 van richtlijn 2002/58/EG om, dat luidt als volgt:

"1. Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, [voor zover] en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.

2. Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze

gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée".

2. Il résulte de cette disposition que, lorsque les données concernées peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée.

Deux hypothèses sont donc prévues, à la condition que ces données "puissent être traitées":

– soit les données ont été rendues anonymes;

– soit l'utilisateur ou l'abonné a donné son consentement; elles ne peuvent alors être traitées que dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée.

Le texte en projet prévoit pour sa part, cinq hypothèses. Celles figurant à l'article 123, § 1er, 1°, 2° et 5°, en projet, de la loi du 13 juin 2005 ne figurent pas dans l'article 9 de la directive 2002/58/CE.

L'une de ces trois autres hypothèses envisagées ne pose pas de difficulté en soi. Ainsi, lorsque le traitement est "nécessaire pour répondre à une obligation légale" (article 123, § 1er, 5°, en projet), il va de soi que, du moment que la disposition légale prévoyant ce traitement répond elle-même au prescrit de la directive 2002/58/CE, spécialement son article 15, paragraphe 1, le traitement est admissible. En d'autres termes, si difficulté il y a, cette dernière ne résiderait dès lors pas dans l'article 123, § 1er, 5°, en projet, de la loi du 13 juin 2005, mais, le cas échéant dans la ou les dispositions prévoyant "l'obligation légale", dispositions qui se situent ailleurs dans le projet et à l'examen desquelles il est renvoyé.

Par contre, les hypothèses visées à l'article 123, § 1er, 1° et 2°, posent question. Elle visent la conservation et le traitement qui sont:

1° "nécessaire[s] pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées le temps nécessaire à cette fin", ou

2° "nécessaire[s] pour déceler des fraudes ou l'utilisation malveillante du réseau, les données étant conservées le temps nécessaire à cette fin".

tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

3. De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden."

2. Uit die bepaling volgt dat, wanneer de betrokken gegevens mogen worden verwerkt, die verwerking slechts plaatsvindt nadat die gegevens anoniem zijn gemaakt of de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde.

Er is dus voorzien in twee gevallen, op voorwaarde dat die gegevens "mogen worden verwerkt":

– ofwel werden de gegevens anoniem gemaakt;

– ofwel heeft de gebruiker of abonnee zijn toestemming gegeven; in dit geval mogen ze slechts worden verwerkt voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde.

De ontworpen tekst voorziet dan weer in vijf gevallen. De gevallen die zijn opgenomen in het ontworpen artikel 123, § 1, 1°, 2° en 5° van de wet van 13 juni 2005, zijn niet opgenomen in artikel 9 van richtlijn 2002/58/EG.

Eén van die drie andere overwogen gevallen levert op zich geen moeilijkheden op. Wanneer de verwerking "noodzakelijk is om te voldoen aan een wettelijke verplichting" (ontworpen artikel 123, § 1, 5°), spreekt het immers voor zich dat die verwerking aanvaardbaar is van zodra de wetsbepaling die in die verwerking voorziet, zelf voldoet aan het voorschrift van richtlijn 2002/58/EG, en in het bijzonder artikel 15, lid 1, ervan. Met andere woorden, zo er al een probleem is, zou dat niet schuilen in het ontworpen artikel 123, § 1, 5°, van de wet van 13 juni 2005, maar, in voorkomend geval, in de bepaling(en) die voorzien in "de wettelijke verplichting", welke bepalingen zich elders in het ontwerp bevinden. Er wordt dan ook verwezen naar het onderzoek van die bepalingen.

De gevallen bedoeld in artikel 123, § 1, 1° en 2°, doen daarentegen vragen rijzen. Ze hebben betrekking op de bewaring en de verwerking:

1° "wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is", of

2° "wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is".

Ces deux hypothèses évoquent celles envisagées également par l'article 4 de l'avant-projet, qui a trait, pour sa part, aux données relatives au trafic, visées par l'article 6 de la directive 2002/58/CE.

Si l'article 15, paragraphe 1, de la même directive, permet aux États membres d'adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus notamment en son article 9, c'est aux conditions prévues par cet article 15. Il faut, spécialement, que la mesure envisagée constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. Une telle mesure, qui consisterait en la conservation de données, doit par ailleurs être limitée dans le temps, à ce qui est nécessaire.

S'agissant de l'article 123 en projet, il y a lieu de relever que

1° le commentaire de l'article ne mentionne aucune des hypothèses dont il est question; à fortiori, le commentaire de l'article ne permet pas de comprendre en quoi et d'apprécier si les mesures envisagées répondraient aux conditions de l'article 15, paragraphe 1, de la directive 2002/58/CE, spécialement en ce qui concerne la nécessité, le but, et la proportionnalité;

2° la mention, dans le texte en projet, de ce que les données sont conservées "le temps nécessaire" à la finalité envisagée manque de précision; il conviendrait que le législateur fixe à toute le moins un délai de conservation maximum, qu'il doit, en outre, être en mesure de justifier.

L'article 123, § 1er, 1° et 2°, en projet, sera réexaminé à la lumière de ces deux observations.

3. Le 2°, premier tiret, entend supprimer les mots "définitivement ou temporairement" qui figurent dans l'article 123, § 2, 1°, e), de la loi du 13 juin 2005.

Le commentaire de l'article s'en explique comme suit:

"Le paragraphe 2 ne vise plus le retrait temporaire ou définitif du consentement, étant donné qu'une telle distinction n'est pas prévue dans la notion de consentement au sens du RGDP".

Cette justification perd toutefois de vue que, selon l'article 9 de la directive 2002/58/CE, les utilisateurs et abonnés qui ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

Die twee gevallen doen denken aan de gevallen waarvan ook sprake is in artikel 4 van het voorontwerp dat zijnerzijds betrekking heeft op de verkeersgegevens, zoals bedoeld in artikel 6 van richtlijn 2002/58/EG.

Artikel 15, lid 1, van dezelfde richtlijn staat de lidstaten toe wettelijke maatregelen te treffen ter beperking van de reikwijdte van de in artikel 9 van deze richtlijn bedoelde rechten en plichten, maar dan wel onder de voorwaarden van dat artikel 15. De overwogen maatregel moet met name een in een democratische samenleving noodzakelijke, redelijke en proportionele maatregel zijn ter waarborging van de nationale veiligheid – d.w.z. de staatsveiligheid – de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem. Een dergelijke maatregel, die zou bestaan in het bewaren van gegevens, moet overigens in de tijd beperkt blijven tot hetgeen noodzakelijk is.

Wat het ontworpen artikel 123 betreft, dient erop te worden gewezen dat

1° in de bespreking van het artikel geen melding wordt gemaakt van de gevallen waarvan sprake; *a fortiori* is het op grond van de bespreking van het artikel niet duidelijk in welk opzicht en of de overwogen maatregelen beantwoorden aan de voorwaarden van artikel 15, lid 1, van richtlijn 2002/58/EG, inzonderheid wat betreft de noodzakelijkheid, het doel en de evenredigheid;

2° de vermelding, in de ontworpen tekst, dat de gegevens "worden bewaard zolang dit voor [het beoogde] doel noodzakelijk is", niet nauwkeurig genoeg is; de wetgever zou op zijn minst een maximale bewaringstermijn moeten bepalen, die hij bovendien moet kunnen rechtvaardigen.

Het ontworpen artikel 123, § 1, 1° en 2°, moet worden herzien in het licht van die twee opmerkingen.

3. De bepaling onder 2°, eerste streepje, strekt tot opheffing van de woorden "definitief of tijdelijk", die voorkomen in artikel 123, § 2, 1°, e), van de wet van 13 juni 2005.

In de bespreking van het artikel staat daarover het volgende:

"Paragraaf 2 beoogt niet langer de tijdelijke of definitieve intrekking van de toestemming aangezien het begrip van toestemming in de zin van de AVG niet voorziet in een dergelijk onderscheid."

Die verantwoording gaat echter voorbij aan het feit dat volgens artikel 9 van richtlijn 2002/58/EG gebruikers en abonnees die hun toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

La disposition à l'examen sera revue de sorte que l'article 123 de la loi du 13 juin 2005 prévoie expressément cette possibilité.

Article 7

Même si le paragraphe 2 en projet habilite le Roi à définir les données à conserver et les exigences auxquelles elles doivent répondre, le dispositif en projet gagnerait à définir expressément à tout le moins la notion de "données de souscription". Il en va de même de la notion de "réseaux électroniques sous-jacents".

Article 10

1. L'article 127/1 en projet énonce, de manière assez générale, quelles catégories d'autorités ont accès aux données conservées en vertu des articles 122, 123, 126, 126/1, et 127, et en vue de quelles finalités.

Dans la philosophie du texte en projet, et comme s'en explique le commentaire de l'article,

"[p]our qu'une autorité puisse obtenir des données de l'opérateur, il est nécessaire qu'elle réponde à une des finalités visées à l'article 127/1 et que sa loi organique ou sectorielle lui donne le pouvoir d'obtenir ces données de l'opérateur".

S'il est aisément compréhensible que, dans l'intention des auteurs de l'avant-projet, les conditions de conservation des données ont vocation à figurer dans la loi du 13 juin 2005, tandis que les conditions d'accès à celles-ci ont vocation à figurer dans les législations organiques des autorités auxquelles il est envisagé de donner l'accès, il n'en demeure pas moins que, pour donner un effet utile à la finalité ou aux finalités d'une conservation, il convient que les autorités ayant accès aux données poursuivent la même finalité. Il convient également que la finalité soit définie avec suffisamment de précision et que les règles définissant les finalités de conservation et d'accès soient facilement compréhensibles.

La question se pose de savoir si le système mis en place par l'article 127/1 en projet, combiné avec les dispositions générales relatives à la conservation des données, d'une part, et avec les dispositions spécifiques qui conditionnent l'accès aux données, d'autre part, rencontre ces exigences.

2. Les objectifs des auteurs de l'avant-projet sont, par l'adoption de l'article 127/1, selon le commentaire de l'article,

"[…] d'une part, d'apporter, dans une certaine mesure, de la sécurité juridique aux opérateurs quant aux autorités disposant d'un droit d'accès aux données qu'ils conservent, et, d'autre part, d'apporter de la transparence aux utilisateurs finaux quant à l'utilisation de leurs données d'identification, de trafic et de localisation".

De voorliggende bepaling moet aldus worden herzien dat artikel 123 van de wet van 13 juni 2005 uitdrukkelijk in die mogelijkheid voorziet.

Artikel 7

Zelfs indien de ontworpen paragraaf 2 de Koning machtigt om de te bewaren gegevens te definiëren en de vereisten waaraan die moeten beantwoorden, zou het beter zijn in het ontworpen dispositief op zijn minst het begrip "abonnementsgegevens", uitdrukkelijk te definiëren. Hetzelfde geldt voor het begrip "onderliggende elektronische communicatienetwerken".

Artikel 10

1. Het ontworpen artikel 127/1 geeft een vrij algemene opsomming van de categorieën van autoriteiten die toegang hebben tot de gegevens die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, en 127, en voor welke doeleinden.

In de filosofie van de ontworpen tekst en zoals in de bespreking van het artikel wordt uiteengezet,

"is het nodig dat [de autoriteit] beantwoordt aan een van de doeleinden bedoeld in artikel 127/1 en dat haar organieke of sectorale wet haar machtigt om deze gegevens te krijgen van de operator opdat [ze] gegevens kan krijgen van de operator."

Hoewel het gemakkelijk te begrijpen valt dat het in de bedoeling van de stellers van het voorontwerp ligt om de voorwaarden voor het bewaren van de gegevens in de wet van 13 juni 2005 op te nemen, terwijl de voorwaarden voor toegang tot die gegevens thuishoren in de organieke wetgeving van de overheden waarvoor een machtiging tot toegang in overweging wordt genomen, neemt dit niet weg dat, om een nuttig gevolg te geven aan de finaliteit of finaliteiten van een bewaring, de autoriteiten die toegang hebben tot de gegevens dezelfde finaliteit dienen na te streven. Het doel dient ook voldoende nauwkeurig te worden omschreven en de regels die de doeleinden van bewaring en toegang omschrijven, moeten gemakkelijk te begrijpen zijn.

De vraag rijst of de bij het ontworpen artikel 127/1 ingevoerde regeling, in samenhang met enerzijds de algemene bepalingen inzake de bewaring van de gegevens, en anderzijds de specifieke bepalingen die de toegang tot de gegevens bepalen, aan die vereisten voldoet.

2. Volgens de bespreking van het artikel hebben de stellers van het voorontwerp, bij het aannemen van artikel 127/1, de volgende doelstellingen:

"(…) enerzijds om, in een zekere mate, de operatoren rechtszekerheid te bieden wat betreft de autoriteiten die het recht hebben om toegang te krijgen tot de gegevens die ze bewaren en anderzijds om de eindgebruikers transparantie te geven over het gebruik van hun identificatie-, verkeers- en locatiegegevens".

La section de législation se demande toutefois si, telle qu'elle est rédigée, cette disposition ne risque pas d'entrainer un effet pervers, allant à l'encontre de la sécurité juridique.

Ainsi, même si elle renvoie expressément, en matière d'accès, aux conditions prévues par les dispositions spécifiques qui habilitent les catégories d'autorités concernées à avoir accès aux données conservées, l'article 127/1 en projet peut donner l'impression que toutes les catégories d'autorités y visées ont accès à toutes les données visées aux articles 122, 123, 126, 126/1.

Or, ceci peut être source de confusion.

Ainsi, la conservation généralisée et indifférenciée des adresses IP source visées à l'article 123 de la loi du 13 juin 2005, tel que le projet envisage de le modifier, et les données qui font l'objet d'une conservation ciblée, visée par l'article 126/1 en projet ne peuvent être conservées qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique.

Cette limitation n'apparait pas à la lecture de l'article 127/1 dont le paragraphe 1er, 1°, se réfère, de manière tout à fait générale, à la prévention, la recherche, la détection de la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infraction commises à l'aide d'un réseau de communications électroniques.

Certes, s'agissant de la conservation géographique ciblée, l'article 126/1 mentionne que les données concernées sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personnes physiques. Par ailleurs, concernant le ministère public par exemple, le respect du critère de "criminalité grave", résulte également de l'article 39*quinquies* en projet, du Code d'instruction criminelle (article 17 de l'avant-projet).

Il reste toutefois que, dès lors que l'article 127/1, § 1er, en projet, entend décrire la finalité de l'accès, celle-ci doit pourvoir être mise en rapport avec la finalité du régime de conservation mis en place. Or, s'agissant de la conservation des adresses IP source, aucune finalité spécifique n'est mentionnée à l'article 126, § 1er, en projet, qui renvoie seulement aux finalités visées à l'article 127/1 en projet. Ce renvoi s'avère insuffisant aux regard des exigences de la Cour de Justice en ce qui concerne les fins de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique.

La disposition en projet doit dès lors revue aux fins de faire apparaitre clairement le lien entre la finalité de la conservation et la finalité de l'accès, et de lever toute ambiguïté qui serait de nature à laisser supposer, par exemple, que dans des cas où la conservation ne pourrait avoir lieu qu'à des fins de

De afdeling Wetgeving vraagt zich echter zich af of die bepaling, zoals ze is geformuleerd, niet een pervers effect zou kunnen hebben dat in strijd is met de rechtszekerheid.

Aldus kan het ontworpen artikel 127/1, ook al verwijst het, wat de toegang betreft, uitdrukkelijk naar de voorwaarden die zijn vastgesteld in de specifieke bepalingen op grond waarvan de categorieën van betrokken autoriteiten toegang hebben tot de bewaarde gegevens, de indruk wekken dat alle daarin genoemde categorieën van autoriteiten toegang hebben tot alle in de artikelen 122, 123, 126, en 126/1 bedoelde gegevens.

Dit kan evenwel tot verwarring leiden.

Zo kunnen de algemene en ongedifferentieerde bewaring van de IP-bron adressen bedoeld in artikel 123 van de wet van 13 juni 2005, zoals het bij het ontwerp wordt gewijzigd, en de gegevens die het voorwerp uitmaken van een gerichte bewaring als bedoeld in het ontworpen artikel 126/1, enkel worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid.

Die beperking blijkt niet uit de lezing van artikel 127/1, waarvan paragraaf 1, 1°, heel algemeen verwijst naar de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronisch-communicatienetwerk.

Wat de doelgerichte geografische bewaring betreft, vermeldt artikel 126/1 dat de betrokken gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon. Wat het openbaar ministerie betreft, volgt de naleving van het criterium "zware criminaliteit" tevens uit het ontworpen artikel 39*quinquies*, van het Wetboek van Strafvordering (artikel 17 van het voorontwerp).

Aangezien het ontworpen artikel 127/1, § 1, ertoe strekt de finaliteit van de toegang te omschrijven, neemt dat niet weg dat die finaliteit in verband moet kunnen worden gebracht met de finaliteit van de ingevoerde regeling voor de bewaring van de gegevens. Wat evenwel de bewaring van IP-bron adressen betreft, wordt in het ontworpen artikel 126, § 1, die enkel verwijst naar de doeleinden bedoeld in het ontworpen artikel 127/1, geen enkele specifieke finaliteit genoemd. Die verwijzing is ontoereikend in het licht van de eisen van het Hof van Justitie met betrekking tot de bescherming van de nationale veiligheid, de bestrijding van ernstige criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid.

De ontworpen bepaling moet derhalve worden herzien om het verband tussen het doeleinde van de bewaring en het doeleinde van de toegang duidelijk te maken en om elke dubbelzinnigheid weg te nemen die ertoe zou kunnen leiden dat bijvoorbeeld in gevallen waarin de bewaring enkel kan

lutte contre la criminalité grave, des autorités pourraient y avoir accès en vue de lutter contre une criminalité non grave.

2. L'appréciation de la notion de "sanction administrative à caractère pénal" – à savoir, selon le commentaire de l'article, une sanction qualifiée d'administrative en droit interne, mais susceptible d'être qualifiée de pénale au sens de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales – ne peut être laissée ni à l'opérateur qui donnerait l'accès aux données conservées ni à l'autorité qui demanderait l'accès aux données.

Cette notion éminemment jurisprudentielle dépend ainsi d'une appréciation au cas par cas, qui ne se concilie pas avec la prévisibilité et la précision attendue d'une législation qui met en place un système d'ingérence dans le droit au respect de la vie privée.

3. Compte tenu des éléments ainsi mis en exergue, la section de législation se demande si la disposition à l'examen n'est pas plus de nature à nuire à la sécurité juridique qu'à garantir celle-ci.

Elle sera réexaminée à la lumière des observations qui précèdent.

Article 11

1. La section de législation n'aperçoit pas la portée de l'alinéa 3 de l'article 127/2, § 2, en projet, qui prévoit:

"Les opérateurs sont en mesure d'établir des liens entre les données conservées pour les autorités".

Le commentaire de l'article mentionne à ce propos:

"Il revient aux opérateurs de décider comment ils s'organisent pour la conservation des données au bénéfice des autorités (en particulier les données conservées conformément aux articles 126, 126/1, 127). Dès lors, si une même donnée est visée dans plusieurs articles, ils peuvent conserver la donnée une seule fois. Par contre, les opérateurs doivent être mesure d'établir des liens entre les données conservées pour les autorités. Ceci est nécessaire vu que pour répondre à une demande d'une autorité, un opérateur pourrait être amené à consulter des données conservées sur base de différents articles".

Ce faisant, le commentaire de l'article ne permet pas de mieux comprendre quelle sera la nature du "lien" à établir par l'opérateur entre les données conservées.

Il convient à tout le moins que la disposition à l'examen n'impose pas d'obligation telle que l'opérateur s'en trouverait ainsi chargé d'apprécier le contenu des données concernées et la pertinence, en opportunité, d'établir un lien entre

plaatsvinden ter bestrijding van zware criminaliteit, de autoriteiten toegang tot die gegevens zouden kunnen krijgen om niet-zware criminaliteit te bestrijden.

2. De beoordeling van het begrip "administratieve sanctie met strafkarakter" – d.i., volgens de bespreking van het artikel, een sanctie die in het interne recht als administratieve sanctie wordt bestempeld, maar die als strafrechtelijk kan worden aangemerkt in de zin van het Verdrag inzake de bescherming van de Rechten van de Mens en de Fundamentele Vrijheden – mag niet worden overgelaten aan de operator die toegang tot de bewaarde gegevens zou verlenen, noch aan de autoriteit die toegang tot de gegevens zou vragen.

Dat bij uitstek jurisprudentiële begrip hangt dus af van een beoordeling van elk geval afzonderlijk, wat niet verenigbaar is met de voorzienbaarheid en de nauwkeurigheid die wordt verwacht van een wettelijke regeling die voorziet in een systeem van inmenging in het recht op eerbiediging van het privéleven.

3. Gelet op de aldus benadrukte elementen, vraagt de afdeling Wetgeving zich af of de voorliggende bepaling niet eerder van aard is om de rechtszekerheid te ondermijnen, in plaats van deze te waarborgen.

Die bepaling moet in het licht van de voorgaande opmerkingen opnieuw worden onderzocht.

Artikel 11

1. Het is de afdeling Wetgeving niet duidelijk wat de strekking is van het derde lid van het ontworpen artikel 127/2, § 2, dat als volgt luidt:

"De operatoren zijn in staat verbanden te leggen tussen de gegevens bewaard voor de autoriteiten."

In de bespreking van het artikel wordt in dat verband het volgende vermeld:

"Het is aan de operatoren om te beslissen hoe ze zich organiseren voor de bewaring van de gegevens ten behoeve van de autoriteiten (in het bijzonder de gegevens bewaard conform de artikelen 126, 126/1, 127). Wanneer eenzelfde gegeven wordt bedoeld in verscheidene artikelen, mogen ze dat gegeven dus één keer bewaren. De operatoren moeten daarentegen in staat zijn om verbanden te leggen tussen de gegevens bewaard voor de autoriteiten. Dat is nodig aangezien een operator, om te antwoorden op een verzoek van een autoriteit, genoopt zou kunnen zijn om gegevens te raadplegen die zijn bewaard op basis van verschillende artikelen."

Aldus laat de bespreking van het artikel niet toe om beter te begrijpen wat de aard is van het "verband" dat de operator moet leggen tussen de bewaarde gegevens.

De voorliggende bepaling mag op zijn minst geen verplichting opleggen die de operator zou belasten met de beoordeling, uit opportuniteitsoverwegingen, van de inhoud van de desbetreffende gegevens en van de relevantie om tussen die

celles-ci. En d'autres termes, le lien à établir ne peut être que technique ou technologique, et l'établissement de celui-ci ne peut amener l'opérateur à se livrer, en quelque sorte, à un examen ou une analyse des données auxquelles seules les autorités qui y ont accès peuvent se livrer.

Selon les délégués du ministre interrogés à ce propos, telle n'est pas l'intention. La disposition à l'examen et le commentaire de l'article seront revus aux fins de faire apparaitre sans ambiguïté l'intention qui y préside.

3. Concernant la destruction des données, prévue par l'article 127/2, § 3, alinéa 2, 1°, en projet, le dispositif répondrait mieux aux exigences relatives à la destruction irrémédiable des données si, une autorité, tel l'Institut, était spécifiquement chargée de contrôler régulièrement cette destruction[43].

Article 12

Selon le paragraphe 3 de l'article 127/3 en projet,

"Le Roi peut déterminer, après avis des autorités de protection des données compétentes et de l'Institut:

1° les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité;

2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en ce compris lui imposer, le cas échéant, de faire l'objet d'un avis de sécurité positif;

3° si un avis de sécurité positif est imposé, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un officier de sécurité comme prévu à l'article 22*quinquies*, § 6, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ainsi que les règles qui s'appliquent en l'absence d'un tel officier;

4° les règles permettant que les autorités belges qui ont besoin de connaître les coordonnées de la Cellule de coordination et de ses membres en soient informés;

5° les autres règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles, y compris, le cas échéant et par autorité concernée

a) le mode de transfert, la forme et le contenu des demandes et des réponses;

[43] Voir, en ce sens, l'avis n° 58.449/4, point 3.4.2.2.2.

gegevens een verband te leggen. Met andere woorden, het te leggen verband kan enkel technisch of technologisch van aard zijn, en het leggen van dat verband mag de operator er als het ware niet toe brengen om de gegevens waartoe alleen de autoriteiten die daartoe gemachtigd zijn, toegang hebben, te onderzoeken of te analyseren.

Op een vraag in dat verband hebben de gemachtigden van de minister geantwoord dat dit niet de bedoeling is. De voorliggende bepaling en de bespreking van het artikel moeten worden herzien om de bedoeling van de steller ervan duidelijk weer te geven.

3. Wat de in het ontworpen artikel 127/2, § 3, tweede lid, 1°, beoogde vernietiging van de gegevens betreft, zou het dispositief beter tegemoetkomen aan de vereisten inzake de onherroepelijke vernietiging van de gegevens indien een autoriteit, zoals het Instituut, specifiek zou worden belast met de regelmatige controle op die vernietiging.[43]

Artikel 12

Paragraaf 3 van het ontworpen artikel 127/3 luidt als volgt:

"De Koning kan na advies van de bevoegde gegevensbeschermingsautoriteiten, en van het Instituut het volgende bepalen:

1° de vereisten waaraan de Coördinatiecel moeten beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid;

2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inclusief hem in voorkomend geval verplichten om het voorwerp uit te maken van een positief veiligheidsadvies;

3° indien een positief veiligheidsadvies wordt opgelegd, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een veiligheidsofficier aan te stellen zoals bepaald in artikel 22*quinquies*, § 6, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

4° de regels die het mogelijk maken dat de Belgische autoriteiten die de contactgegevens van de Coördinatiecel en van de leden ervan moeten kennen, daarvan op de hoogte worden gebracht;

5° de overige regels die de samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen regelen, met inbegrip van, in voorkomend geval en per betrokken overheid:

a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;

[43] Zie in die zin advies 58.449/4, punt 3.4.2.2.2.

b) le degré d'urgence de traitement des demandes;

c) le délai de réponse;

d) la disponibilité requise du service;

e) les modalités de test de la collaboration;

f) les tarifs de rétribution de cette collaboration;

Si nécessaire, le Roi peut prévoir des règles différentes selon différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et le lieu où ils opèrent leurs activités".

Cette disposition appelle plusieurs observations.

2. L'article 127/3, § 3, en projet, prévoit que le Roi "peut" fixer les règles dont l'objet y est énuméré, et non pas qu'Il "fixe" celles-ci.

Par conséquent, en l'absence de mise en œuvre par le Roi de la possibilité qui Lui est conférée par la disposition en projet, aucune règle ne sera fixée concernant les différents points énumérés.

À titre d'exemple, il pourrait ainsi advenir qu'aucune règle ne soit fixée concernant les exigences auxquelles les membres de la Cellule de coordination doivent répondre.

Or, ces exigences sont essentielles en vue d'assurer que la Cellule de coordination collaborera de manière effective et efficace avec les autorités, et qu'elle disposera de toutes les garanties appropriées pour la conservation et la transmission sécurisée des données concernées, conformément au prescrit de la loi en projet.

Par conséquent, il convient que l'habilitation en projet soit rédigée de manière telle que le Roi ne soit pas simplement autorisé à fixer les règles concernées, mais qu'il soit tenu de les fixer.

3. Il appartient au législateur de déterminer les critères à mettre en œuvre par le Roi lorsqu'Il pourvoira à l'exécution de la disposition en projet, spécialement s'agissant des règles prévues au paragraphe 3, alinéa 1er, 2° et 3°, en projet.

Il en va particulièrement ainsi de la question de principe de savoir si un avis de sécurité positif sera ou non requis, indépendamment même des règles différentes qui seraient imposées à des catégories d'opérateurs différentes, sur la base des critères prévus à l'alinéa 2 du paragraphe 3 en projet[44].

[44] Dans un sens similaire, voir l'avis n° 58.449/4, observation sous l'article 5.

b) het dringendheidsniveau voor de behandeling van de verzoeken;

c) de reactietermijn voor de antwoorden;

d) de vereiste beschikbaarheid van de dienst;

e) de modaliteiten voor het testen van de samenwerking;

f) de tarieven van de vergoeding van die samenwerking.

Indien nodig kan de Koning verschillende regels bepalen volgens verschillende categorieën van operatoren, met name volgens het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en de plaats waar zij hun activiteiten uitvoeren."

Die bepaling geeft aanleiding tot verschillende opmerkingen.

2. In het ontworpen artikel 127/3, § 3, wordt bepaald dat de Koning de regels waarvan het voorwerp erin is opgenomen, "kan" bepalen en niet dat Hij die regels "bepaalt".

Bij gebrek aan uitvoering door de Koning van de mogelijkheid die Hem wordt verleend bij die ontworpen bepaling, zal bijgevolg geen enkele regel met betrekking tot de verschillende opgesomde punten worden vastgesteld.

Zo zou het bijvoorbeeld kunnen dat er geen enkele regel betreffende de vereisten waaraan de leden van de Coördinatiecel moeten voldoen, wordt bepaald.

Die vereisten zijn evenwel van essentieel belang teneinde te verzekeren dat de Coördinatiecel doeltreffend en efficiënt zal samenwerken met de autoriteiten en dat ze over alle passende waarborgen zal beschikken voor de bewaring en de veilige overdracht van de betrokken gegevens, overeenkomstig de bepalingen van de ontworpen wet.

Bijgevolg dient de ontworpen machtiging zodanig te worden opgesteld dat de Koning niet alleen gemachtigd, maar ertoe gehouden is om de desbetreffende regels vast te leggen.

3. Het staat aan de wetgever om de criteria te bepalen die de Koning moet hanteren wanneer Hij uitvoering moet geven aan de ontworpen bepaling, in het bijzonder wat betreft de regels die vervat zijn in de ontworpen paragraaf 3, eerste lid, 2° en 3°.

Dat geldt in het bijzonder voor de principiële vraag of al dan niet een positief veiligheidsadvies wordt opgelegd, zelfs los van het feit dat de verschillende regels die, op basis van de criteria waarin het tweede lid van de ontworpen derde paragraaf voorziet, aan verschillende categorieën van operatoren zouden worden opgelegd.[44]

[44] Zie in soortgelijke zin advies 58.449/4, opmerking bij artikel 5.

4. La disposition en projet sera revue et complétée à la lumière des observations qui précèdent.

Article 13

L'article 13 de l'avant-projet envisage d'insérer dans la loi du 13 juin 2005 un article 127/4 nouveau, rédigé comme suit:

"Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les conditions dans lesquelles les fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public enregistrent et conservent les données permettant l'identification des personnes concernées de l'équipement terminal ou du service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, en vue de la poursuite et la répression d'infractions pénales, et en vue de la répression d'appels malveillants vers les services d'urgence, en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les mesures techniques et administratives imposées aux fournisseurs visées à l'alinéa 1er, en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par les articles 46*bis*, 88*bis*, 90*ter* à 90*decies*, 464/13, 464/25 et 464/26 du Code d'instruction criminelle, ainsi qu'aux conditions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs visés à l'alinéa 1er font en sorte que les données mentionnées à l'alinéa 1er soient accessibles de manière illimitée depuis la Belgique".

Ces habilitations sont manifestement excessives. S'agissant des fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public, elles ont en effet pour objet d'habiliter le Roi à fixer intégralement les régimes applicables:

– en matière d'enregistrement et de conservation des données permettant l'identification des personnes concernées, de l'équipement terminal ou du service de communications électroniques employé, en vue, de surcroit, de la poursuite et

4. De voorliggende bepaling moet worden herzien in het licht van de voorgaande opmerkingen.

Artikel 13

Artikel 13 van het voorontwerp strekt ertoe in de wet van 13 juni 2005 een nieuw artikel 127/4 in te voegen dat als volgt luidt:

"Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de voorwaarden vast waaronder de aanbieders van private elektronische-communicatienetwerken en elektronische-communicatiediensten die niet openbaar beschikbaar zijn de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische-communicatiedienst, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten en met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, voor het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de technische en administratieve maatregelen vast die aan de aanbieders beoogd in het eerste lid worden opgelegd om de betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke [communicatie] mogelijk te maken onder de voorwaarden bepaald door de artikelen 46*bis*, 88*bis*, 90*ter* tot 90*decies*, 464/13, 464/25 en 464/26 van het Wetboek van strafvordering, evenals de voorwaarden bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De aanbieders beoogd in het eerste lid zorgen ervoor dat de in het eerste lid van deze paragraaf vermelde gegevens onbeperkt toegankelijk zijn vanuit België."

Die machtigingen zijn kennelijk te verregaand. Met betrekking tot de aanbieders van private elektronische-communicatienetwerken en elektronische-communicatiediensten die niet voor het publiek toegankelijk zijn, hebben ze immers tot doel de Koning te machtigen om volledig de regelingen te bepalen die gelden:

– inzake de registratie en de bewaring van de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische-communicatiedienst, ook met het oog op het opsporen en de

la répression d'infractions pénales, de la répression d'appels malveillants vers les services d'urgence, de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, et de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998;

– en ce qui concerne les mesures en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998.

Eu égard au principe de légalité inscrit à l'article 22 de la Constitution, de telles ingérences dans le droit au respect de la vie privée, plus spécialement la conservation et l'accès à des données à caractère personnel doivent être organisées par un régime encadré à suffisance par le législateur.

Un tel régime fait totalement défaut en l'espèce.

Par conséquent, la disposition à l'examen sera fondamentalement revue.

Article 14

1. Au paragraphe 2, alinéa 3, en projet, il convient de remplacer les mots "visés à l'alinéa 1er" par les mots "visés à l'alinéa 2".

2. Au paragraphe 2, alinéa 6, en projet, il convient de définir la nature de la nullité envisagée: s'agit-il d'une nullité de plein droit et d'ordre public, comme on peut le supposer?

Article 16

1. L'article 16 entend insérer un 2°/1 dans l'article 14, § 2, de la loi du 17 janvier 2003 'relative au statut du régulateur des secteurs des postes et des télécommunications belges', en vue de permettre à l'Institut de "demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions".

L'Institut pourrait ainsi avoir accès à l'ensemble des données énumérées, sans qu'une distinction soit opérée entre les catégories de données et sans que soit explicitée la finalité précise, qui justifie l'accès.

L'article 127/1, § 1er, en projet, ne permet pas de mieux circonscrire l'ingérence à laquelle l'Institut est ainsi habilité à procéder puisque cet article 127/1, § 1er, en projet, se

beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, voor het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998;

– met betrekking tot de maatregelen om de betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie mogelijk te maken onder de voorwaarden bepaald in het Wetboek van Strafvordering en in de wet van 30 november 1998.

Gelet op het in artikel 22 van de Grondwet vervatte legaliteitsbeginsel, moet voor dergelijke inmengingen in het recht op eerbiediging van het privéleven, meer bepaald het bewaren van en de toegang tot persoonsgegevens, voorzien worden in een regeling die naar behoren afgebakend wordt door de wetgever.

In casu ontbreekt een dergelijke regeling totaal.

De voorliggende bepaling moet bijgevolg grondig herzien worden.

Artikel 14

1. In de ontworpen paragraaf 2, derde lid, dienen de woorden "De in het eerste lid bedoelde" vervangen te worden door de woorden "De in het tweede lid bedoelde".

2. In de ontworpen paragraaf 2, zesde lid, dient de aard omschreven te worden van de nietigheid waarvan sprake is: gaat het, zoals verondersteld kan worden, om nietigheid van rechtswege en van openbare orde?

Artikel 16

1. Artikel 16 strekt ertoe een punt 2°/1 in te voegen in artikel 14, § 2, van de wet van 17 januari 2003 'met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector' teneinde het voor het Instituut mogelijk te maken om "van de operatoren de identificatie-, verkeers- of locatiegegevens [te] vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten".

Het Instituut zou aldus toegang kunnen hebben tot alle gegevens die opgesomd worden, zonder dat een onderscheid gemaakt wordt tussen de categorieën van gegevens en zonder dat uitdrukkelijk aangegeven wordt welke precieze bedoeling die toegang rechtvaardigt.

Het ontworpen artikel 127, § 1, maakt geen betere afbakening mogelijk van de inmenging waartoe het Instituut aldus gemachtigd wordt, aangezien in dat ontworpen artikel 127/1,

borne à prévoir que la conservation des données visées aux articles 122, 123, 126, 126/1 et 127, de la loi du 13 juin 2005, tels qu'ils résulteront de leur modification par le texte en projet, a pour finalité, s'agissant de l'Institut, la mise en œuvre et le contrôle de la loi du 13 juin 2005.

Quant au commentaire de l'article, il mentionne:

"La disposition insérée vise à permettre à l'Institut d'avoir accès aux données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, lorsque cela s'avère nécessaire à l'accomplissement de l'une de ses missions.

Tel est le cas notamment en cas de contrôle du respect par les opérateurs de leurs obligations légales, telles que l'obligation d'adresser une facturation détaillée, prévue à l'article 110 de la loi du 13 juin 2005 relative aux communications électroniques, ou dans le cadre de la mise en œuvre de l'article 114 de cette même loi. Par exemple, en matière de facturation détaillée, l'IBPT doit être en mesure de demander à l'opérateur de lui fournir un échantillon de factures. Or, ces factures reprennent des données de trafic, telles que les destinataires, dates, heures et durées des communications passées".

2. Force est de constater qu'un accès aussi général que celui prévu par le texte en projet ne parait pas se justifier sur le plan de la proportionnalité, au regard de l'article 15, paragraphe 1, de la directive 2002/58/CE compris à la lumière de la jurisprudence y relative de la Cour de Justice.

L'exemple mentionné au commentaire de l'article, qui apparait extrêmement ciblé, dément au contraire la nécessité de l'ampleur de l'accès autorisé.

Tout aussi fondamentalement, la question se pose de savoir quelles sont les garanties effectives dont les personnes concernées bénéficieraient contre les éventuels abus.

3. La disposition à l'examen sera revue à la lumière des observations qui précèdent.

Article 24

1. Il résulte du commentaire de l'article que l'article 16/2/1 en projet de la loi du 30 novembre 1998, vise, en son alinéa 1er, 1°, une injonction de "*quick freeze*" classique des données déjà conservées par les opérateurs, tandis que l'alinéa 1er, 2°, concerne une injonction de "*quick freeze*" pour l'avenir.

Cette distinction n'apparait pas clairement du dispositif en projet, spécialement la portée exacte de l'injonction prévue par l'alinéa 1er, 2°, en projet.

§ 1, enkel bepaald wordt dat, wat het Instituut betreft, de bewaring van de gegevens bedoeld in de artikelen 122, 123, 126, 126/1 en 127, van de wet van 13 juni 2005, zoals die zullen luiden nadat ze bij de ontworpen tekst gewijzigd zullen zijn, "de uitvoering en de toetsing van de wet" van 13 juni 2005 als doel heeft.

In de bespreking van het artikel staat in dat verband het volgende:

"De ingevoegde bepaling beoogt dat het Instituut toegang kan hebben tot de identificatie-, verkeers- of locatiegegevens in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, wanneer dat nodig blijkt voor de vervulling van een van zijn opdrachten.

Dat is met name het geval bij de controle van de inachtneming door de operatoren van hun wettelijke verplichtingen zoals de verplichting om een gedetailleerde facturering op te stellen, vastgelegd in artikel 110 van de wet van 13 juni 2005 betreffende de elektronische communicatie, of in het kader van de tenuitvoerbrenging van artikel 114 van diezelfde wet. Zo moet het BIPT, in het geval van de gedetailleerde facturering, in staat zijn om een operator een staal van zijn facturen te vragen. Deze facturen bevatten verkeersgegevens, zoals de ontvangers, data, tijdstippen en duur van de gevoerde gesprekken."

2. Vastgesteld moet worden dat een toegang die zo algemeen is als die waarin door de ontworpen tekst voorzien wordt, wat de proportionaliteit betreft, niet verantwoord lijkt ten aanzien van artikel 15, lid 1, van richtlijn 2002/58/EG, zoals begrepen in het licht van de desbetreffende rechtspraak van het Hof van Justitie.

Het in de bespreking van het artikel vermelde voorbeeld, dat uitermate gericht blijkt te zijn, ontkracht daarentegen de noodzaak om zo'n ruime toegang toe te staan.

Even fundamenteel is de vraag welke daadwerkelijke waarborgen de betrokken personen zouden genieten tegen eventuele misbruiken.

3. De voorliggende bepaling moet in het licht van de voorgaande opmerkingen herzien worden.

Artikel 24

1. Uit de bespreking van het artikel blijkt dat het eerste lid, 1°, van het ontworpen artikel 16/2/1 van de wet van 30 november 1998 betrekking heeft op een bevel tot een klassieke "*quick freeze*" van de reeds door de operatoren bewaarde gegevens, terwijl het eerste lid, 2°, ervan betrekking heeft op een bevel tot een "*quick freeze*" voor de toekomst.

In het ontworpen dispositief komt dat onderscheid niet duidelijk tot uiting, inzonderheid niet wat de exacte draagwijdte is van het bevel waarin het ontworpen eerste lid, 2°, voorziet.

2. Par ailleurs, concernant la durée de conservation des données, il convient de distinguer les deux hypothèses précitées.

Ainsi, pour l'opération de "*quick freeze*" classique, l'alinéa 4 de la disposition en projet répond à la question de savoir quel sera le délai de conservation des données dont la conservation a été ordonnée.

Par contre, s'agissant de l'opération de "*quick freeze*" pour l'avenir, la disposition en projet manque de clarté: elle ne permet pas de faire la distinction entre la durée de la mesure de "*quick freeze*", d'une part, et la durée de conservation des données ainsi gelées, d'autre part. Sur ce point, aux fins de garantir que l'opération de "*quick freeze*" pour l'avenir n'excède pas ce qui est strictement nécessaire à la sécurité nationale, le texte en projet devrait être complété aux fins de fixer une durée maximum de l'opération, sous réserve d'un éventuel renouvellement[45]. Un autre biais pourrait consister à limiter la conservation des données à la durée du "*quick freeze*". Il convient en tout cas de lever toute ambiguïté sur cette question.

Enfin, la section de législation n'aperçoit pas, dans le contexte du système ainsi mis en place, la portée exacte de l'alinéa 8 qui prévoit que les données conservées par les opérateurs sont détruites douze mois après le début de leur conservation.

3. La disposition en projet sera revue aux fins de lever toute ambiguïté quant au système mis en place, notamment quant à la durée de l'opération de "*quick freeze*" pour l'avenir, à la durée de conservation des données, ce en vue de garantir que ces durées soient limitées au strict nécessaire, et que les données soient détruites par les opérateurs dès que cette nécessité n'est plus rencontrée.

Article 28

Comme l'avait déjà souligné la section de législation dans son avis n° 42.178/2 donné le 19 février 2007 sur un avant-projet devenu la loi du 4 février 2010 'relative aux méthodes de recueil des données par les services de renseignement et de sécurité'[46], les principes de proportionnalité et de subsidiarité conditionnent le recours aux méthodes spécifiques et, à fortiori, aux méthodes exceptionnelles, en vue de garantir que celles-ci seront mises en œuvre dans des conditions respectueuses des droits fondamentaux.

Pour garantir le respect de ces principes, la disposition en projet devrait être complétée aux fins de prévoir la durée maximale – moyennant le cas échéant prolongation justifiée

[45] Comparer avec l'article 39*quinquies*, alinéa 3, 6ème et 7ème tirets, en projet, du Code d'instruction criminelle (article 17 de l'avant-projet).

[46] *http://www.raadvst-consetat.be/dbx/avis/42178.pdf*.

2. Bovendien dient met betrekking tot de duur van bewaring van de gegevens een onderscheid gemaakt te worden tussen de twee voormelde gevallen.

Zo wordt met betrekking tot de klassieke "*quick freeze*" in het vierde lid van de ontworpen bepaling een antwoord gegeven op de vraag hoelang de gegevens bewaard moeten worden waarvoor een bevel tot bewaring gegeven werd.

Wat daarentegen de "*quick freeze*" voor de toekomst betreft, is de ontworpen bepaling niet duidelijk genoeg: op basis van die bepaling is het niet mogelijk om een onderscheid te maken tussen de duur van de "*quick freeze*" maatregel enerzijds en de duur van bewaring van de aldus bevroren gegevens anderzijds. Om ervoor te zorgen dat de "*quick freeze*" voor de toekomst niet verder gaat dan wat strikt noodzakelijk is voor de nationale veiligheid, zou de ontworpen tekst op dat punt aangevuld moeten worden teneinde, onder voorbehoud van een eventuele verlenging, een maximumduur vast te stellen voor de bewaring.[45] Een andere mogelijkheid zou erin kunnen bestaan om de bewaring van de gegevens te beperken tot de duur van de "*quick freeze*". Elke dubbelzinnigheid ter zake dient hoe dan ook weggenomen te worden.

In de context van de aldus ingevoerde regeling , is het de afdeling Wetgeving ten slotte niet duidelijk wat de exacte draagwijdte is van het achtste lid waarin bepaald wordt dat de door de operatoren bewaarde gegevens twaalf maanden na het begin van hun bewaring vernietigd worden.

3. De ontworpen bepaling moet herzien worden teneinde elke dubbelzinnigheid over de ingevoerde regeling weg te nemen, in het bijzonder wat betreft de duur van de "*quick freeze*" voor de toekomst en wat betreft de bewaartermijn van de gegevens, en dit om te garanderen dat die termijn tot het strikt noodzakelijke beperkt wordt en dat de gegevens door de operatoren vernietigd worden zodra die noodzaak komt te vervallen.

Artikel 28

De afdeling wetgeving heeft in haar advies 42.178/2 van 19 februari 2007 over een voorontwerp dat geleid heeft tot de wet van 4 februari 2010 'betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten'[46], reeds benadrukt dat, hoewel de evenredigheids-en subsidiariteitsbeginselen bepalend zijn voor het aanwenden van de specifieke methodes en, *a fortiori*, de uitzonderlijke methodes, het bovendien van belang is na te gaan of de bij het voorontwerp ingevoerde controlemiddelen de effectieve waarborg bieden dat deze methodes zullen worden aangewend met inachtneming van de fundamentele rechten.

Om de naleving van die beginselen te garanderen, zou de ontworpen bepaling moeten worden aangevuld om te voorzien in een maximumduur – waarbij in voorkomend geval wordt

[45] Vergelijk met het ontworpen artikel 39*quinquies*, derde lid, zesde en zevende streepje, van het Wetboek van Strafvordering (artikel 17 van het voorontwerp).

[46] *http://www.raadvst-consetat.be/dbx/adviezen/42178.pdf*.

par la stricte nécessité – du repérage ou de la localisation, durée qui serait proportionnée à la gravité des éléments justifiant le recours à la méthode.

Par ailleurs, au titre des garanties procédurales, la section de législation n'aperçoit pas ce qui peut justifier que, pour la méthode spécifique envisagée, une décision écrite du dirigeant du service ne soit pas requise, comme c'est le cas pour d'autres méthodes spécifiques.

La disposition à l'examen sera revue à la lumière de ces observations.

Article 34

L'article 62, paragraphe 2, alinéa 2, en projet, de la loi du 7 avril 2019 'établissant un cadre pour la sécurité des réseaux et des systèmes d'informations d'intérêt général pour la sécurité publique' prévoit que pour avoir accès aux données d'identification, de trafic et de localisation conservées par les opérateurs, le Centre pour la Cybersécurité (en abrégé "CSIRT") national "respecte les règles et les procédures prévues par la loi du 13 juin 2005 relative aux communications électroniques".

Cette disposition manque de précision. Elle doit viser les dispositions précises de la loi du 13 juin 2005 qui auront vocation à s'appliquer au CSIRT national, le cas échéant, selon différentes hypothèses.

L'article 62 en projet sera revu et complété en conséquence.

Article 36

1. L'article 36 prévoit que la loi en projet "entre en vigueur [lire: "produit ses effets"] le jour où l'annulation de la loi du 29 mai 2016 par l'arrêt n°57/2021 de la Cour constitutionnelle prend effet".

Le commentaire de l'article mentionne:

"La loi prend effet rétroactivement afin de ne pas créer un vide juridique dans lequel des données importantes de communications électroniques qui pourraient être cruciales pour l'enquête ne soient plus conservées".

Tel qu'il est rédigé, l'article 36 entend faire rétroagir la loi à l'examen au jour où l'annulation de la loi du 29 mai 2016 a elle-même pris effet, soit, au jour de l'entrée en vigueur de cette loi.

2.2. En effet, l'avant-projet à l'examen se donne pour objet la mise en place d'un système articulé de conservation et d'accès à des données à caractère personnel dans la sphère des communications électroniques.

voorzien in een verlenging die wordt gerechtvaardigd door de strikte noodzakelijkheid – van de opsporing of lokalisatie, welke duur in verhouding zou staan tot de ernst van de gegevens die de aanwending van de methode rechtvaardigen.

Bovendien ziet de afdeling Wetgeving, wat de procedurele waarborgen betreft, niet in hoe het gerechtvaardigd kan worden dat voor de voorgenomen specifieke methode geen schriftelijke beslissing van het diensthoofd vereist is, zoals het geval is voor andere specifieke methoden.

De voorliggende bepaling moet worden herzien in het licht van die opmerkingen.

Artikel 34

Het ontworpen artikel 62, paragraaf 2, tweede lid, van de wet van 7 april 2019 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid' bepaalt dat het nationaal Computer Security Incident Response Team (afgekort "CSIRT") om toegang te krijgen tot de door de operatoren bewaarde identificatie- , verkeers- en locatiegegevens, zich houdt aan "de regels en procedures bedoeld in de wet van 13 juni 2005 betreffende de elektronische communicatie".

Die bepaling laat qua duidelijkheid te wensen over. Ze moet verwijzen naar de precieze bepalingen van de wet van 13 juni 2005 die, in voorkomend geval, uitgaande van verschillende hypotheses, van toepassing zullen zijn op het Nationaal CSIRT.

Het ontworpen artikel 62 moet dienovereenkomstig worden herzien en aangevuld.

Artikel 36

1. Artikel 36 bepaalt dat de ontworpen wet "in werking treedt [lees: "uitwerking heeft"] op de dag waarop de vernietiging van de wet van 29 mei 2016 door het arrest nr. 57/2021 van het Grondwettelijk Hof gevolgen ressorteert".

De bespreking van het artikel stelt het volgende:

"De wet treedt retroactief in werking, zodat er geen juridisch vacuüm ontstaat waardoor belangrijke elektronische communicatiegegevens die cruciaal zouden zijn voor het onderzoek, niet langer zouden bewaard worden".

Zoals artikel 36 is gesteld, strekt het ertoe aan de voorliggende wet terugwerkende kracht te verlenen tot de dag waarop de vernietiging van de wet van 29 mei 2016 zelf uitwerking heeft gehad, dat wil zeggen tot de dag van de inwerkingtreding van die wet.

2.2. Het voorliggende voorontwerp strekt immers tot invoering van een gearticuleerd systeem voor de bewaring van en de toegang tot persoonsgegevens op het gebied van de elektronische communicatie.

Le cœur du mécanisme en projet réside dans les articles 126 à 127/4 que l'avant-projet entend insérer dans la loi du 13 juin 2005.

La méconnaissance de ces nouvelles dispositions sera sanctionnée pénalement en vertu des modifications que l'article 15 de l'avant-projet entend apporter à l'article 145, § 1er, de la même loi.

Cet article 15 entend par ailleurs ajouter un paragraphe 3*ter* au même article 145, rédigé comme suit:

"Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement:

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données conservées par l'opérateur pour les autorités;

2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1°, les détient, les révèle à une autre personne, les divulgue ou en fait un usage quelconque".

Par conséquent, l'effet rétroactif conféré à l'avant-projet par son article 36 méconnait le principe de la non-rétroactivité des lois pénales consacré par l'article 7 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et par l'article 15 du Pacte international relatif aux droits civils et politiques.

2.3. Par ailleurs, il convient de rappeler que, dans son arrêt n° 57/2021, la Cour constitutionnelle a refusé de faire application de la possibilité offerte par l'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 'sur la Cour constitutionnelle', de maintenir les effets des dispositions annulées de la loi du 29 mai 2016. Ce faisant, elle a mis en œuvre ce que la Cour de justice avait elle-même jugé dans son arrêt *La Quadrature du Net*, à savoir qu'il serait porté

"atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire"[47].

L'annulation prononcée a donc elle-même "pris effet" *ex tunc,* au jour de l'entrée en vigueur de la loi du 29 mai 2016.

La rétroactivité conférée au dispositif à l'examen aboutira à conférer *ex post* un fondement légal à une série d'ingérences dans le droit au respect de la vie privée qui s'en trouvent aujourd'hui dépourvues, par l'effet de l'arrêt d'annulation

De kern van de ontworpen regeling ligt in de artikelen 126 tot 127/4 die bij het voorontwerp worden ingevoegd in de wet van 13 juni 2005.

De schending van die nieuwe bepalingen zal strafrechtelijk worden bestraft krachtens de wijzigingen die bij artikel 15 van het voorontwerp worden aangebracht in artikel 145, § 1, van dezelfde wet.

Dat artikel 15 strekt er tevens toe aan hetzelfde artikel 145 een paragraaf 3*ter* toe te voegen die luidt als volgt:

"Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de door de operator voor de autoriteiten bewaarde gegevens op enige manier overneemt, bij zich houdt of er enig gebruik van maakt.

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt."

De terugwerkende kracht die aan het voorontwerp bij artikel 36 ervan wordt verleend, schendt bijgevolg het beginsel dat strafwetten niet terugwerken, welk beginsel is vastgelegd in artikel 7 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en in artikel 15 van het Internationaal verdrag inzake burgerrechten en politieke rechten.

2.3. Voorts dient eraan te worden herinnerd dat het Grondwettelijk Hof in zijn arrest nr. 57/2021 de bij artikel 8, derde lid, van de bijzondere wet op het Grondwettelijk Hof van 6 januari 1989 geboden mogelijkheid heeft geweigerd om de gevolgen van de vernietigde bepalingen van de wet van 29 mei 2016 te handhaven. Daarmee heeft het Hof uitvoering gegeven aan hetgeen het Hof van Justitie zelf in zijn arrest *La Quadrature du Net* had geoordeeld, namelijk dat:

"aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn."[47]

De uitgesproken nietigverklaring heeft dus zelf *ex tunc* "uitwerking gehad" op de dag waarop de wet van 29 mei 2016 in werking is getreden.

De terugwerkende kracht die aan het voorliggende dispositief wordt verleend, zal ertoe leiden dat *ex post* rechtsgrond wordt verleend aan een reeks inmengingen in het recht op eerbiediging van het privéleven waarvoor thans geen

[47] Point 217.

[47] Punt 217.

n° 57/2021, non asso de la Cour constitutionnelle, non assorti de limite dans le temps, compte tenu de l'arrêt *La Quadrature du Net* de la Cour de Justice. En tant qu'elle a pour effet de valider pour le passé des ingérences, dans les droits fondamentaux des personnes – dont les données ont été conservées – qui doivent être considérées comme contraires au droit de l'Union, pareille rétroactivité n'est pas admissible au regard du droit de l'Union[48].

3. Il résulte des considérations qui précèdent que l'article 36 doit être omis.

Le greffier, *Le président,*

Anne-Catherine VAN GEERSDAELE Martine BAGUET

rechtsgrond voorhanden is als gevolg van het vernietigingsarrest nr. 57 2021 van het Grondwettelijk Hof dat, gelet op het arrest *La Quadrature du Net* van het Hof van Justitie, geen beperking in de tijd bevat. In zoverre ze tot gevolg heeft dat de inmengingen in de grondrechten van personen – van wie de gegevens zijn bewaard, voor het verleden worden gevalideerd – welke inmengingen geacht moeten worden strijdig te zijn met het Unierecht, is een dergelijke terugwerkende kracht niet aanvaardbaar in het licht van het Unierecht[48].

3. Uit de voorgaande overwegingen volgt dat artikel 36 moet worden weggelaten.

De griffier, *De voorzitter,*

Anne-Catherine VAN GEERSDAELE Martine BAGUET

[48] Il convient de rappeler, pour le surplus, que la Cour constitutionnelle dans son arrêt n° 57/2021 du 22 avril 2021, a expressément envisagé que les preuves qui auraient été recueillies en application des dispositions annulées de la loi du 29 mai 2016 puissent être déclarées admissibles au cas par cas:

"B.24.3. Il appartient au juge pénal compétent de statuer, le cas échéant, sur l'admissibilité des preuves qui ont été recueillies lors de la mise en œuvre des dispositions annulées, conformément à l'article 32 du titre préliminaire du Code de procédure pénale et à la lumière des précisions apportées par la Cour de justice dans l'arrêt du 6 octobre 2020 précité"

[48] Voor het overige dient eraan te worden herinnerd dat het Grondwettelijk Hof in zijn arrest nr. 57/2021 van 22 april 2021 uitdrukkelijk heeft bepaald dat de bewijzen die zouden zijn verzameld met toepassing van de vernietigde bepalingen van de wet van 29 mei 2016, per geval toelaatbaar kunnen worden verklaard:
"B.24.3 Het staat aan de bevoegde strafrechter, in voorkomend geval, uitspraak te doen over de toelaatbaarheid van de bewijzen die werden verzameld bij de tenuitvoerlegging van de vernietigde bepalingen, overeenkomstig artikel 32 van de voorafgaande titel van het Wetboek van stafvordering en in het licht van de door het Hof van Justitie in het voormelde arrest van 6 oktober 2020 aangebrachte preciseringen."

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

Sur la proposition du ministre de la Justice,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le ministre de la Justice est chargé de présenter en Notre nom à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2

Modifications à la loi du 13 juin 2005 relative aux communications électroniques

Art. 2

Dans l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, modifié en dernier lieu par la loi du 17 février 2022 modifiant diverses dispositions en matière de communications électroniques en vue d'introduire des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G modifiant diverses dispositions en matière de communications électroniques en vue d'introduire des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G, les modifications suivantes sont apportées:

1° les 5/5° et 5/6° sont insérés, rédigés comme suit:

"5/5°: "une fraude": un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

Op de voordracht van de minister van Justitie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Justitie is ermee belast in Onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen, waarvan de tekst hierna volgt:

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2

Wijzigingen aan de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 2

In artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van de wet van 17 februari 2022 tot wijziging van diverse bepalingen inzake elektronische communicatie met het oog op de invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-dienstentot wijziging van diverse bepalingen inzake elektronische communicatie met het oog op de invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten, worden de volgende wijzigingen aangebracht:

1° de bepalingen onder 5/5° en 5/6° worden ingevoegd, luidende:

"5/5°: "fraude": een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten

de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques;";

"5/6°: "utilisation malveillante du réseau ou du service": utilisation du réseau ou service de communication électronique afin d'importuner son correspondant ou de provoquer des dommages;";

2° au lieu du 74°, annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un 74° rédigé comme suit:

"74° "Appels infructueux": toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau;";

3° l'article est complété par les 91°, 92° et 93°, rédigés comme suit:

"91° "données de communications électroniques": le contenu de communications électroniques et les métadonnées de communications électroniques;";

"92° "contenu de communications électroniques": le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son;";

"93° "métadonnées de communications électroniques": les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.".

Art. 3

L'article 107/5, inséré par la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, est remplacé par ce qui suit:

"Art. 107/5. § 1er. Afin de favoriser la sécurité numérique, l'utilisation de la cryptographie est libre dans les limites prévues aux §§ 2 à 4.

nadele van de operator of eindgebruiker, via het gebruik van een elektronische-communicatiedienst;";

"5/6°: "kwaadwillig gebruik van het netwerk of van de dienst": gebruik van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen;";

2° in plaats van de bepaling onder 74°, vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een bepaling onder 74° ingevoegd, luidende:

"74° "Oproeppoging zonder resultaat": iedere communicatie waarbij een oproep wel werd doorgezonden, maar onbeantwoord is gebleven of door de netwerkbeheerder is beantwoord;";

3° het artikel wordt aangevuld met de bepalingen onder 91°, 92° en 93°, luidende:

"91° "elektronische-communicatiegegevens": de inhoud en de metagegevens van elektronische communicatie;";

"92° "inhoud van elektronische communicatie": de inhoud die wordt uitgewisseld door middel van elektronische-communicatiediensten, met name tekst, spraak, video, beelden en geluid;";

"93° "elektronische-communicatiemetagegevens": de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie; met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie.".

Art. 3

Artikel 107/5, ingevoegd bij de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, wordt vervangen als volgt:

"Art. 107/5. § 1. Ter bevordering van de digitale veiligheid is het gebruik van versleuteling vrij binnen de in de paragrafen 2 tot en met 4 gestelde grenzen.

§ 2. Le recours à la cryptographie ne peut pas empêcher les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant.

§ 3. Le recours à la cryptographie, utilisé par un opérateur, visant à garantir la sécurité des communications, ne peut pas empêcher l'exécution d'une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et localiser des communications non accessibles au public.

§ 4. L'utilisation de la cryptographie par un opérateur étranger, dont l'utilisateur final ou l'abonné est situé sur le territoire belge, ne peut pas empêcher l'exécution d'une demande d'une autorité compétente telle que visée aux paragraphes 2 à 3.

Toute clause contractuelle prise par les opérateurs faisant obstacle à l'exécution de cet alinéa est interdite et nulle de plein droit.".

Art. 4

Il est inséré un article 121/8, rédigé comme suit:

"§ 1er. Sans prendre connaissance du contenu des communications, les opérateurs prennent les mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés.

Le Roi peut préciser les mesures à prendre par les opérateurs en vertu de l'alinéa 1er.

L'Institut a le pouvoir de donner des instructions contraignantes, y compris des instructions concernant les dates limites de mise en œuvre, en vue de l'application du présent paragraphe.

§ 2. Lorsque cela se justifie au regard de la gravité des circonstances, qui doivent être examinées au cas par cas, les mesures appropriées visées au paragraphe 1er, alinéa 1er, peuvent comprendre notamment:

— des mesures au niveau du réseau, tels que le blocage des numéros, de services, des URLs, de noms de domaine, d'adresses IP ou de tout autre élément d'identification de la communication électronique;

§ 2. Het gebruik van versleuteling mag noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of het verstrekken van de identificatiegegevens van de oproeper, niet verhinderen.

§ 3. Het gebruik van versleuteling door een operator, met als doel de veiligheid van de communicatie te waarborgen, mag geen beletsel vormen voor de uitvoering van een gericht verzoek van een bevoegde autoriteit, onder de bij wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie.

§ 4. Het gebruik van versleuteling door een buitenlandse operator, wiens eindgebruiker of abonnee zich op het Belgisch grondgebied bevindt, mag de uitvoering van een verzoek van een bevoegde overheid, zoals bedoeld in de paragrafen 2 tot 3, niet verhinderen.

Elk contractueel beding dat door de operatoren wordt opgesteld en de uitvoering van dit lid belemmert, is verboden en van rechtswege nietig.".

Art. 4

Er wordt een artikel 121/8 ingevoegd, luidende:

"§ 1. Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden.

De Koning kan de door de operatoren krachtens het eerste lid te treffen maatregelen preciseren.

Het Instituut is bevoegd om bindende instructies te geven, met inbegrip van instructies betreffende de uitvoeringstermijnen, met het oog op de toepassing van deze paragraaf.

§ 2. Wanneer dat gerechtvaardigd is ten aanzien van de ernst van de omstandigheden, die per geval onderzocht moeten worden, kunnen de in paragraaf 1, eerste lid, bedoelde passende maatregelen met name het volgende omvatten:

— maatregelen op netwerkniveau, zoals de blokkering van nummers, diensten, URL's, domeinnamen, IP-adressen of elk ander element ter identificatie van de elektronische communicatie;

— des mesures au niveau de l'utilisateur final, telles que la désactivation complète ou partielle de certains services ou équipements.".

Art. 5

Dans l'article 122 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, les modifications suivantes sont apportées:

1° Dans le paragraphe 1er:

L'alinéa 2 est abrogé;

2° Dans le paragraphe 2:

— l'alinéa 1er est remplacé par ce qui suit:

"§ 2. Par dérogation au paragraphe 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs peuvent conserver et traiter les données de trafic nécessaires à cette fin."

— dans l'alinéa 2, les mots "de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" sont remplacés par les mots "du RGPD et de la loi du 30 juillet 2018";

— dans l'alinéa 3, le mot "énumérées" est remplacé par le mot "visées";

3° Dans le paragraphe 3:

— dans l'alinéa 1er, 2°, les mots "la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées" sont remplacés par les mots "le consentement au sens de l'article 4 du RGPD";

— dans l'alinéa 1er, 3°, les mots "la possibilité de retirer le consentement donné de manière simple" sont remplacés par les mots "la possibilité de retirer le consentement donné facilement et à tout moment";

— dans l'alinéa 2, les mots "de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" sont remplacés par les mots "du RGPD et de la loi du 30 juillet 2018";

— maatregelen op het niveau van de eindgebruiker, zoals de volledige of gedeeltelijke deactivering van bepaalde diensten of apparatuur.".

Art. 5

In artikel 122 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, worden de volgende wijzigingen aangebracht:

1° In paragraaf 1:

Wordt het tweede lid opgeheven;

2° In paragraaf 2:

— wordt het eerste lid vervangen als volgt:

"§ 2. In afwijking van paragraaf 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken."

— worden in het tweede lid de woorden "van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "van de AVG en van de wet van 30 juli 2018";

— wordt in het derde lid het woord "opgesomd" vervangen door het woord "bedoeld";

3° In paragraaf 3:

— worden in het eerste lid, 2°, de woorden "de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat verkeersgegevens die op hem betrekking hebben worden verwerkt" vervangen door de woorden "de toestemming in de zin van artikel 4 van de AVG";

— worden in het eerste lid, 3° de woorden "op eenvoudige wijze" vervangen door de woorden "makkelijk en te allen tijde";

— worden in het tweede lid de woorden "van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "van de AVG en van de wet van 30 juli 2018";

4° Le paragraphe 4 est remplacé comme suit:

“Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l’article 121/8, § 1er, de permettre d’établir la fraude ou l’utilisation malveillante du réseau ou du service ou d’identifier son auteur et son origine, l’opérateur:

1° conserve les données reprises dans le “Call detail record” (CDR) ou dans un registre fonctionnellement équivalent, ainsi que les données de localisation de l’auteur de la fraude présumée ou de l’utilisation malveillante présumée du réseau lorsqu’elles sont disponibles, 4 mois à partir de la date de la communication;

2° conserve pendant 12 mois à partir de la date de la communication les données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles;

3° conserve les données visées au 1° et qui sont relatives à une fraude spécifique identifiée ou une utilisation malveillante du réseau spécifique identifiée le temps nécessaire à son analyse et à sa résolution, le cas échéant au-delà du délai de 4 mois visé au 1°;

4° conserve les données de trafic visées au 2° et relatives à une utilisation malveillante spécifique du réseau, le temps nécessaire au traitement de cette dernière, le cas échéant au-delà du délai de 12 mois visé au 2°;

5° traite les données de trafic nécessaires à ces fins, en ce compris, lorsque c’est nécessaire, les données visées au paragraphe 2.

Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l’article 121/8, § 1er, de permettre d’établir la fraude ou l’utilisation malveillante du réseau ou du service, d’identifier son auteur et son origine, l’opérateur peut conserver et traiter d’autres données que celles visées à l’alinéa 1er considérées nécessaires à ces fins.

Le Roi peut préciser et étendre, par arrêté délibéré en Conseil des ministres et après avis de l’Institut et de l’Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire pour la poursuite des finalités prévues au présent paragraphe.

4° Paragraaf 4 wordt vervangen als volgt:

“In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, dient de operator:

1° de gegevens opgenomen in de “Call detail record” (CDR) of in een functioneel gelijkwaardig register te bewaren, alsook de locatiegegevens van de dader van de vermeende fraude of het vermeende kwaadwillige gebruik van het netwerk wanneer deze beschikbaar zijn, gedurende 4 maanden vanaf de datum van de communicatie;

2° gedurende 12 maanden vanaf de datum van de communicatie de verkeersgegevens betreffende de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten te bewaren;

3° de in 1° bedoelde gegevens die betrekking hebben op een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk te bewaren gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van 4 maanden zoals bedoeld in 1°;

4° de verkeersgegevens bedoeld in 2° en met betrekking tot een specifiek kwaadwillig gebruik van het netwerk te bewaren gedurende de periode die nodig is voor de verwerking ervan, in voorkomend geval langer dan de termijn van 12 maanden zoals bedoeld in 2°;

5° de noodzakelijke verkeersgegevens daartoe te verwerken, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.

In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en verwerken, die voor deze doeleinden nodig worden geacht.

De Koning kan, bij besluit vastgesteld na overleg in de “raad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de doeleinden waarin deze paragraaf voorziet, preciseren en uitbreiden.

En cas de fraude présumée ou d'utilisation malveillante présumée, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec la fraude présumée ou l'utilisation malveillante présumée.";

5° Un paragraphe 4/1 est inséré, rédigé comme suit:

"§ 4/1. Par dérogation au paragraphe 1er, les opérateurs peuvent conserver et traiter les données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

Ils peuvent les conserver pour une durée de douze mois à partir de la date de la communication.

Ils peuvent conserver les données visées à l'alinéa 1er relatives à une atteinte spécifique à la sécurité du réseau pendant la durée nécessaire pour la traiter, le cas échéant au-delà du délai de 12 mois visé à l'alinéa 2.

En cas d'atteinte à la sécurité de leurs réseaux et services de communications électroniques, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec l'atteinte à la sécurité de leurs réseaux et services de communications électroniques.";

6° Un paragraphe 4/2 est inséré, rédigé comme suit:

"§ 4/2. Par dérogation au paragraphe 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation imposée par une norme législative formelle, pour la durée requise à cette fin.";

7° Le paragraphe 5 est remplacé comme suit:

"§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination.";

In geval van vermeende fraude of van vermeend kwaadwillig gebruik, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermeende fraude of het vermeende kwaadwillig gebruik doorsturen.";

5° Een paragraaf 4/1 wordt ingevoerd, luidend:

"§ 4/1. In afwijking van paragraaf 1 mogen de operatoren die verkeersgegevens bewaren en verwerken die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

Zij mogen deze bewaren voor een duur van twaalf maanden vanaf de datum van de communicatie.

Ze mogen de in het eerste lid bedoelde gegevens met betrekking tot een specifieke schending van de veiligheid van het netwerk bewaren gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van 12 maanden zoals bedoeld in het tweede lid.

In geval van schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten doorsturen.";

6° Een paragraaf 4/2 wordt ingevoerd, luidende:

"§ 4/2. In afwijking van paragraaf 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm, voor de daartoe benodigde duur.";

7° Paragraaf 5 wordt vervangen als volgt:

"§ 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten die gebruik maken van verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel.";

8° Dans le paragraphe 6, les mots “L’Institut” sont remplacé par les mots “L’Institut, le Service de médiation pour les télécommunications,”.

Art. 6

À l’article 123 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, les modifications suivantes sont apportées:

1° Le paragraphe 1er est remplacé par ce qui suit:

“§ 1er. Sans préjudice de l’application du RGPD et de la loi du 30 juillet 2018, les opérateurs de réseaux mobiles ne peuvent conserver et traiter de données de localisation autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final que dans les cas suivants:

1° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées maximum 12 mois à partir de la date de la communication, sauf en cas d’atteinte spécifique à la sécurité du réseau nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

2° lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l’utilisation malveillante du réseau, les données étant conservées maximum 4 mois à partir de la date de la communication, sauf en cas de fraude ou d’utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

3° lorsque les données ont été rendues anonymes;

4° lorsque le traitement s’inscrit dans le cadre de la fourniture d’un service qui fait usage de données de trafic ou de localisation;

5° lorsque le traitement est nécessaire pour répondre à une obligation imposée par une norme législative formelle.”;

2° Dans le paragraphe 2:

dans le 2°, les mots “la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l’intéressé ou son représentant légal accepte que des données de localisation se rapportant à lui soient traitées”

8° In paragraaf 6 worden de woorden “het Instituut” vervangen door de woorden “het Instituut, de Ombudsdienst voor telecommunicatie,”.

Art. 6

In artikel 123 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, worden de volgende wijzigingen aangebracht:

1° De eerste paragraaf wordt vervangen als volgt:

“§ 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen:

1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard gedurende maximaal 12 maanden vanaf de datum van de communicatie, tenzij in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, waarbij de gegevens worden bewaard gedurende maximaal 4 maanden vanaf de datum van de communicatie, tenzij in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

3° wanneer de gegevens anoniem gemaakt zijn;

4° wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens;

5° wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm.”;

2° In paragraaf 2:

worden in de bepaling onder 2°, de woorden “de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat locatiegegevens die op hem betrekking

sont remplacés par les mots “le consentement au sens de l’article 4 du RGPD”;

3° Le paragraphe 4, alinéa 1er, est remplacé par ce qui suit:

“§ 4. Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l’autorité de l’opérateur ou du tiers qui fournit le service qui fait usage de données de trafic ou de localisation, ou par la Cellule de coordination de l’opérateur visée à l’article 127/3.”.

Art. 7

L’article 125, § 2, de la même loi est abrogé.

Art. 8

L’article 126 de la même loi est remplacé par ce qui suit:

“Art. 126. § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, conservent les données énumérées par le Roi, l’arrêté étant pris après avis de l’Autorité de protection des données et de l’Institut.

Cet arrêté ne peut comprendre que des données de souscription de l’abonné au service ainsi que des données qui sont nécessaires pour identifier l’utilisateur final, l’équipement terminal ou le service de communications électroniques employé. Il ne porte pas sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l’adresse IP du destinataire de la communication ou sur la localisation de l’équipement terminal.

Par données de souscription, on entend les produits auxquels l’abonné a souscrit, le début et la fin du service ainsi que les identifiants et différents numéros qui lui sont attribués lors de la souscription au service.

Les opérateurs ne conservent les données visées à l’alinéa 1er que pour autant qu’ils les traitent ou les génèrent dans le cadre de la fourniture des réseaux ou services de communications électroniques concernés.

hebben worden verwerkt” vervangen door de woorden “de toestemming in de zin van artikel 4 van de AVG”;

3° Paragraaf 4, eerste lid, wordt vervangen als volgt:

“§ 4. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst die gebruik maakt van verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator waarvan sprake in artikel 127/3.”.

Art. 7

Artikel 125, § 2, van dezelfde wet wordt opgeheven.

Art. 8

Artikel 126 van dezelfde wet wordt vervangen als volgt:

“Art. 126. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten bieden, alsook de operatoren die de elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de door de Koning opgesomde gegevens, waarbij het besluit wordt genomen na advies van de Gegevensbeschermingsautoriteit en van het Instituut.

Dat besluit mag niets anders bevatten dan de abonnementsgegevens van de abonnee inzake de dienst alsook de gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren. Het besluit heeft geen betrekking op de inhoud van elektronische-communicatie, noch op de metagegevens van de elektronische communicatie die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur.

Onder abonnementsgegevens wordt verstaan de producten waarop de abonnee heeft ingetekend, het begin en het einde van de dienst alsook de identificatiecodes en verschillende nummers die eraan zijn toegewezen bij de intekening op de dienst.

De operatoren bewaren de in het eerste lid bedoelde gegevens maar voor zover ze deze in het kader van de verstrekking van de elektronische-communicatienetwerken of -diensten in kwestie verwerken of ze genereren.

§ 2. Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Par dérogation à l'alinéa 1er, les opérateurs conservent les adresses IP à la source de la connexion, autres que celle qui a été utilisée pour souscrire au service, ainsi que les autres données techniques d'identification des utilisateurs finaux, des équipements terminaux ou du service de communications électroniques utilisé, dont la liste est fixée par le Roi, jusqu'à douze mois après la fin de la session.

§ 3. Le Roi fixe, après avis de l'Autorité de protection des données et de l'Institut, les exigences auxquelles les données visées au paragraphe 1er, alinéa 1er, doivent répondre.".

Art. 9

Dans la même loi, un article 126/1 est inséré, rédigé comme suit:

"Art. 126/1. § 1er. Sans préjudice du RGDP et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées au paragraphe 2, pour les zones géographiques visées au paragraphe 3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans le présent article.

Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communication électroniques concernés.

Ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.

§ 2. Les données visées au paragraphe 1er sont les données fixées par le Roi, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, et qui ressortent de la catégorie suivante:

§ 2. De operatoren bewaren de in paragraaf 1, eerste lid, beoogde gegevens vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is.

In afwijking van het eerste lid bewaren de operatoren de andere IP-adressen aan de bron van de verbinding dan diegene die is gebruikt om in te tekenen op de dienst, alsook de overige technische identificatiegegevens van de eindgebruikers, van de eindtoestellen of van de gebruikte elektronische-communicatiedienst, waarvan de lijst wordt vastgesteld door de Koning, tot twaalf maanden na het einde van de sessie.

§ 3. De Koning bepaalt, na advies van de Gegevensbeschermingsautoriteit en van het Instituut, de vereisten waaraan de in paragraaf 1, eerste lid, bedoelde gegevens moeten beantwoorden.".

Art. 9

In dezelfde wet, wordt een artikel 126/1 ingevoegd, luidende:

"Art. 126/1. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische communicatienetwerken aanbieden, de in paragraaf 2 bedoelde gegevens voor de geografische zones bedoeld in paragraaf 3, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in huidig artikel.

Elke operator bewaart de gegevens die door hem gegenereerd of verwerkt zijn in het kader van de verstrekking van de betrokken elektronische communicatiediensten en -netwerken.

Deze gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

§ 2. De gegevens bedoeld in paragraaf 1 zijn de gegevens bepaald door de Koning, bij een in Ministerraad overlegd besluit, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en van de minister, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, en die behoren tot de volgende categorie:

Les métadonnées de communications électroniques, en ce compris l'origine et la destination de la communication, la localisation de l'équipement terminal lors de la communication et les métadonnées des appels infructueux, pour autant que ces dernières données soient, dans le cadre de la fourniture des services de communications électroniques concernés:

i° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs; ou

ii° en ce qui concerne les données de l'internet, journalisées par ces opérateurs.

Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les exigences auxquelles ces données doivent répondre.

§ 3. Les zones géographiques dans lesquelles sont conservées les données visées au paragraphe 2 sont les suivantes:

1° la zone géographique composée des:

— arrondissements judiciaires dans lesquels au moins 3 infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées durant l'année sur une moyenne des trois années calendriers qui précèdent celle en cours;

— zones de police, dans lesquelles, au moins 3 infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précèdent celle en cours, moins de 3 infractions visées à l'article 90*ter* §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années qui précèdent celle en cours ont été constatées.

Dans l'hypothèse visée au 1er tiret, le délai de conservation des données visées au paragraphe 2 est de:

a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois dernières années calendriers qui précèdent celle en cours;

De metagegevens van elektronische communicatie, met inbegrip van de herkomst en de bestemming van de communicatie, de plaats van de eindapparatuur tijdens de communicatie, en de metagegevens van oproeppogingen zonder resultaat, voor zover die laatste gegevens in het kader van de aanbieding van de bedoelde elektronische-communicatiediensten:

i° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren; of

ii° wat de internetgegevens betreft, door deze operatoren worden gelogd.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten bepalen waaraan deze gegevens moeten beantwoorden.

§ 3. De geografische zones waarbinnen de gegevens bedoeld in paragraaf 2 bewaard worden, zijn de volgende:

1° de geografische zones bestaande uit:

— de gerechtelijke arrondissementen waar minstens 3 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4 van het Wetboek van Strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;

— de politiezones waar minstens 3 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan 3 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de 3 voorbije kalenderjaren.

In het geval bedoeld in het eerste streepje bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2:

a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90*ter*, §§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) 12 mois, s'il y a 7 ou plus de 7 d'infractions visées à l'article 90*ter* §§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Dans l'hypothèse visée au deuxième tiret, le délai de conservation des données visées au paragraphe 2 est de:

a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90*ter* §§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois dernières années calendriers qui précèdent celle en cours;

b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90*ter* §§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) 12 mois, s'il y a 7 ou plus de 7 infractions visées à l'article 90*ter*§§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non 5.

Les statistiques relatives au nombre d'infractions visées à l'article 90*ter* §§ 2 à 4 du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police.

Les périmètres des arrondissements judiciaires visés au 1° sont fixés par l'article 4 de l'annexe au Code judiciaire.

Les périmètres des zones de police visées au 1° sont celles fixés à l'annexe de l'arrêté royal 24 octobre 2001 portant la dénomination des zones de police.

La direction, visée à l'article 44/11 de la loi sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de

b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld zijn in de 3 voorbije kalenderjaren.

In het geval bedoeld in het tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2:

a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;

c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet 5 bereikt.

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1 000 inwoners vastgesteld in de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet op het politieambt.

De grenzen van de gerechtelijke arrondissementen bedoeld onder 1° zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De grenzen van de politiezones bedoeld onder 1° zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

De directie, zoals bedoeld in artikel 44/11 van de wet op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone

police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.

Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que leur durée de conservation.

Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation, ainsi que leur durée de conservation aux opérateurs.

2° Toutes les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.

Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin qu'il prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées au § 2 sur l'ensemble du territoire.

L'obligation de conservation visée à l'alinéa précédent est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa précédent, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les

naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

2° Alle geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2° van de wet van 10 juli 2006 betreffende de dreigingsanalyse, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de dreigingsanalyse, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze de nodige maatregelen kan nemen om de operatoren in te lichten en tot een bewaring van de gegevens bedoeld in § 2 over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het vorige lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het vorige lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst

opérateurs suppriment les données qui ont déjà été conservées à cette fin.

3° Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave, à savoir:

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2., 3°, 4° et 5° de la Code de la Navigation;

b) les gares au sens de l'article 2, 5° de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;

g) les armuriers et les stands de tir au sens de l'article 2, points 1 et 19 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

h) les établissements visés à l'article 3.1.a) de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

i) les établissements SEVESO visés dans l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

3° De gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2., 3°, 4° en 5° van het Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5° van de Wet van 27 april 2018 houdende de spoorwegpolitie;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad, alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenissen in de zin van artikel 2, 15°, van de Basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gesteld, bedoeld in artikel 606 van het Wetboek van Strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;

g) de wapenkamers en schietstanden zoals bedoeld in artikel 2, punten 1 en 19 van de Wet van 8 juni 2006 houdende de economische en individuele activiteiten met wapens;

h) de faciliteiten bedoeld in artikel 3.1.a) van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de SEVESO-inrichtingen zoals bedoeld in het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

k) le siège social de la S.A. Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de service essentiels désignés sur base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

m) le cas échéant sans préjudice du § 6 alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave fixées par arrêté royal.

4° Les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:

a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution et les cabinets ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenants;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren en de uitvoeringsbesluiten; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de nv Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en versleutelde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd § 6, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

4° De zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten en de ministeriële kabinetten;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:

i) les assemblées législatives au sens de l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) le palais royal;

iv) les domaines royaux;

v) les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du Titre III de la Constitution;

vi) les communes dans lesquelles se trouvent des domaines militaires;

vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'État;

e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:

i) les hôpitaux au sens de l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soin;

ii) la Banque nationale de Belgique;

g) le cas échéant, sans préjudice du § 6 alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.

5° Les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir:

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union Européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ii) de gemeentehuizen en de stadhuizen;

iii) het koninklijk paleis;

iv) de koninklijke domeinen;

v) de gebouwen toegewezen aan de instellingen bedoeld in Titel III, hoofdstukken 5 tot 7 van de Grondwet;

vi) de gemeenten waar zich militaire domeinen bevinden;

vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;

e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:

i) de ziekenhuizen zoals bedoeld in artikel 2 van de Gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;

g) in voorkomend geval, en onverminderd § 6, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.

5° De zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:

a) de ambassades en diplomatieke vertegenwoordigingen;

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuren bestemd voor de NAVO;

d) les institutions de l'Espace économique européen;

e) les institutions des Nations Unies;

f) le cas échéant, sans préjudice du § 6 alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.

Pour chaque catégorie de zone visée à l'alinéa 1er, 3° à 5° inclus, le Roi détermine l'étendue du périmètre de la zone.

Chaque autorité compétente dans l'une des matières visées à l'alinéa 1er, points 3° à 5°, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.

Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée au paragraphe 1er dans cette zone.

À l'exception de la liste des lieux visés à l'alinéa 1er, point 4°, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences la liste actualisée des zones visées à l'alinéa 1er, 3° à 5° inclus, où une conservation de données est obligatoire.

L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées à l'alinéa 1er, 3° à 5° inclus, soient retirées de la liste.

Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa précédent, le ministre de la Défense, le ministre de la Justice, et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.

L'arrêté ministériel visé à l'alinéa précédent est publié par voie de mention au *Moniteur belge*.

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd § 6, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

Voor elke categorie van zone bedoeld in het eerste lid, 3° tot en met 5° bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in het eerste lid, punten 3° tot en met 5°, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld in paragraaf 1 in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in het eerste lid, punt 4°, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in het eerste lid, punten 3° tot en met 5°, waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

Het controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het gemotiveerde bevel geven dat bepaalde geografische zones bedoeld in het eerste lid, punten 3° tot en met 5°, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vorige lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het vorige lid wordt bekendgemaakt via vermelding in het *Belgisch Staatsblad*.

Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.

Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 4. Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone.

Lorsque, compte tenu de la technologie utilisée par l'opérateur, celui-ci n'est pas en mesure de localiser l'équipement terminal ayant participé à la communication, y compris l'appel infructueux, de façon plus précise que sa localisation sur le territoire national, l'opérateur conserve les données visées au paragraphe 2 pour la durée la plus courte fixée en exécution du présent article, à la condition qu'en exécution du présent article l'ensemble du territoire national soit soumis à une obligation de conservation. Lorsque cette condition n'est pas remplie, l'opérateur concerné par le présent alinéa ne conserve pas de données en exécution du présent article.

Lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur conserve les données de trafic pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone visée au paragraphe 3.

Les opérateurs conservent les données relatives à la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, énumérées dans l'arrêté royal visé au paragraphe 2, alinéa 2, lorsque cet équipement se trouve dans une zone visée au paragraphe 3.

Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée au paragraphe 3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent, si disponible à cet effet, la localisation satellitaire d'un équipement terminal.

Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données à une

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van huidig artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 4. De operatoren bewaren de verkeersgegevens voor iedere communicatie of alle oproepen zonder resultaat die vanuit of naar een geografisch gebied als bedoeld in paragraaf 3 worden gevoerd.

Indien de operator, als gevolg van de door hem gebruikte technologie, niet in staat is de eindapparatuur die betrokken is bij de communicatie, met inbegrip van de oproeppoging zonder resultaat, nauwkeuriger te lokaliseren dan de lokalisatie ervan op het nationale grondgebied, bewaart de operator de in paragraaf 2 bedoelde gegevens gedurende de kortste overeenkomstig huidig artikel bepaalde termijn, op voorwaarde dat overeenkomstig dit artikel het gehele nationale grondgebied gedekt is door een bewaarplicht. Indien niet aan deze voorwaarde is voldaan, bewaart de betrokken operator geen gegevens in uitvoering van huidig artikel.

Wanneer de eindgebruiker zich tijdens een elektronische communicatie verplaatst, bewaart de operator de verkeersgegevens voor zover de eindgebruiker zich op een bepaald moment van de communicatie bevindt in een gebied bedoeld in paragraaf 3.

De operatoren bewaren de gegevens met betrekking tot de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, die opgesomd zijn in het koninklijk besluit bedoeld in paragraaf 2, tweede lid, wanneer die apparatuur zich bevindt in een in paragraaf 3 bedoeld gebied.

Om te bepalen of eindapparatuur zich in een geografisch gebied als bedoeld in paragraaf 3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens die beschikbaar zijn. Zij maken hiervoor, indien beschikbaar, gebruik van de satellietlocatie van eindapparatuur.

Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot een

zone visée au paragraphe 3, il conserve les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.

Lorsqu'un point d'agrégation de l'opérateur, telle une antenne, couvre plusieurs zones géographiques visées au paragraphe 3 qui sont soumises à des durées de conservation différentes, l'opérateur conserve les données pour ce point d'agrégation pendant la durée de conservation la plus courte.

Lorsqu'en application du présent article, différentes durées de conservation sont applicables à des mêmes données, les opérateurs conservent les données pendant la durée la plus courte.

§ 5. Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, et après avis des autorités de protection des données compétentes et de l'Institut, les éléments suivants:

— les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées au paragraphe 3;

— la liste des différentes autorités compétentes dans les matières visées au paragraphe 3, alinéa 1er, points 2° à 5°;

— les modalités de communication des informations par les autorités compétentes vers le service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er;

— s'il y échet, les zones géographiques additionnelles visées au paragraphe 3, alinéa 1er, points 3°, m), 4°, g) et 5°, f).

L'arrêté royal visé à l'alinéa 1er, 4ème tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1er en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal.

§ 6. Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et de la Sécurité, et de l'Institut et des autorités de protection des données compétentes, un

in paragraaf 3 bedoelde zone, bewaart hij de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.

Wanneer een aggregatiepunt van de operator, zoals een antenne, verschillende in paragraaf 3 bedoelde geografische gebieden dekt die onderworpen zijn aan een verschillende bewaringstermijn, bewaart de operator de gegevens voor dat aggregatiepunt gedurende de kortste bewaringstermijn.

Wanneer op grond van dit artikel verschillende bewaringstermijnen van toepassing zijn op dezelfde gegevens, bewaren de operatoren de gegevens gedurende de kortste termijn.

§ 5. De Koning kan, bij een besluit vastgesteld na overleg in de ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister, na raadpleging van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende bepalen:

— de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones;

— de lijst van de verschillende autoriteiten die bevoegd zijn voor de in paragraaf 3, eerste lid, punten 2° tot en met 5° bedoelde aangelegenheden;

— de modaliteiten voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de modaliteiten voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen;

— in voorkomend geval, de bijkomende geografische zones bedoeld in paragraaf 3, eerste lid, punten 3°, m), 4°, g) en 5°,f).

Elke drie jaar dient het koninklijk besluit bedoeld in het eerste lid, vierde streepje te worden hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 voor wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.

§ 6. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité Inlichtingen en Veiligheid, en van het Instituut en de autoriteiten bevoegd voor de bescherming

rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 5, afin de vérifier si des dispositions doivent être adaptées.

Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 5 répondent toujours aux critères visés au paragraphe 3, alinéa 1er, points 3° à 5° et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.

Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.

Le rapport d'évaluation comprend également le pourcentage du territoire national auquel s'applique l'obligation de conservation des données en vertu du présent article.

Ce rapport est envoyé à l'Organe de contrôle de l'information policière et au Comité permanent R.".

van de gegevens , jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 5 bedoelde koninklijk besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 5 bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in paragraaf 3, eerste lid, punten 3° tot 5° en of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit.

Het evaluatieverslag bevat ook het percentage van het nationale grondgebied waarvoor de verplichting tot gegevensbewaring op basis van huidig artikel van toepassing is.

Dit evaluatierapport wordt gestuurd naar het controleorgaan op de politionele informatie en naar het Vast Comité I.".

Art. 10

Dans le paragraphe 2 de l'article 127 de la même loi, les mots "à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements" sont remplacés par les mots "à l'exception de systèmes d'encryptage, qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements, qui font l'objet de règles particulières prévues à l'article 107/5".

Art. 10

In paragraaf 2 van artikel 127 van dezelfde wet worden de woorden "met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen" vervangen door de woorden "met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen, welke onder specifieke regels vallen die vastgesteld worden in artikel 107/5".

Art. 11

Dans la même loi, un article 127/1 est inséré, rédigé comme suit:

"Art 127/1. § 1er. Pour l'application du présent article, la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux:

Art. 11

In dezelfde wet, wordt een artikel 127/1 ingevoegd, luidende:

"Art. 127/1. § 1. Voor de toepassing van dit artikel omvat zware criminaliteit met name de feiten waarvoor er ernstige aanwijzingen bestaan:

1° qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88*bis*, alinéa 1er, du Code d'instruction criminelle;

2° qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 au sens de l'article XV.70 du Code de droit économique;

3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) ou aux dispositions prises sur la base ou en exécution de ces articles.

§ 2. Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle:

1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique;

3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques;

4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information;

5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques;

6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave;

7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

1° dat ze de minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88*bis*, eerste lid, van het Wetboek van Strafvordering tot gevolg kunnen hebben;

2° dat ze kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht;

3° dat ze een inbreuk zouden kunnen vormen op de artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening betreffende machtsmisbruik) of op de bepalingen die worden genomen op basis of ter uitvoering van deze artikelen.

§ 2. Enkel de volgende autoriteiten mogen van een operator gegevens krijgen die worden bewaard krachtens de artikelen 122 en 123, voor de doeleinden hieronder voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm:

1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;

2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;

3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;

5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;

6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;

7° de administratieve autoriteiten belast met het behoud van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid;

8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave;

9° l'Institut dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle;

10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques.

§ 3. Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.

Seules les autorités visées au paragraphe 2, peuvent obtenir d'un opérateur des données conservées en vertu des articles 126 et 127 pour les finalités prévues dans ce même paragraphe, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

Par dérogation à l'alinéa 2, les autorités visées au paragraphe 2, 10°, ne peuvent pas obtenir d'un opérateur des adresses IP attribuées à la source de la connexion.

Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.

§ 4. Les données conservées en vertu de l'article 126/1 le sont pour les autorités et finalités visées au paragraphe 2, 1°, 2°, 3° et 6°.

Seules les autorités visées au paragraphe 2, 1°, 2°, 3°, 6° et 9° peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu de l'article 126/1, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

§ 5. La norme législative formelle de droit belge visée aux paragraphes 2 à 4 précise:

8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;

9° het Instituut in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;

10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

§ 3. De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.

Enkel de autoriteiten bedoeld in paragraaf 2, mogen van een operator gegevens ontvangen die worden bewaard krachtens de artikelen 126 en 127 voor de doeleinden waarin dezelfde paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.

In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen voor de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.

§ 4. De gegevens die worden bewaard krachtens artikel 126/1 worden bewaard voor de autoriteiten en doeleinden bedoeld in paragraaf 2, 1°, 2°, 3° en 6°.

Enkel de in paragraaf 2, 1°, 2°, 3°, 6° en 9°, bedoelde autoriteiten mogen van een operator voor de doeleinden beoogd in dezelfde paragraaf, de krachtens artikel 126/1 bewaarde gegevens krijgen, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

§ 5. De formele wettelijke norm van Belgisch recht bedoeld in de paragrafen 2 tot 4 preciseert:

— la ou les catégories d'entreprises auxquelles l'autorité peut demander des données;

— les catégories de données qui peuvent être demandées;

— les finalités poursuivies;

— les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.

Le ministre fait publier au *Moniteur belge* une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1 et 127.

À la demande du ministre ou de l'Institut, les autorités belges visées aux paragraphes 2 à 4 fournissent les informations nécessaires pour la rédaction de cette circulaire.

§ 6. Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1 ou 127 comprennent les mentions minimales suivantes:

1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service;

2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central;

3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité;

4° le délai de réponse souhaité.

§ 7. L'Institut transmet annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de données conservées en vertu des articles 122, 123, 126, 126/1 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment:

— de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen;

— de categorieën van gegevens die mogen gevraagd worden;

— de beoogde doeleinden;

— de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit.

De "laat in het *Belgisch Staatsblad* een omzendbrief publiceren die een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127.

Op het verzoek van de "of van het Instituut verstrekken de Belgische autoriteiten bedoeld in de paragrafen 2 tot 4 de informatie die nodig is om deze omzendbrief op te stellen.

§ 6. De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 of 127, omvatten de volgende minimale vermeldingen:

1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;

2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;

3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;

4° de gewenste antwoordtermijn.

§ 7. Het Instituut stuurt jaarlijks aan de "en de "van Justitie statistieken over de verstrekking aan de autoriteiten van gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127. Deze "s sturen die jaarlijks door naar de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name:

1° les cas dans lesquels des données conservées ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données conservées n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l'information confidentielle.

Les données qui concernent l'application de l'alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

L'Institut demande aux opérateurs et au service désigné par le Roi les informations qui lui permettent de remplir l'obligation visée à l'alinéa 1er.".

Art. 12

Dans la même loi, un article 127/2 est inséré, rédigé comme suit:

"§ 1er. Les opérateurs veillent à garantir la qualité des métadonnées de communications électroniques conservées et, pour ce qui concerne les données conservées pour les autorités, à ce qu'elles soient de la même qualité que les données traitées dans le cadre de la fourniture du réseau ou du service de communications électroniques.

Les opérateurs mettent tout en œuvre pour établir les liens techniques entre les données conservées pour les autorités qui sont nécessaires pour répondre à leurs demandes.

§ 2. Pour ce qui concerne les données d'identification de l'abonné et les métadonnées de communications électroniques, conservées pour les autorités, les opérateurs:

1° garantissent que les données conservées sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ou traitées par le service;

2° mettent en œuvre des mesures de protection technologique qui rendent les données conservées,

1° de gevallen waarin bewaarde gegevens zijn verstrekt aan de bevoegde autoriteiten overeenkomstig de toepasselijke wettelijke bepalingen;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken om bewaarde gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens noch vertrouwelijke informatie omvatten.

De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens bijgevoegd bij het verslag dat de "van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering moet uitbrengen aan het Parlement.

Het Instituut vraagt aan de operatoren en aan de door de Koning aangewezen dienst de informatie aan de hand waarvan het de in het eerste lid bedoelde verplichting kan vervullen.".

Art. 12

In dezelfde wet, wordt een artikel 127/2 ingevoegd, luidende:

"§ 1. De operatoren garanderen de kwaliteit van de bewaarde metagegevens van elektronische communicatie en, in het geval van de gegevens bewaard voor de autoriteiten, zorgen ze ervoor dat ze dezelfde kwaliteit hebben als de gegevens die worden verwerkt in het kader van de verstrekking van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst.

De operatoren stellen alles in het werk om de technische verbanden te leggen tussen de gegevens bewaard voor de autoriteiten die nodig zijn om op hun vragen te antwoorden.

§ 2. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie, bewaard voor de autoriteiten, dienen de operatoren:

1° te garanderen dat de bewaarde gegevens onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk of verwerkt door de dienst;

2° te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie,

dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

3° ne peuvent utiliser les données conservées pour d'autres finalités que la fourniture de ces données aux autorités, sauf lorsqu'ils obtiennent le consentement des abonnés concernés conformément à l'article 4 du RGDP et sans préjudice d'autres dispositions légales.

§ 3. Pour ce qui concerne les données d'identification de l'abonné et les métadonnées de communications électroniques, les opérateurs:

1° conservent les données sur le territoire de l'Union européenne et fournissent en Belgique les données demandées par une autorité belge;

2° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données ou rendent ces données anonymes;

3° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, conformément à l'article 105/1;

4° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 127/3, § 1er, de manière manuelle ou automatisée;

5° assurent une traçabilité de l'exploitation des données conservées.

§ 4. La traçabilité visée au paragraphe 3, alinéa 1er, 5°, s'effectue à l'aide d'un journal.

L'opérateur prend les mesures nécessaires pour que chaque consultation des données qu'il conserve pour les autorités génère de manière automatisée un enregistrement dans le journal des données suivantes: l'identité de la personne ayant consulté les données, le moment de la consultation et les données consultées.

Ce journal comprend également les informations et documents suivants, qui, le cas échéant, y sont introduits de manière manuelle:

onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

3° mogen de bewaarde gegevens niet gebruiken voor andere doeleinden dan de verstrekking van deze gegevens aan de autoriteiten, tenzij wanneer ze de toestemming krijgen van de betrokken abonnees, conform artikel 4 van de AVG en onverminderd andere wettelijke bepalingen.

§ 3. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie dienen de operatoren:

1° de gegevens op het grondgebied van de Europese Unie te bewaren en in België de door een Belgische autoriteit gevraagde gegevens te verstrekken;

2° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt van elke drager worden verwijderd of dat deze gegevens worden geanonimiseerd;

3° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij onbedoeld hetzij onrechtmatig, tegen een onbedoeld verlies of onbedoelde wijziging of tegen niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, conform artikel 105/1;

4° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 127/3, § 1, op manuele of op geautomatiseerde wijze;

5° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord.

§ 4. De in de paragraaf 3, eerste lid, 5°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek.

De operator neemt de nodige maatregelen opdat elke raadpleging van de gegevens die hij bewaart voor de autoriteiten, automatisch in het logboek een registratie van de volgende gegevens genereert: de identiteit van de persoon die de gegevens heeft geraadpleegd, het moment van de raadpleging en de geraadpleegde gegevens.

Dit logboek bevat eveneens de volgende informatie en documenten, die eventueel manueel daarin worden ingevoerd:

1° l'identité de l'autorité demanderesse, l'objet, la date et l'heure de la demande, une copie de la demande ou un lien vers cette dernière;

2° pour ce qui concerne la réponse de l'opérateur à la demande de l'autorité: l'identité de son destinataire, la date et l'heure de son envoi ainsi que le moyen de communication utilisé pour l'envoyer.

Le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte.

Les données de ce journal sont conservées pendant une période de dix ans. À l'échéance de la période de conservation, les données du journal sont détruites.

L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal. Toute modification des données reprises dans le journal est interdite. Toute consultation du journal est journalisée.

Le Roi peut préciser, après avis de l'Autorité de protection des données et de l'Institut, les exigences à respecter par les opérateurs concernant le journal.

Dans le cadre du contrôle de l'opérateur, l'Institut et l'Autorité de protection des données peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.

§ 5. Si l'Institut dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2, 3 ou 4, il peut l'obliger à se soumettre à un contrôle de sécurité effectué par un organisme qualifié indépendant, proposé par l'opérateur à l'Institut pour accord.

Cet organisme ne prend pas connaissance des demandes des autorités envers les opérateurs, en ce compris le journal visé au paragraphe 4.

Le rapport et les résultats de ce contrôle de sécurité sont communiqués à l'Institut. Le coût du contrôle est à la charge de l'opérateur.".

Art. 13

Dans la même loi, un article 127/3 est inséré, rédigé comme suit:

1° de identiteit van de vragende autoriteit, het voorwerp, de datum en het tijdstip van het verzoek, een kopie van het verzoek of een link naar dit laatste;

2° wat betreft het antwoord van de operator op het verzoek van de autoriteit: de identiteit van zijn geadresseerde, de datum en het tijdstip van de verzending ervan alsook het communicatiemiddel dat werd gebruikt voor de verzending.

Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan.

De gegevens van dit logboek worden bewaard gedurende een periode van tien jaar. Nadat deze bewaringstermijn is verstreken, worden de logboekgegevens vernietigd.

De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen. Elke wijziging van de in het logboek opgenomen gegevens is verboden. Elke raadpleging van het logboek wordt geregistreerd.

De Koning kan, na advies van de Gegevensbeschermingsautoriteit en van het Instituut, de eisen bepalen die de operatoren in acht moeten nemen wat betreft het logboek.

In het kader van de controle van de operator mogen het Instituut en de Gegevensbeschermingsautoriteit dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.

§ 5. Indien het Instituut over aanwijzingen beschikt die zouden kunnen duiden op een inbreuk van een operator op paragraaf 2, 3 of 4, dan kan het de operator verplichten om zich te onderwerpen aan een veiligheidscontrole door een gekwalificeerde onafhankelijke instantie die de operator ter goedkeuring voorlegt aan het Instituut.

Die instantie neemt geen kennis van de verzoeken van de autoriteiten jegens de operatoren, inclusief het logboek bedoeld in paragraaf 4.

Het rapport en de resultaten van deze veiligheidscontrole worden bezorgd aan het Instituut. De kosten van de controle worden door de operator gedragen.".

Art. 13

In dezelfde wet, wordt een artikel 127/3 ingevoegd, luidende:

"Art. 127/3. § 1er. Auprès de chaque opérateur est constituée une Cellule de coordination, chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques.

Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l'alinéa 1er. Ils peuvent cependant, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur.

Ces autorités adressent leurs demandes à cette cellule.

Le cas échéant, plusieurs opérateurs peuvent créer une Cellule de coordination commune. En pareil cas, chaque opérateur prend les mesures nécessaires pour que cette Cellule de coordination commune soit en mesure de répondre aux demandes qui lui sont adressées.

Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité.

§ 2. Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel. Ces membres ne communiquent aux préposés que les données strictement nécessaires pour obtenir cette aide.

Chaque opérateur veille à la confidentialité des données traitées par la Cellule de coordination.

Les membres de la Cellule de coordination disposent d'un avis de sécurité positif et non périmé, visé à l'article 22*quinquies*/1 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Un avis de sécurité a une durée de validité de maximum 5 ans.

L'autorité administrative compétente pour le traitement des avis est le ministre de la Justice.

Le Roi définit des mesures de sécurité alternatives à un avis de sécurité, qui sont adaptées aux personnes pour lesquelles un avis de sécurité ne peut être rendu, à défaut d'informations suffisantes les concernant.

Par dérogation à l'alinéa 3, une personne visée à l'alinéa 6 peut faire partie de la Cellule de coordination,

"Art. 127/3. § 1. Bij elke operator wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.

Enkel de leden van de Coördinatiecel mogen antwoorden op de verzoeken van de autoriteiten met betrekking tot de gegevens bedoeld in het eerste lid. Ze mogen echter, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator.

Deze autoriteiten richten hun verzoeken tot deze cel.

In voorkomend geval kunnen verscheidene operatoren een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval neemt elke operator de nodige maatregelen opdat deze gemeenschappelijke Coördinatiecel in staat is om te antwoorden op de verzoeken die eraan worden gericht.

De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens, en van het Instituut, de vereisten waaraan de Coördinatiecel moet beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid.

§ 2. De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim. Deze leden delen aan de aangestelden enkel de gegevens mee die strikt noodzakelijk zijn om die bijstand te krijgen.

Elke operator waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel.

De leden van de Coördinatiecel beschikken over een positief en niet-achterhaald veiligheidsadvies bedoeld in artikel 22*quinquies*/1 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Een veiligheidsadvies heeft een maximale geldigheidsduur van 5 jaar.

De administratieve instantie die bevoegd is voor de behandeling van de adviezen is de "van Justitie.

De Koning bepaaltalternatieve veiligheidsmaatregelen die passend zijn voor de personen voor wie een veiligheidsadvies niet kan worden verstrekt wegens gebrek aan voldoende informatie.

In afwijking van het derde lid kan een in het zesde lid bedoelde persoon deel uitmaken van de Coördinatiecel, wanneer deze alternatieve veiligheidsmaatregelen in acht

en respectant ces mesures de sécurité alternatives et sans disposer d'un avis de sécurité.

Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut:

1° pour les opérateurs autres que ceux qui disposent déjà d'un officier de sécurité en raison d'autres activités que la Cellule de coordination, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un tel officier en fonction du nombre de demandes reçues de la part des autorités judiciaires, ainsi que les règles qui s'appliquent en l'absence d'un tel officier;

2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en particulier en matière d'emploi des langues;

3° les règles permettant l'accès des autorités belges habilitées aux coordonnées de la Cellule de coordination et de ses membres.

§ 3. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs finaux. Il met, sur demande, à la disposition de l'Institut, des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Chaque opérateur est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur base des articles 122, 123, 126, 126/1 et 127.

§ 4. Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles. Sont déterminés, entre autres, les éléments suivants, le cas échéant et par autorité concernée:

a) le mode de transfert, la forme et le contenu des demandes et des réponses;

b) le degré d'urgence de traitement des demandes;

c) le délai de réponse;

d) la disponibilité requise du service;

e) les modalités de test de la collaboration;

f) les tarifs de rétribution de cette collaboration.

worden genomen en zonder over een veiligheidsadvies te beschikken.

De Koning bepaalt na advies van de autoriteiten bevoegd voor de bescherming van de gegevens, en van het Instituut het volgende:

1° voor de andere operatoren dan diegene die reeds over een veiligheidsofficier beschikken wegens andere activiteiten dan de Coördinatiecel, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een dergelijke officier aan te stellen in functie van het aantal verzoeken ontvangen vanwege de gerechtelijke autoriteiten, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inzonderheid wat het gebruik van de talen betreft;

3° de regels voor de toegang van de gemachtigde Belgische autoriteiten tot de contactgegevens van de Coördinatiecel en zijn leden.

§ 3. Elke operator stelt een interne procedure voor het beantwoorden van de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens van eindgebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en zijn antwoord.

Elke operator wordt beschouwd als verwerkingsverantwoordelijke in de zin van de AVG, voor de gegevens verwerkt op basis van artikelen 122, 123, 126, 126/1 en 127.

§ 4. De Koning bepaalt na advies van de autoriteiten bevoegd voor de bescherming van de gegevens, en van het Instituut de regels voorde samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen. Zo worden onder andere, in voorkomend geval en per betrokken overheid, de volgende zaken geregeld:

a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;

b) het dringendheidsniveau voor de behandeling van de verzoeken;

c) de antwoordtermijn;

d) de vereiste beschikbaarheid van de dienst;

e) de modaliteiten voor het testen van de samenwerking;

f) de tarieven voor de vergoeding van die samenwerking.

Si nécessaire et pour l'application du présent article, le Roi peut prévoir des règles différentes selon différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et la fourniture ou non d'un réseau de communications électroniques en Belgique.".

Art. 14

À l'article 145 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, les modifications suivantes sont apportées:

1° Le paragraphe 1er est remplacé par ce qui suit:

"§ 1er. Est punie d'une amende de 50 à 100 000 euros, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 107/5, 124, 126 à 127/3, 133 et les arrêtés pris en exécution des articles 9, § 7, 32, 39, § 3, 47, 106/2, 126, 126/1, 127, 127/2 et 127/3.";

2° au lieu du paragraphe 3*ter*, annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré un paragraphe 3*ter* rédigé comme suit:

"§ 3*ter*. Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement:

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données conservées par l'opérateur pour les autorités;

2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1°, les détient, les révèle à une autre personne, les divulgue ou en fait un usage quelconque.".

Indien nodig en voor de toepassing van dit artikel, kan de Koning verschillende regels bepalen al naargelang de verschillende categorieën van operatoren, met name volgens het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en of zij al dan niet een elektronische-communicatienetwerk aanbieden in België.".

Art. 14

In artikel 145 van dezelfde wet, laatstelijk gewijzigd door de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, worden de volgende wijzigingen aangebracht:

1° Paragraaf 1 wordt vervangen als volgt:

"§ 1. Met een geldboete van 50 tot 100 000 euro wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 107/5, 124, 126 tot en met 127/3, 133 en de ter uitvoering van de artikelen 9, § 7, 32, 39, § 3, 47, 106/2, 126, 126/1,127, 127/2 en 127/3 genomen besluiten overtreedt.";

2° in de plaats van paragraaf 3*ter*, vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt een als volgt luidende paragraaf 3*ter* ingevoegd:

"§ 3*ter*. Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de door de operator voor de autoriteiten bewaarde gegevens op enige manier overneemt, bij zich houdt of er enig gebruik van maakt;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.".

CHAPITRE 3

Modifications à la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques

Art. 15

L'article 8 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques est complété par un alinéa rédigé comme suit:

"Dans le cadre de l'application de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, après la désignation d'une infrastructure critique et au moins annuellement, la DGCC fournit au service désigné par le Roi, la commune dans laquelle l'infrastructure critique est située ou, le cas échéant, une liste des communes dans lesquelles les infrastructures critiques sont situées.".

CHAPITRE 4

Modifications à la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 16

L'article 2, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, modifié par la loi du 25 avril 2007, est complété par le 5°, rédigé comme suit:

"5° "Données relatives à l'utilisateur final ou à l'abonné":

— les données de souscription de l'abonné au service;

— les données visant à établir l'identité civile de l'abonné ou de l'utilisateur final, en ce compris les données de paiement;

— les données techniques d'identification de l'utilisateur final, de l'équipement terminal ou du service de communications électroniques, sans que ces données ne puissent donner des informations sur le destinataire de la communication, en ce compris les adresses IP du destinataire de la communication ou sur la localisation précise de l'équipement terminal;

HOOFDSTUK 3

Wijzigingen aan de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

Art. 15

Artikel 8 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren wordt aangevuld met een lid, luidende:

"De ADCC bezorgt na de aanduiding van een kritieke infrastructuur en minstens jaarlijks de gemeente waarin de kritieke infrastructuur zich bevindt of in voorkomend geval een lijst van gemeenten waarin de kritieke infrastructuren zich bevinden aan de door de Koning aangewezen dienst voor de toepassing van artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie.".

HOOFDSTUK 4

Wijzigingen aan de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en elecommunicatiesector

Art. 16

Artikel 2, eerste lid van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, gewijzigd bij de wet van 25 april 2007, wordt aangevuld met de bepaling onder 5°, luidende:

"5° "Gegevens betreffende de eindgebruiker of de abonnee":

— de intekeningsgegevens van de abonnee op de dienst;

— de gegevens ter vaststelling van de burgerlijke identiteit van de abonnee of van de eindgebruiker, met inbegrip van de betalingsgegevens;

— de technische identificatiegegevens van de eindgebruiker, van de eindapparatuur of van de elektronische-communicatiedienst, zonder dat deze gegevens informatie kunnen verstrekken over de bestemmeling van de communicatie, met inbegrip van de IP-adressen van de bestemmeling van de communicatie of over de precieze locatie van de eindapparatuur;

— les données visant à déterminer le moment de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement au réseau en raison de l'extinction de cet équipement.".

Art. 17

À l'article 14 de la même loi, modifié en dernier lieu par la loi du 17/02/2022 modifiant diverses dispositions en matière de communications électroniques en vue d'introduire des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G, les modifications suivantes sont apportées:

1° Au paragraphe 1er, au 3°, la disposition sous d) est remplacée par ce qui suit:

"d) les articles 14, § 2, 2° et 2°/1, 21, §§ 5 à 7, 25, §§ 8 à 10 et 28/1 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges;";

2° Au paragraphe 2, les 2/1° et 2/2° sont insérés, rédigés comme suit:

"2°/1 peut exiger d'un opérateur des données relatives à l'utilisateur final ou à l'abonné ou d'autres métadonnées de communications électroniques, qui sont nécessaires à l'accomplissement de l'une de ses missions d'application et de contrôle des dispositions prévues à l'article 14, paragraphe 1er, 3°, a) et g) à i), aux conditions prévues aux articles 25, §§ 8 à 9 et 28/1, §§ 1er et 2;

2°/2 peut exiger d'un opérateur de lui permettre de consulter une base de données contenant les données dont la conservation est prévue par ou en vertu des articles 122, 123, 126, 126/1 et 127 de la loi du 13 juin 2005 relative aux communications, pour le contrôle du respect par un opérateur de ces articles ou de leurs arrêtés d'exécution, aux conditions prévues aux articles 25, § 10 et 28/1, § 3;".

Art. 18

L'article 25 de la même loi, modifié en dernier lieu par la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, est complété par les paragraphes 8 à 11, rédigés comme suit:

— de gegevens ter bepaling van het moment van de verbinding van de eindapparatuur met het netwerk na een heropstart van die apparatuur en het moment waarop de verbinding van die apparatuur met het netwerk wordt verbroken doordat die apparatuur wordt uitgeschakeld.".

Art. 17

In artikel 14 van dezelfde wet, laatstelijk gewijzigd bij de wet van 17/02/2022 tot wijziging van diverse bepalingen inzake elektronische communicatie met het oog op de invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten, worden de volgende wijzigingen aangebracht:

1° In paragraaf 1, wordt in de bepaling onder 3°, de bepaling onder d) vervangen als volgt:

"d) de artikelen 14, § 2, 2° en 2°/1, 21, §§ 5 tot en met 7, 25, §§ 8 tot en met 10 en 28/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;";

2° In paragraaf 2, de bepalingen onder 2/1° en 2/2° worden ingevoegd, luidende:

"2°/1 kan het Instituut van een operator gegevens betreffende de eindgebruiker of de abonnee, of andere metagegevens van elektronische communicatie opvragen, die noodzakelijk zijn voor de vervulling van een van zijn opdrachten inzake toepassing en controle van de in artikel 14, paragraaf 1, 3°, a) en g) tot i), vastgestelde bepalingen, onder de voorwaarden van de artikelen 25, §§ 8 tot 9, en 28/1, §§ 1 en 2;

2°/2 kan het Instituut van een operator eisen dat deze het Instituut een databank laat raadplegen die gegevens bevat die moeten worden bewaard door of krachtens de artikelen 122, 123, 126, 126/1 en 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie, om te controleren of een operator deze artikelen of de uitvoeringsbesluiten ervan naleeft, onder de voorwaarden van de artikelen 25, § 10 en 28/1, § 3;".

Art. 18

Artikel 25 van dezelfde wet, laatstelijk gewijzigd bij de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, wordt aangevuld met de paragrafen 8 tot 11, luidende:

"§ 8. Pour les besoins de l'accomplissement de leurs missions, les officiers de police judiciaire de l'Institut peuvent exiger d'un opérateur de leur fournir des données relatives à l'utilisateur final ou à l'abonné conservées par l'opérateur, qui sont nécessaires afin de rechercher, de constater ou de poursuivre une infraction à une loi visée à l'article 24, lorsque celle-ci est commise au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications au sens de la loi du 13 juin 2005 relative aux communications électroniques.

L'officier de police judiciaire soumet sa demande motivée à l'autorisation préalable de son supérieur hiérarchique.

§ 9. Pour les besoins de l'accomplissement de leurs missions, les officiers de police judiciaire de l'Institut peuvent exiger d'un opérateur de leur fournir des métadonnées de communications électroniques autres que les données relatives à l'utilisateur final ou à l'abonné, qui sont nécessaires afin de rechercher, de constater ou de poursuivre une infraction à une loi visée à l'article 24, lorsque celle-ci est commise au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications au sens de la loi du 13 juin 2005 relative aux communications électroniques.

L'officier de police judiciaire soumet sa demande motivée à l'autorisation préalable du juge d'instruction, sauf cas d'urgence dûment justifié.

En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction la demande envoyée à l'opérateur sans délai après cet envoi. Un contrôle ultérieur est effectué par le juge d'instruction.

§ 10. Par dérogation aux paragraphes 8 et 9, à la demande d'un officier de police judiciaire de l'Institut et après autorisation du Conseil de l'Institut, un opérateur permet à cet officier de consulter ses bases de données qui mettent en œuvre les articles 126, 126/1 et 127 de la loi du 13 juin 2005 relative aux communications électroniques, afin de contrôler le respect de ces articles et de leurs arrêtés d'exécution.

Ces officiers ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

"§ 8. Ten behoeve van de vervulling van hun opdrachten kunnen de officieren van gerechtelijke politie van het Instituut van een operator eisen dat hij hen door de operator bewaarde gegevens betreffende de eindgebruiker of de abonnee verstrekt, die nodig zijn om een inbreuk op een in artikel 24 bedoelde wet te kunnen opsporen, vaststellen of vervolgen, wanneer die is gepleegd door middel van apparatuur, netwerken of diensten voor elektronische communicatie of radiocommunicatie in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie.

De officier van gerechtelijke politie legt zijn met redenen omkleed verzoek vooraf voor goedkeuring voor aan zijn hiërarchische meerdere.

§ 9. Ten behoeve van de vervulling van hun opdrachten kunnen de officieren van gerechtelijke politie van het Instituut van een operator eisen dat hij hen andere metagegevens van elektronische communicatie verstrekt dan de gegevens betreffende de eindgebruiker of de abonnee, die nodig zijn om een inbreuk op een in artikel 24 bedoelde wet te kunnen opsporen, vaststellen of vervolgen, wanneer die is gepleegd door middel van apparatuur, netwerken of diensten voor elektronische communicatie of radiocommunicatie in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie.

De officier van gerechtelijke politie legt zijn met redenen omkleed verzoek ter voorafgaande goedkeuring voor aan de onderzoeksrechter, tenzij in een naar behoren gerechtvaardigd noodgeval.

In een naar behoren gerechtvaardigd noodgeval zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het Instituut het naar de operator verzonden verzoek na deze verzending onverwijld mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.

§ 10. In afwijking van de paragrafen 8 en 9, staat een operator op verzoek van een officier van gerechtelijke politie van het Instituut en na toestemming van de Raad van het Instituut, het aan deze officier toe om zijn databanken te raadplegen die uitvoering verlenen aan de artikelen 126, 126/1 en 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie uitvoeren, om de naleving van die artikelen en van de uitvoeringsbesluiten ervan te controleren.

Deze officiers mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid om inbreuken gepleegd door de operator vast te stellen.

§ 11. Les officiers de police judiciaire de l'Institut consignent les demandes visées aux paragraphes 8, 9 et 10 dans un inventaire.".

§ 11. De officiers van gerechtelijke politie van het Instituut nemen de verzoeken bedoeld in de paragrafen 8, 9 en 10 op in een inventaris.".

Art. 19

Art. 19

Dans le chapitre III de la même loi, il est inséré un article 28/1, rédigé comme suit:

In hoofdstuk III van dezelfde wet wordt een artikel 28/1 ingevoegd, luidende:

"Art. 28/1. § 1er. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), les membres du personnel de l'Institut, qui n'agissent pas dans un cadre pénal, peuvent exiger d'un opérateur de leur fournir des données relatives à l'utilisateur final ou à l'abonné conservées par l'opérateur.

"Art. 28/1. § 1. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mogen de personeelsleden van het Instituut die niet in een strafrechtelijk kader optreden, van een operator eisen dat hij hen door de operator bewaarde gegevens betreffende de eindgebruiker of de abonnee verstrekt.

Le membre du personnel soumet sa demande motivée à l'autorisation préalable de son supérieur hiérarchique.

Het personeelslid legt zijn met redenen omkleed verzoek ter voorafgaandegoedkeuring voor aan zijn hiërarchische meerdere.

§ 2. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), les membres du personnel de l'Institut, qui n'agissent pas dans un cadre pénal, peuvent exiger d'un opérateur de leur fournir des métadonnées de communications électroniques conservées par l'opérateur, autres que les données relatives à l'utilisateur final ou à l'abonné.

§ 2. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mogen de personeelsleden van het Instituut die niet in een strafrechtelijk kader optreden, van een operator eisen dat hij hen andere door de operator bewaarde metagegevens van elektronische communicatie verstrekt dan de gegevens betreffende de eindgebruiker of de abonnee.

Il soumet préalablement sa demande motivée à l'approbation de l'Autorité de protection des données, sauf cas d'urgence dûment justifié. En cas d'urgence dûment justifiée, il communique à l'Autorité de protection des données, la demande envoyée à l'opérateur sans délai après cet envoi. Un contrôle ultérieur est effectué par l'Autorité de protection des données.

Hij legt zijn met redenen omkleed verzoek vooraf voor goedkeuring voor aan de Gegevensbeschermingsautoriteit, behalve in een naar behoren gerechtvaardigd noodgeval. In een naar behoren gerechtvaardigd noodgeval deelt hij het naar de operator verzonden verzoek na deze verzending onverwijld mee aan de Gegevensbeschermingsautoriteit. De Gegevensbesch ermingsautoriteit voert daarna een controle uit.

§ 3. L'alinéa 2 du paragraphe 2 n'est pas applicable lorsque l'Institut contrôle le respect par un opérateur des articles 122 et 123 de la loi du 13 juin 2005 relative aux communications électroniques, en consultant si nécessaire les bases de données qui mettent en œuvre ces articles.

§ 3. Het tweede lid van paragraaf 2 is niet van toepassing wanneer het Instituut de naleving door de operator van de artikelen 122 en 123 van de wet van 13 juni 2005 betreffende de elektronische communicatie controleert, in voorkomend geval door de databanken die uitvoering verlenen aan deze artikelen te raadplegen.

§ 4. Les demandes qui sont formulées conformément aux paragraphes 1er, 2 et 3 sont consignées dans un inventaire tenu auprès de l'Institut.".

§ 4. De verzoeken die worden geformuleerd overeenkomstig de paragrafen 1, 2 en 3 worden opgenomen in een inventaris die bij het Instituut wordt bijgehouden.".

CHAPITRE 5

Modifications au Code d'instruction criminelle

Art. 20

Dans le Code d'instruction criminelle, un article 39*quinquies* est inséré, rédigé comme suit:

"Art. 39*quinquies*. § 1. Lors de la recherche de crimes et délits, le procureur du Roi peut, s'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, ordonner, par une décision écrite et motivée, à un ou plusieurs acteurs visés à l'alinéa 2, de conserver les données visées à l'article 88*bis*, § 1, alinéa 1er, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu'il juge nécessaires.

L'ordre visé à l'alinéa 1er peut être donné, directement ou par l'intermédiaire du service de police désigné par le Roi, à:

– l'opérateur d'un réseau de communications électroniques; et

– toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La décision écrite et motivée mentionne:

— le nom du procureur du Roi qui ordonne la conservation;

— l'infraction qui fait l'objet de l'ordre;

— les circonstances de fait de la cause qui justifient la conservation;

— l'indication précise d'un ou de plusieurs des éléments suivants: la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;

— le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;

HOOFDSTUK 5

Wijzigingen aan het Wetboek van strafvordering

Art. 20

In het Wetboek van strafvordering wordt een artikel 39*quinquies* ingevoerd, luidende:

"Art. 39*quinquies*. § 1. Bij het opsporen van de misdaden en de wanbedrijven kan de procureur des Konings, wanneer er ernstige aanwijzingen zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, bij een met redenen omklede en schriftelijke beslissing aan een of meerdere van de actoren bedoeld in het tweede lid bevelen de noodzakelijke gegevens bedoeld in artikel 88*bis*, § 1, eerste lid, die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Het bevel bedoeld in het eerste lid kan, rechtstreeks of via de door de Koning aangewezen politiedienst, gegeven worden aan:

– de operator van een elektronisch communicatienetwerk; en

– iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

De met redenen omklede en schriftelijke beslissing vermeldt:

— de naam van de procureur des Konings die de bewaring beveelt;

— het strafbare feit waarop het bevel betrekking heeft;

— de feitelijke omstandigheden van de zaak die de bewaring van de gegevens rechtvaardigen;

— de precieze aanduiding van één of meerdere van de volgende elementen: de persoon of de personen, de communicatiemiddelen of de plaatsen waarop de bewaring betrekking heeft;

— in voorkomend geval, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden;

— la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;

— la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. L'ordre doit être confirmé dans les plus brefs délais dans la forme prévue à l'alinéa 3.

§ 2. Les acteurs visés au § 1er, alinéa 2 veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, est punie d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

§ 4. L'accès aux données conservées conformément à cet article n'est possible qu'en application de l'article 88*bis*.".

Art. 21

Dans l'article 88*bis* du même Code, inséré par la loi du 11 février 1991 et modifié en dernier lieu par la loi du 5 mai 2019, les modifications suivantes sont apportées:

1° Le paragraphe 2, inséré par la loi du 29 mai 2016 et annulé par l'arrêt n° 57/2021 du 22 avril 2021 de la Cour Constitutionnelle, est rétabli dans la rédaction suivante:

"Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent:

— pour une infraction visée au livre II, titre I*ter*, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;

— de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevel, onverminderd een hernieuwing;

— de duur van bewaring van deze gegevens, die niet langer mag zijn dan zes maanden. Deze termijn kan schriftelijk worden verlengd.

In spoedeisende gevallen kan het bevel tot bewaring mondeling worden gegeven. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde lid.

§ 2. De actoren bedoeld in § 1, tweede lid zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van zesentwintig tot twintigduizend euro of met één van die straffen alleen.

§ 4. De toegang tot de overeenkomstig dit artikel bewaarde gegevens kan slechts met toepassing van artikel 88*bis*.".

Art. 21

In artikel 88*bis*, ingevoegd bij de wet van 11 februari 1991 en laatstelijk gewijzigd bij de wet van 5 mei 2019, worden de volgende wijzigingen aangebracht:

1° Paragraaf 2, ingevoegd bij de wet van 29 mei 2016 en vernietigd door arrest nr. 57/2021 van 22 april 2021 van het Grondwettelijk Hof, wordt hersteld als volgt:

"Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:

— voor een strafbaar feit bedoeld in boek II, titel I*ter*, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift;

— pour une autre infraction visée à l'article 90*ter*, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;

— pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.";

2° Le paragraphe 3, inséré par la loi du 29 mai 2016, modifié par la loi du 5 mai 2019 et annulé par l'arrêt n° 57/2021 du 22 avril 2021 de la Cour Constitutionnelle, est rétabli dans la rédaction suivante:

"La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.".

— voor een ander strafbaar feit bedoeld in artikel 90*ter*, §§ 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

— voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.";

2° Paragraaf 3, ingevoegd bij de wet van 29 mei 2016, gewijzigd bij de wet van 5 mei 2019 en vernietigd door arrest nr. 57/2021 van 22 april 2021 van het Grondwettelijk Hof, wordt hersteld als volgt:

"De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Dezelfde personen zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.".

CHAPITRE 6

Modifications à la loi du 5 août 1992 sur la fonction de police

Art. 22

À l'article 42 de la loi du 5 août 1992 sur la fonction de police, modifié par la loi du 12 novembre 2017, les modifications suivantes sont apportées:

1° Le mot "§ 1er." est inséré au début de l'article;

HOOFDSTUK 6

Wijzigingen aan de wet van 5 augustus 1992 op het politieambt

Art. 22

In artikel 42 van wet van 5 augustus 1992 op het politieambt, gewijzigd bij de wet van 12 november 2017, worden de volgende wijzigingen aangebracht:

1° Het woord "§ 1." wordt ingevoegd aan het begin van het artikel;

2° L'article est complété par les paragraphes 2 et 3, rédigés comme suit:

"§ 2. Un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue.

Seules les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication et relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, concernant la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données, sont communiquées.

La réquisition est adressée par l'officier de police judiciaire visé au paragraphe 2, alinéa 1er, à:

— l'opérateur d'un réseau de communications électroniques; ou

— toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

§ 3. La réquisition et sa justification sont notifiées par la Cellule Personnes Disparues à l'Organe de contrôle, au plus tard dans les 48 heures après la réquisition.

Si l'Organe de contrôle estime que les conditions pour effectuer cette réquisition ne sont pas remplies, il ordonne, de manière motivée, l'interdiction d'exploiter les données obtenues par ce moyen et l'effacement des données.

Cette décision motivée est notifiée dans les meilleurs délais possibles par l'Organe de contrôle à la Cellule Personnes Disparues.".

2° Het artikel wordt aangevuld met de paragrafen 2 en 3, luidende:

"§ 2. Een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kan, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood en de opsporing van personen van wie de verdwijning onrustwekkend is, en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon opvorderen.

Enkel de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen en met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, betreffende de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan de opvordering, worden meegedeeld.

De vordering wordt via de officier van gerechtelijke politie bedoeld in paragraaf 2, eerste lid 1, gericht aan:

— de operator van een elektronisch communicatienetwerk; of

— iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

§ 3. De Cel Vermiste Personen stelt het Controleorgaan uiterlijk binnen 48 uur na de vordering in kennis van de vordering en de motivering ervan.

Indien het Controleorgaan van oordeel is dat niet aan de voorwaarden voor de uitvoering van deze vordering is voldaan, beveelt zij, met opgave van redenen, dat de aldus verkregen gegevens niet mogen worden gebruikt en vernietigd moeten worden.

Deze met redenen omklede beslissing wordt door het Controleorgaan zo spoedig mogelijk meegedeeld aan de Cel Vermiste Personen.".

CHAPITRE 7

Modifications à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 23

À l'article 3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, la disposition sous 10° est complétée par les mots ", quelle que soit la nature de l'émetteur ou du récepteur".

Art. 24

À l'article 7 de la même loi, les mots ", chargée de la sécurité nationale," sont insérés entre les mots "La Sûreté de l'État" et "a pour mission".

Art. 25

Dans l'article 11 de la même loi, les mots ", chargé de la sécurité nationale," sont insérés entre les mots "Renseignement et de la Sécurité" et "a pour mission".

Art. 26

Au chapitre III, une section 3/1 est insérée, intitulée "Réquisitions de conservation".

Art. 27

Dans la section 3/1, insérée par l'article 26, un article 13/6 est inséré, rédigé comme suit:

"Art. 13/6. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à:

1° la conservation des données de trafic et de localisation de moyens de communications électroniques qui sont à sa disposition au moment de la réquisition;

2° la conservation des données de trafic et de localisation qu'il génère et traite à partir de la réquisition.

HOOFDSTUK 7

Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Art. 23

In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, wordt de bepaling onder 10° aangevuld met de woorden ", ongeacht de aard van de afzender of de ontvanger;".

Art. 24

In artikel 7 van dezelfde wet, worden de woorden ", belast met de nationale veiligheid," ingevoegd tussen de woorden "Veiligheid van de Staat" en "heeft als opdracht".

Art. 25

In artikel 11 van dezelfde wet, worden de woorden ", belast met de nationale veiligheid," ingevoegd tussen de woorden "Inlichting en Veiligheid" en "heeft als opdracht".

Art. 26

In hoofdstuk III, wordt een afdeling 3/1 ingevoegd, luidende "Vorderingen tot bewaring".

Art. 27

In afdeling 3/1, ingevoegd bij artikel 26, wordt een artikel 13/6 ingevoegd, luidende:

"Art. 13/6. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst om over te gaan tot:

1° de bewaring van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen waarover hij beschikt op het tijdstip van de vordering;

2° de bewaring van de verkeers- en lokalisatiegegevens die hij op basis van de vordering genereert en verwerkt.

La réquisition visée à l'alinéa 1er repose sur une décision écrite et motivée du dirigeant du service ou de son délégué.

§ 2. La réquisition est adressée à l'opérateur ou au fournisseur visé au § 1er, alinéa 1er et mentionne:

1° la nature des données de trafic et de localisation à conserver;

2° les personnes, les groupements, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation doivent être conservées;

3° pour la mesure visée au § 1er, alinéa 1er, 1°, le délai de conservation des données qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

4° pour la mesure visée au § 1er, alinéa 1er, 2°:

— la durée de la mesure qui ne peut excéder six mois à compter de la date de la réquisition sans préjudice de la possibilité de prolongation en suivant la même procédure;

— le délai de conservation qui ne peut excéder six mois à compter de la date de la communication sans préjudice de la possibilité de prolongation en suivant la même procédure;

5° la date de la réquisition;

6° la signature du dirigeant du service ou de son délégué;

§ 3. En cas d'urgence, le dirigeant du service ou son délégué peut requérir la conservation verbalement. Cette réquisition verbale est confirmée par écrit au plus tard le premier jour ouvrable qui suit.

§ 4. Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.

Chaque décision de réquisition est notifiée avec sa motivation au Comité permanent R. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la réquisition.

Lorsqu'il est mis fin prématurément à la réquisition, l'opérateur d'un réseau de communications électroniques

De in het eerste lid bedoelde vordering is gebaseerd op een schriftelijke en gemotiveerde beslissing van het diensthoofd of zijn gedelegeerde.

§ 2. De vordering is gericht aan de in § 1, eerste lid bedoelde operator of verstrekker en vermeldt:

1° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

2° de personen, groeperingen, geografische gebieden, communicatiemiddelen en/of gebruikswijze waarvan de verkeers- en lokalisatiegegevens moeten bewaard worden;

3° voor de maatregel bedoeld in § 1, eerste lid, 1°, de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

4° voor de maatregel bedoeld in § 1, eerste lid, 2°:

— de duur van de maatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

— de bewaartermijn die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

5° de datum van de vordering;

6° de handtekening van het diensthoofd of van zijn gedelegeerde;

§ 3. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de bewaring mondeling vorderen. Deze mondelinge vordering wordt schriftelijk bevestigd uiterlijk op de eerstvolgende werkdag.

§ 4. De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring.

Elke beslissing tot vordering en de motivering ervan worden ter kennis gebracht van het Vast Comité I. Indien het Vast Comité I een onwettigheid vaststelt, maakt het een einde aan de vordering.

Indien de vordering voortijdig wordt beëindigd, wordt de gevorderde operator van een elektronisch

ou le fournisseur d'un service de communications électroniques requis en est averti le plus rapidement possible.

§ 5. Pour l'exécution de la réquisition, le dirigeant du service ou son délégué peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale.

§ 6. Toute personne qui refuse de prêter son concours aux réquisitions visées aux § § 1er et 5 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 7. Le Roi peut déterminer, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs et des fournisseurs.".

Art. 28

Dans la même section, un article 13/7 est inséré, rédigé comme suit:

"Art. 13/7. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs d'un réseau de communications électroniques et des fournisseurs d'un service de communications électroniques afin de procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traitées par eux.

§ 2. La réquisition visée au § 1er ne peut avoir lieu qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

§ 3. La demande du dirigeant du service de requérir la conservation mentionne, sous peine d'illégalité:

1° la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible;

communicatienetwerk of de verstrekker van een elektronische communicatiedienst daarvan zo spoedig mogelijk op de hoogte gebracht.

§ 5. Voor de uitvoering van de vordering kan het diensthoofd of zijn gedelegeerde de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag.

§ 6. Eenieder die weigert zijn medewerking te verlenen aan de in § 1 en § 5 bedoelde vorderingen, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.

§ 7. De Koning kan, op voorstel van de "van Justitie, de "van Landsverdediging en de "bevoegd voor de elektronische communicatie, de nadere regels bepalen voor de samenwerking van de operatoren en de verstrekkers.".

Art. 28

In dezelfde afdeling wordt een artikel 13/7 ingevoegd, luidende:

"Art. 13/7. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, de medewerking vorderen van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronisch communicatiedienst om over te gaan tot de algemene en ongedifferentieerde bewaring van de door hen gegenereerde en verwerkte verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen.

§ 2. De in § 1 bedoelde vordering kan enkel ingesteld worden mits een voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar akkoord binnen vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

§ 3. De vraag van het diensthoofd om een vordering tot bewaring in te stellen vermeldt, op straffe van onwettigheid:

1° de ernstige dreiging tegen de nationale veiligheid die reëel en actueel of voorzienbaar is;

2° les circonstances de fait qui justifient la conservation généralisée et indifférenciée des données de trafic et de localisation;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure de conservation qui ne peut excéder six mois à compter de la date de la réquisition. Elle peut être prolongée en suivant la même procédure;

5° le délai de conservation des données qui ne peut excéder six mois à compter de la date de la communication. Elle peut être prolongée en suivant la même procédure;

6° le cas échéant, les motifs qui justifient l'extrême urgence visée au § 5;

7° la date de la demande;

8° la signature du dirigeant du service.

§ 4. La réquisition est adressée aux opérateurs et aux fournisseurs visés au § 1er et mentionne:

1° la date de l'accord de la Commission;

2° la nature des données de trafic et de localisation à conserver;

3° la durée de la mesure et le délai de conservation des données;

4° la date de la réquisition;

5° la signature du dirigeant du service ou de son délégué.

§ 5. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, en cas d'indisponibilité, d'un autre membre de la Commission. L'auteur de l'accord en informe immédiatement les autres membres de la Commission. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant l'accord. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

§ 6. La réquisition de conservation généralisée et indifférenciée est confirmée par arrêté royal.

L'arrêté royal ne mentionne que:

2° de feitelijke omstandigheden die de ongedifferentieerde en algemene bewaring van de verkeers- en lokalisatiegegevens rechtvaardigen;

3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

4° de duur van de bewaringsmaatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering. Hij kan volgens dezelfde procedure worden verlengd;

5° de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie. Hij kan volgens dezelfde procedure worden verlengd;

6° in voorkomend geval, de redenen die de in § 5 bedoelde hoogdringendheid rechtvaardigen;

7° de datum van de vraag;

8° de handtekening van het diensthoofd.

§ 4. De vordering is gericht aan de in § 1 bedoelde operatoren en verstrekkers en vermeldt:

1° de datum van het akkoord van de Commissie;

2° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

3° de duur van de maatregel en de bewaartermijnvan de gegevens;

4° de datum van de vordering;

5° de handtekening van het diensthoofd of zijn gedelegeerde.

§ 5. In geval van hoogdringendheid vraagt het diensthoofd vooraf om het mondelinge akkoord van de voorzitter van de Commissie of, indien deze niet beschikbaar is, een ander lid van de Commissie. De auteur van het akkoord informeert onmiddellijk de andere commissieleden. Het diensthoofd bevestigt zijn vraag schriftelijk binnen 24 uur volgend op het akkoord. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord is gedurende vijf dagen geldig.

§ 6. De vordering tot een algemene en ongedifferentieerde bewaring wordt bevestigd bij koninklijk besluit.

Het koninklijk besluit vermeldt enkel:

1° la date de l'accord de la Commission

2° la date de la réquisition;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure et le délai de conservation des données;

En l'absence de confirmation par arrêté royal dans le mois de la réquisition, cette réquisition prend fin.

Les opérateurs d'un réseau de communications électroniques et les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 7. Pour l'exécution de la réquisition, le dirigeant du service peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale et l'accord de la Commission.

§ 8. Toute personne qui refuse de prêter son concours aux réquisitions visées aux § § 1er et 7 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 9. La Commission transmet sans délai la demande du dirigeant du service et son accord au Comité permanent R.

§ 10. Le service de renseignement et de sécurité fait rapport à la Commission toutes les deux semaines sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

§ 11. Le dirigeant du service met fin à la réquisition, nonobstant la confirmation par arrêté royal, lorsque la conservation n'est plus utile pour lutter contre la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, lorsque cette menace a disparu ou lorsqu'il constate une illégalité.

Lorsque la Commission ou le Comité permanent R constate une illégalité, il est mis fin à la réquisition nonobstant la confirmation par arrêté royal.

Lorsqu'il est mis fin prématurément à la réquisition, les opérateurs d'un réseau de communications électroniques

1° de datum van het akkoord van de Commissie;

2° de datum van de vordering;

3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

4° de duur van de maatregel en de bewaartermijn van de gegevens;

Bij gebrek aan bevestiging bij koninklijk besluit binnen een maand na de vordering, eindigt de vordering.

De gevorderde operatoren van een elektronisch communicatienetwerk of verstrekkers van een elektronische communicatiedienst worden hiervan zo spoedig mogelijk op de hoogte gebracht.

§ 7. Voor de uitvoering van de vordering kan het diensthoofd de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag en het akkoord van de Commissie.

§ 8. Eenieder die weigert zijn medewerking te verlenen aan de in § 1 en § 7 bedoelde vorderingen wordt gestraft met een geldboete van zesentwintig tot twintigduizend euro.

§ 9. De Commissie geeft onverwijld de vraag van het diensthoofd en haar akkoord door aan het Vast Comité I.

§ 10. De inlichtingen- en veiligheidsdienst brengt om de twee weken verslag uit aan de Commissie over de evolutie van de dreiging. Dit verslagbelicht de elementen die ofwel de handhaving van de algemene en ongedifferentieerde bewaring, ofwel de beëindiging ervan rechtvaardigen.

§ 11. Het diensthoofd beëindigt de vordering, niettegenstaande de bevestiging bij koninklijk besluit, wanneer de bewaring niet langer van nut is voor de bestrijding van de reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, wanneer deze dreiging is verdwenen of wanneer hij een onwettigheid vaststelt.

Wanneer de Commissie of het Vast Comité I een onwettigheid vaststelt, wordt een einde gemaakt aan de vordering niettegenstaande de bevestiging bij koninklijk besluit.

Indien voortijdig aan de vordering een einde wordt gemaakt, worden de gevorderde operatoren van elektronisch

ou les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 12. Le Roi détermine, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs et des fournisseurs.".

Art. 29

À l'article 18/7 de la même loi, les modifications suivantes sont apportées:

1° Au paragraphe 1er, les mots "Dans l'intérêt de l'exercice des missions, le dirigeant du service peut, par une décision écrite" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions";

2° Au paragraphe 1er, 2°, les mots "la communication des factures afférentes aux abonnements identifiés," sont insérés entre les mots "afin de l'obtenir" et les mots "les données relatives à la méthode de paiement";

3° Au paragraphe 3, alinéa 2, les mots "le dirigeant du service" sont remplacés par les mots "le service concerné".

Art. 30

À l'article 18/8 de la même loi, le paragraphe 2 est abrogé.

Art. 31

À l'article 18/14, § 1er, les mots "Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions,".

Art. 32

À l'article 18/17, les mots "Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent" sont remplacés par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions".

communicatienetwerken of de verstrekkers van elektronische communicatiediensten daarvan zo spoedig mogelijk op de hoogte gebracht.

§ 12. De Koning bepaalt, op voorstel van de "van Justitie, de "van Landsverdediging en de "bevoegd voor de elektronische communicatie, de nadere regels voor de samenwerking van de operatoren en de verstrekkers.".

Art. 29

In artikel 18/7 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° In paragraaf 1 worden de woorden "In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing,"vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,";

2° In paragraaf 1 worden in de bepaling onder 2° de woorden "de mededeling van de facturen met betrekking tot de geïdentificeerde abonnementen," ingevoegd tussen de woorden "tot het bekomen van" en de woorden "de gegevens betreffende de betalingswijze";

3° In paragraaf 3, tweede lid, worden de woorden "het diensthoofd" vervangen door de woorden "de betrokken dienst".

Art. 30

In artikel 18/8 van dezelfde wet wordt paragraaf 2 opgeheven.

Art. 31

In artikel 18/14, § 1 worden de woorden "In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing,"vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,".

Art. 32

In artikel 18/17, § 1, worden de woorden "In het belang van de uitvoering van hun opdrachten kunnen de", vervangen door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,".

CHAPITRE 8

Modifications à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 33

À l'article 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, rétabli par la loi du 2 mai 2007 et modifié par les lois des 25 avril 2014 et 31 juillet 2017, il est inséré un paragraphe 1erbis/1 rédigé comme suit:

"§ 1er*bis*/1. Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1er, alinéa 2, de conserver les données visées au paragraphe 1er, alinéa 1er, qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.

Les paragraphes 1er, alinéas 4 et 5, et 3 s'appliquent par analogie à l'ordre visé à l'alinéa 1er.

Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soient garanties et à ce que les données soient conservées de manière sécurisée.

L'auditeur ou, en son absence, l'auditeur adjoint demande sans délai l'autorisation préalable d'un juge d'instruction pour requérir la communication des données visées au paragraphe 1er, alinéa 1er, qui font l'objet d'un ordre de conservation visé à l'alinéa 1er et fait part de cet ordre au juge d'instruction. Si le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre de conservation ou s'il estime que cet ordre n'était pas légitime ou justifié, cet ordre devient caduc. Dans ce cas, l'auditeur ou, en son absence, l'auditeur adjoint fait sans délai savoir au destinataire de l'ordre de conservation que celui-ci est devenu caduc.".

HOOFDSTUK 8

Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 33

In artikel 84 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, hersteld bij de wet van 2 mei 2007 en gewijzigd bij de wetten van 25 april 2014 en 31 juli 2017, wordt een paragraaf 1*bis*/1 ingevoegd, luidende:

"§ 1*bis*/1. Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de in paragraaf 1, tweede lid, bedoelde actoren bevelen om de gegevens bedoeld in paragraaf 1, eerste lid, die riskeren te worden verwijderd of anoniem gemaakt, te bewaren totdat hij de toestemming van een onderzoeksrechter heeft bekomen om de mededeling van deze gegevens te vorderen.

Paragrafen 1, vierde en vijfde lid, en 3 zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.

De in paragraaf 1, tweede lid, bedoelde actoren zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, verzoekt onverwijld de voorafgaande toestemming van een onderzoeksrechter om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens die het voorwerp uitmaken van een in het eerste lid bedoeld bevel tot bewaring en bezorgt dit bevel aan de onderzoeksrechter. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel tot bewaring betrekking heeft of oordeelt dat dit bevel niet wettig of niet gerechtvaardigd was, vervalt het bevel. In dat geval brengt de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de bestemmeling van het bevel tot bewaring er onverwijld van op de hoogte dat het vervallen is.".

CHAPITRE 9

Modifications à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS")

Art. 34

L'article 62 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est remplacé par ce qui suit:

"§ 1. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 60 et 61. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.

§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, le CSIRT national peut obtenir d'un opérateur, au sens de l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques, des données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 91° de la loi du 13 juin 2005 relative aux communications électroniques conservées par celui-ci.

Les finalités poursuivies par les tâches précitées sont:

— la prévention de menaces graves contre la sécurité publique;

— l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information;

— la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave.

Lorsque le CSIRT national adresse à un opérateur une demande de données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.

HOOFDSTUK 9

Wijzigingen aan de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk-en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet")

Art. 34

Artikel 62 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt vervangen als volgt:

"§ 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, a) tot e), van deze wet, kan het nationale CSIRT gegevens over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie verkrijgen van een operator als bedoeld in artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die deze gegevens bewaart.

De doeleinden van voornoemde taken zijn:

— het voorkomen van ernstige bedreigingen voor de openbare veiligheid;

— het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen;

— het voorkomen, onderzoeken en opsporen van misdrijven die *online* of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten.

Indien het nationale CSIRT een operator een verzoek om gegevens over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hiërarchische meerdere.

Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de communications électroniques au sens de l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques autres que celles visées à l'alinéa précédent, cette demande doit faire l'objet d'un contrôle préalable par l'Autorité de protection des données créé par la loi du 3 décembre 2017.

En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visée à l'alinéa précédent et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa précédent pour permettre un contrôle ultérieur.

Le directeur du CSIRT national désigne expressément les personnes habilitées à traiter ces données de communications électroniques.

Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées.

§ 3. Pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

§ 4. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.".

Art. 35

Dans l'article 65, § 2, de la même loi, les mots "des données de communications électroniques," sont insérés entre les mots "des données ou des identifiants de connexion," et "des données de géolocalisation".

Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegevens als bedoeld in artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie die geen in het vorige lid bedoelde gegevens zijn, stuurt, moet dat verzoek vooraf worden gecontroleerd door de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017.

In dringende en naar behoren gemotiveerde gevallen kan het nationale CSIRT optreden zonder de voorafgaande controle bedoeld in het vorige lid, en de gegevens rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het vorige lid bedoelde overheid gestuurd om een latere controle mogelijk te maken.

De directeur van het nationale CSIRT wijst uitdrukkelijk de personen aan die gemachtigd zijn om deze elektronische-communicatiegegevens te verwerken.

Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd.

§ 3. Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

§ 4. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.".

Art. 35

In artikel 65, § 2, van dezelfde wet worden de woorden "elektronische communicatiegegevens," ingevoegd tussen de woorden "verbindingsgegevens of -identificatoren," en de woorden "locatie-gegevens".

CHAPITRE 10

Modification à la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits

Art. 36

L'article 11, § 1er, de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits, remplacé par la loi du 10 avril 2014, est complété par un alinéa rédigé comme suit:

"Ils peuvent identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique.

À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification à:

1° l'opérateur d'un réseau de communications électroniques; et

2° toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Sans préjudice d'une éventuelle délégation, chaque demande d'identification doit être approuvée au préalable, par écrit, par le chef du service Inspection produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement.".

CHAPITRE 11

Dispositions transitoires

Art. 37

La conservation ciblée des données sur la base des critères énoncés à l'article 126/1, § 3, alinéa 1er, 3° à 5° de la loi du 13 juin 2005 relative aux communications électroniques, entre en vigueur à la date fixée par le Roi par arrêté délibéré en Conseil des ministres, et au plus tard le 1er janvier 2027.

HOOFDSTUK 10

Wijziging aan de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten

Art. 36

Artikel 11, § 1, van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedings-middelen en andere producten, vervangen bij de wet van 10 april 2014, wordt aangevuld met een lid, luidende:

"Zij mogen natuurlijke en rechtspersonen identificeren aan de hand van het telefoonnummer van de betrokkene of het IP-adres dat aan de bron van de elektronische communicatie ligt.

Hiertoe mogen zij met gemotiveerd verzoek de verstrekking van de identificatiedocumenten en gegevens vorderen van:

1° de operator van een elektronisch communicatienetwerk; en

2° iedereen die binnen het Belgisch grondgebied, op welke wijze ook een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

Onverminderd een eventuele delegatie, dient elk identificatieverzoek voorafgaand, door het diensthoofd van de Inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden.".

HOOFDSTUK 11

Overgangsbepalingen

Art. 37

De gerichte gegevensbewaring op basis van de criteria voorzien in artikel 126/1, § 3, eerste lid, 3° tot 5° van de wet van 13 juni 2005 betreffende de elektronische communicatie treedt in werking op de door de Koning bij een in "raad overlegd besluit bepaalde datum en uiterlijk op 1 januari 2027.

Pour la première application de l'article 126/1, § 3, alinéa 1er, 3° à 5° de la loi du 13 juin 2005 relative aux communications électroniques, les autorités compétentes visées à l'article 126/1, § 3, alinéa 3 de la même loi, transmettent les informations nécessaires au service désigné par le Roi à une date fixée par l'arrêté royal visé à l'alinéa 1er et au plus tard le 1er janvier 2026.

Art. 38

Les ministres de la Justice et de l'Intérieur déterminent la durée de conservation des données visées à l'article 126/1, § 2 de la loi du 13 juin 2005 relative aux communications électroniques, par arrondissement judiciaire et par zone de police, et sur la base des critères visés à l'article 126/1, § 3, alinéa 1er, 1°, de la même loi, qui s'appliquent à partir de l'entrée en vigueur de la présente loi jusqu'à la publication de l'arrêté ministériel visé à l'article 126/1, § 3, alinéa 1er, 1° de la même loi.

Donné à Bruxelles, le 16 mars 2022

PHILIPPE

Par le Roi:

Le ministre de la Justice,

Vincent VAN QUICKENBORNE

Bij de eerste toepassing van het artikel 126/1, § 3, eerste lid, 3° tot 5° van de wet van 13 juni 2005 betreffende de elektronische communicatie, delen de in artikel 126/1, § 3, derde lid van dezelfde wet bedoelde bevoegde autoriteiten de nodige informatie naar de door de Koning aangewezen dienst op een datum die vastgesteld wordt bij het in het eerste lid bedoelde koninklijk besluit en uiterlijk op 1 januari 2026.

Art. 38

De ministers van Justitie en van Binnenlandse Zaken bepalen de bewaartermijn van de gegevens bedoeld in artikel 126/1, § 2, van de wet van 13 juni 2005 betreffende de elektronische communicatie, per gerechtelijke arrondissement en per politiezone, en op basis van de criteria bedoeld in artikel 126/1, § 3, eerste lid, 1° van dezelfde wet, die zal gelden vanaf de inwerkingtreding van de huidige wet tot de publicatie van het ministerieel besluit bedoeld in artikel 126/1, § 3, eerste lid, 1° van dezelfde wet.

Gegeven te Brussel, 16 maart 2022

FILIP

Van Koningswege:

De minister van Justitie,

Vincent VAN QUICKENBORNE

COORDINATION DES ARTICLES	
TEXTE DE BASE	**TEXTE ADAPTÉ AU PROJET DE LOI**
CHAPITRE 2 – Modifications à la loi du 13 juin 2005 relative aux communications électroniques	
TITRE Ier. - Définitions et principes généraux.	TITRE Ier. - Définitions et principes généraux.
CHAPITRE Ier. - Généralités.	CHAPITRE Ier. - Généralités.
Art. 2	**Art. 2**
Pour l'application de la présente loi, il faut entendre par :	Pour l'application de la présente loi, il faut entendre par :
1° "Institut" : l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;	1° "Institut" : l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;
2° "ministre" : les ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi;	2° "ministre" : les ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi;
3° “réseau de communications électroniques”: les systèmes de transmission, qu’ils soient ou non fondés sur une infrastructure permanente ou une capacité d’administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l’acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d’autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l’internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de services de médias audiovisuels ou sonores;	3° “réseau de communications électroniques”: les systèmes de transmission, qu’ils soient ou non fondés sur une infrastructure permanente ou une capacité d’administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l’acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d’autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l’internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de services de médias audiovisuels ou sonores;
3/1° “réseau à très haute capacité”: soit un réseau de communications électroniques qui est entièrement composé d’éléments de fibre optique au moins jusqu’au point de distribution	3/1° “réseau à très haute capacité”: soit un réseau de communications électroniques qui est entièrement composé d’éléments de fibre optique au moins jusqu’au point de distribution

au lieu de desserte, soit un réseau de communications électroniques qui est capable d'offrir, dans des conditions d'heures de pointe habituelles, une performance du réseau comparable en termes de débit descendant et ascendant, de résilience, de paramètres liés aux erreurs, de latence et de gigue; la performance du réseau peut être jugée comparable indépendamment des variations de l'expérience de l'utilisateur final qui sont dues aux caractéristiques intrinsèquement différentes du support par lequel se fait la connexion ultime du réseau au point de terminaison du réseau ;	au lieu de desserte, soit un réseau de communications électroniques qui est capable d'offrir, dans des conditions d'heures de pointe habituelles, une performance du réseau comparable en termes de débit descendant et ascendant, de résilience, de paramètres liés aux erreurs, de latence et de gigue; la performance du réseau peut être jugée comparable indépendamment des variations de l'expérience de l'utilisateur final qui sont dues aux caractéristiques intrinsèquement différentes du support par lequel se fait la connexion ultime du réseau au point de terminaison du réseau ;
4° " fourniture d'un réseau de communications électroniques " : la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques;	4° " fourniture d'un réseau de communications électroniques " : la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques;
5° "service de communications électroniques": le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus et à l'exception des services de médias audiovisuels ou sonores, comprend les types de services suivants:	5° "service de communications électroniques": le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus et à l'exception des services de médias audiovisuels ou sonores, comprend les types de services suivants:
a) un service d'accès à l'internet;	a) un service d'accès à l'internet;
b) un service de communications interpersonnelles; et	b) un service de communications interpersonnelles; et
c) des services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine;	c) des services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine;
5/1° "service d'accès à l'internet": un service de communications électroniques accessibles au public, qui fournit un accès à l'internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés;	5/1° "service d'accès à l'internet": un service de communications électroniques accessibles au public, qui fournit un accès à l'internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'internet, quels que soient la technologie de réseau ou les équipements terminaux utilisés;
5/2° "service de communications interpersonnelles": un service normalement	5/2° "service de communications interpersonnelles": un service normalement

fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service;	fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service;
5/3° "service de communications interpersonnelles fondé sur la numérotation": un service de communications interpersonnelles qui établit une connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation ou qui permet la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;	5/3° "service de communications interpersonnelles fondé sur la numérotation": un service de communications interpersonnelles qui établit une connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation ou qui permet la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;
5/4° "service de communications interpersonnelles non fondé sur la numérotation": un service de communications interpersonnelles qui n'établit pas de connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;	5/4° "service de communications interpersonnelles non fondé sur la numérotation": un service de communications interpersonnelles qui n'établit pas de connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation;
	5/5°: « une fraude » : un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques ;
	5/6° : « utilisation malveillante du réseau ou du service » : utilisation du réseau ou service de communication électronique afin d'importuner son correspondant ou de provoquer des dommages ;

6° " donnée de trafic " : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication;	6° " donnée de trafic " : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication;
7° "informations relatives à la localisation de l'appelant": dans un réseau mobile public, les données traitées qui proviennent de l'infrastructure de réseau ou de l'appareil mobile et qui indiquent la position géographique de l'équipement terminal mobile d'un utilisateur final et, dans un réseau fixe public, les données relatives à l'adresse physique du point de terminaison du réseau ;	7° "informations relatives à la localisation de l'appelant": dans un réseau mobile public, les données traitées qui proviennent de l'infrastructure de réseau ou de l'appareil mobile et qui indiquent la position géographique de l'équipement terminal mobile d'un utilisateur final et, dans un réseau fixe public, les données relatives à l'adresse physique du point de terminaison du réseau ;
8° " service à données de trafic " : un service qui exige un traitement particulier des données de trafic allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication ;	8° " service à données de trafic " : un service qui exige un traitement particulier des données de trafic allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication ;
9° " service à données de localisation " : un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;	9° " service à données de localisation " : un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication;
10° " réseau public de communications électroniques " : un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de [...] services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau;	10° " réseau public de communications électroniques " : un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de [...] services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau;
10/1° " réseau de communications électroniques à haut débit " : un réseau de communications électroniques pouvant fournir des services d'accès au haut débit à une vitesse supérieure ou égale à 30 Mbit/s;	10/1° " réseau de communications électroniques à haut débit " : un réseau de communications électroniques pouvant fournir des services d'accès au haut débit à une vitesse supérieure ou égale à 30 Mbit/s;
11° "opérateur": une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public;	11° "opérateur": une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public;
11/1° "gestionnaire d'infrastructures passives" : un acteur économique qui, d'une part, fournit	11/1° "gestionnaire d'infrastructures passives" : un acteur économique qui, d'une part, fournit

un service de production, de transport ou de distribution de gaz; d'électricité (y compris pour l'éclairage public) ou d'eau (y compris l'évacuation ou le traitement et l'assainissement des eaux usées, et les systèmes d'égouts); un service de chauffage; ou des services de transport (y compris les voies ferrées, les routes, les ports et les aéroports), et qui, d'autre part, met à disposition des éléments de son réseau sans que ceux-ci deviennent eux-mêmes un élément actif d'un réseau de communications électroniques ;	un service de production, de transport ou de distribution de gaz; d'électricité (y compris pour l'éclairage public) ou d'eau (y compris l'évacuation ou le traitement et l'assainissement des eaux usées, et les systèmes d'égouts); un service de chauffage; ou des services de transport (y compris les voies ferrées, les routes, les ports et les aéroports), et qui, d'autre part, met à disposition des éléments de son réseau sans que ceux-ci deviennent eux-mêmes un élément actif d'un réseau de communications électroniques ;
11/2° "autorisation générale": un cadre juridique mis en place, qui garantit le droit de fournir des réseaux ou des services de communications électroniques et qui fixe les obligations propres au secteur pouvant s'appliquer à tous les types de réseaux et de services de communications électroniques ou à certains d'entre eux;	11/2° "autorisation générale": un cadre juridique mis en place, qui garantit le droit de fournir des réseaux ou des services de communications électroniques et qui fixe les obligations propres au secteur pouvant s'appliquer à tous les types de réseaux et de services de communications électroniques ou à certains d'entre eux;
12° " utilisateur " : une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public;	12° " utilisateur " : une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public;
13° " utilisateur final " : un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public;	13° " utilisateur final " : un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public;
14° " consommateur " : toute personne physique qui utilise ou demande un service de communications électroniques accessible au public à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ;	14° " consommateur " : toute personne physique qui utilise ou demande un service de communications électroniques accessible au public à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ;
14/1° "microentreprise": entreprise ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;	14/1° "microentreprise": entreprise ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;
14/2° "petite entreprise": entreprise ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;	14/2° "petite entreprise": entreprise ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l'article 1:24 du Code des sociétés et associations;

14/3° “moyenne entreprise”: entreprise ne dépassant pas la moyenne annuelle de 249 travailleurs mis au travail, calculée conformément à l’article 1:24 du Code des sociétés et associations;	14/3° “moyenne entreprise”: entreprise ne dépassant pas la moyenne annuelle de 249 travailleurs mis au travail, calculée conformément à l’article 1:24 du Code des sociétés et associations;
14/4° “micro-organisation à but non lucratif”: association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l’article 1:28 du Code des sociétés et associations;	14/4° “micro-organisation à but non lucratif”: association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail, calculée conformément à l’article 1:28 du Code des sociétés et associations;
14/5° “petite organisation à but non lucratif”: association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l’article 1:28 du Code des sociétés et associations;	14/5° “petite organisation à but non lucratif”: association sans but lucratif, association internationale sans but lucratif ou fondation ne dépassant pas la moyenne annuelle de 49 travailleurs mis au travail, calculée conformément à l’article 1:28 du Code des sociétés et associations;
15° " abonné " : toute personne physique ou morale, autre qu’un opérateur, partie à un contrat avec un opérateur qui fournit des services de communications électroniques accessibles au public, pour la fourniture de tels services;	15° " abonné " : toute personne physique ou morale, autre qu’un opérateur, partie à un contrat avec un opérateur qui fournit des services de communications électroniques accessibles au public, pour la fourniture de tels services;
15/1° “abonné comptant un maximum de 9 travailleurs”: abonné ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail calculée, selon le cas, conformément aux articles 1:24 ou 1:28 du Code des sociétés et associations;	15/1° “abonné comptant un maximum de 9 travailleurs”: abonné ne dépassant pas la moyenne annuelle de 9 travailleurs mis au travail calculée, selon le cas, conformément aux articles 1:24 ou 1:28 du Code des sociétés et associations;
16° “point de terminaison du réseau”: point physique auquel un utilisateur final obtient l’accès à un réseau public de communications électroniques; dans le cas de réseaux utilisant la commutation et l’acheminement, le point de terminaison du réseau est identifié par une adresse réseau spécifique qui peut être rattachée au numéro ou au nom d’un utilisateur final;	16° “point de terminaison du réseau”: point physique auquel un utilisateur final obtient l’accès à un réseau public de communications électroniques; dans le cas de réseaux utilisant la commutation et l’acheminement, le point de terminaison du réseau est identifié par une adresse réseau spécifique qui peut être rattachée au numéro ou au nom d’un utilisateur final;
16/1° " point d'accès " : un point physique, situé à l'intérieur ou à l'extérieur de l'immeuble, accessible aux opérateurs, qui permet le raccordement à l'infrastructure physique	16/1° " point d'accès " : un point physique, situé à l'intérieur ou à l'extérieur de l'immeuble, accessible aux opérateurs, qui permet le raccordement à l'infrastructure physique

adaptée au haut débit à l'intérieur de l'immeuble ;	adaptée au haut débit à l'intérieur de l'immeuble ;
17° “ressources associées”: les services associés, les infrastructures physiques et autres ressources ou éléments associés à un réseau de communications électroniques ou à un service de communications électroniques, qui permettent ou soutiennent la fourniture de services via ce réseau ou ce service ou en ont le potentiel, et comprennent, entre autres, les bâtiments ou accès aux bâtiments, le câblage des bâtiments, les antennes, tours et autres constructions de soutènement, les gaines, conduites, pylônes, regards de visite et armoires;	17° “ressources associées”: les services associés, les infrastructures physiques et autres ressources ou éléments associés à un réseau de communications électroniques ou à un service de communications électroniques, qui permettent ou soutiennent la fourniture de services via ce réseau ou ce service ou en ont le potentiel, et comprennent, entre autres, les bâtiments ou accès aux bâtiments, le câblage des bâtiments, les antennes, tours et autres constructions de soutènement, les gaines, conduites, pylônes, regards de visite et armoires;
17/1° “service associé”: un service associé à un réseau de communications électroniques ou à un service de communications électroniques, qui permet ou soutient la fourniture, l’autofourniture ou la fourniture automatisée de services via ce réseau ou ce service ou en a le potentiel, et comprend notamment la conversion du numéro d’appel ou des systèmes offrant des fonctionnalités équivalentes et les systèmes d’accès conditionnel et les guides électroniques de programmes, en abrégé “EPG”, ainsi que d’autres services tels que ceux relatifs à l’identité, l’emplacement et l’occupation (à l’exception des services et systèmes qui sont exclusivement utilisés pour les services de médias audiovisuels ou sonores);	17/1° “service associé”: un service associé à un réseau de communications électroniques ou à un service de communications électroniques, qui permet ou soutient la fourniture, l’autofourniture ou la fourniture automatisée de services via ce réseau ou ce service ou en a le potentiel, et comprend notamment la conversion du numéro d’appel ou des systèmes offrant des fonctionnalités équivalentes et les systèmes d’accès conditionnel et les guides électroniques de programmes, en abrégé “EPG”, ainsi que d’autres services tels que ceux relatifs à l’identité, l’emplacement et l’occupation (à l’exception des services et systèmes qui sont exclusivement utilisés pour les services de médias audiovisuels ou sonores);
17/2° " infrastructure physique située à l'intérieur d'un immeuble " : tout élément d'un réseau, tels que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours et poteaux (hormis les câbles, y compris la fibre noire) ainsi que les installations situés au niveau des locaux de l'utilisateur final, y compris dans les éléments en copropriété, qui sont destinés à accueillir des éléments de réseaux d'accès filaires ou sans fil sans devenir eux-mêmes un élément actif du réseau, lorsque ces réseaux permettent de fournir des services de communications électroniques et de raccorder le point d'accès de l'immeuble au point de terminaison du réseau;	17/2° " infrastructure physique située à l'intérieur d'un immeuble " : tout élément d'un réseau, tels que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours et poteaux (hormis les câbles, y compris la fibre noire) ainsi que les installations situés au niveau des locaux de l'utilisateur final, y compris dans les éléments en copropriété, qui sont destinés à accueillir des éléments de réseaux d'accès filaires ou sans fil sans devenir eux-mêmes un élément actif du réseau, lorsque ces réseaux permettent de fournir des services de communications électroniques et de raccorder le point d'accès de l'immeuble au point de terminaison du réseau;

17/3° "nomadicité": caractéristique d'un service de communications électroniques qui permet à ce service d'être utilisé à partir de pratiquement n'importe quelle connexion à un réseau de communications électroniques;	17/3° "nomadicité": caractéristique d'un service de communications électroniques qui permet à ce service d'être utilisé à partir de pratiquement n'importe quelle connexion à un réseau de communications électroniques;
18° " accès " : la mise à la disposition d'un opérateur, dans des conditions bien définies et de manière exclusive ou non exclusive, de ressources et/ou de services en vue de la fourniture de services de communications électroniques, ou l'offre de services de la société de l'information. Cela couvre notamment : l'accès à des éléments de réseaux et à des ressources associées ce qui peut comprendre la connexion des équipements par des moyens fixes ou non (cela comprend en particulier l'accès à la boucle locale ainsi qu'aux ressources et services nécessaires à la fourniture de services par la boucle locale); l'accès à l'infrastructure physique, y compris aux bâtiments, gaines et pylônes; l'accès aux systèmes logiciels pertinents, y compris aux systèmes d'assistance à l'exploitation; l'accès aux systèmes d'information ou aux bases de données pour la préparation de commandes, l'approvisionnement, la commande, les demandes de maintenance et de réparation et la facturation; l'accès à la conversion du numéro d'appel ou à des systèmes offrant des fonctionnalités équivalentes; l'accès aux réseaux fixes et mobiles, notamment pour l'itinérance; l'accès aux services de réseaux virtuels;	18° " accès " : la mise à la disposition d'un opérateur, dans des conditions bien définies et de manière exclusive ou non exclusive, de ressources et/ou de services en vue de la fourniture de services de communications électroniques, ou l'offre de services de la société de l'information. Cela couvre notamment : l'accès à des éléments de réseaux et à des ressources associées ce qui peut comprendre la connexion des équipements par des moyens fixes ou non (cela comprend en particulier l'accès à la boucle locale ainsi qu'aux ressources et services nécessaires à la fourniture de services par la boucle locale); l'accès à l'infrastructure physique, y compris aux bâtiments, gaines et pylônes; l'accès aux systèmes logiciels pertinents, y compris aux systèmes d'assistance à l'exploitation; l'accès aux systèmes d'information ou aux bases de données pour la préparation de commandes, l'approvisionnement, la commande, les demandes de maintenance et de réparation et la facturation; l'accès à la conversion du numéro d'appel ou à des systèmes offrant des fonctionnalités équivalentes; l'accès aux réseaux fixes et mobiles, notamment pour l'itinérance; l'accès aux services de réseaux virtuels;
19° "interconnexion": un type particulier d'accès mis en oeuvre entre opérateurs de réseaux publics au moyen de la liaison physique et logique des réseaux publics de communications électroniques utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre entreprise, ou d'accéder aux services fournis par une autre entreprise lorsque ces services sont fournis par les parties concernées ou par d'autres parties qui ont accès au réseau;	19° "interconnexion": un type particulier d'accès mis en oeuvre entre opérateurs de réseaux publics au moyen de la liaison physique et logique des réseaux publics de communications électroniques utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre entreprise, ou d'accéder aux services fournis par une autre entreprise lorsque ces services sont fournis par les parties concernées ou par d'autres parties qui ont accès au réseau;

20° " interface " : un point de terminaison du réseau et/ou une interface radio, et les spécifications techniques y afférentes;	20° " interface " : un point de terminaison du réseau et/ou une interface radio, et les spécifications techniques y afférentes;
21° [...];	21° [...];
22° “service de communications vocales”: un service de communications électroniques accessible au public permettant d’émettre et de recevoir, directement ou indirectement, des appels nationaux ou nationaux et internationaux, en composant un ou plusieurs numéros d’un plan national ou international de numérotation;	22° “service de communications vocales”: un service de communications électroniques accessible au public permettant d’émettre et de recevoir, directement ou indirectement, des appels nationaux ou nationaux et internationaux, en composant un ou plusieurs numéros d’un plan national ou international de numérotation;
22/1° " appel " : une connexion établie au moyen d'un service de communications interpersonnelles accessible au public permettant une communication vocale bidirectionnelle;	22/1° " appel " : une connexion établie au moyen d'un service de communications interpersonnelles accessible au public permettant une communication vocale bidirectionnelle;
22/2° “service de conversation totale”: un service multimédia de conversation en temps réel assurant la transmission symétrique et bidirectionnelle en temps réel de vidéos animées, de texte en temps réel et de voix entre des utilisateurs situés dans deux lieux différents ou plus;	22/2° “service de conversation totale”: un service multimédia de conversation en temps réel assurant la transmission symétrique et bidirectionnelle en temps réel de vidéos animées, de texte en temps réel et de voix entre des utilisateurs situés dans deux lieux différents ou plus;
23° " boucle locale " : un canal physique utilisé par les signaux de communications électroniques et relie le point de terminaison du réseau à un répartiteur ou à toute autre installation équivalente du réseau public fixe de communications électroniques;	23° " boucle locale " : un canal physique utilisé par les signaux de communications électroniques et relie le point de terminaison du réseau à un répartiteur ou à toute autre installation équivalente du réseau public fixe de communications électroniques;
24° " sous-boucle locale " : partie d'une boucle locale qui relie le point de terminaison du réseau à un point de concentration ou à un point d'accès intermédiaire spécifié du réseau de communications électroniques public fixe;	24° " sous-boucle locale " : partie d'une boucle locale qui relie le point de terminaison du réseau à un point de concentration ou à un point d'accès intermédiaire spécifié du réseau de communications électroniques public fixe;
25° " accès totalement dégroupé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d’une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage de la pleine capacité des infrastructures des réseaux];	25° " accès totalement dégroupé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d’une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage de la pleine capacité des infrastructures des réseaux];

26° " accès à un débit binaire " : accès consistant en la fourniture d'une capacité de transport avec la commutation associée vers un utilisateur pour lequel l'interface chez l'utilisateur est définie par le fournisseur d'accès;	26° " accès à un débit binaire " : accès consistant en la fourniture d'une capacité de transport avec la commutation associée vers un utilisateur pour lequel l'interface chez l'utilisateur est définie par le fournisseur d'accès;
27° " accès partagé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d'une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage d'une partie spécifiée de la capacité des infrastructures des réseaux telle qu'une partie de la fréquence ou l'équivalent;	27° " accès partagé à la boucle locale " : la fourniture d'un accès à la boucle locale ou à la sous-boucle locale d'une entreprise désignée comme étant puissante sur un marché pertinent, autorisant l'usage d'une partie spécifiée de la capacité des infrastructures des réseaux telle qu'une partie de la fréquence ou l'équivalent;
28° " accès dégroupé à la boucle locale " : la fourniture d'un accès totalement dégroupé ou d'un accès partagé à la boucle locale n'impliquant pas de changement en ce qui concerne la propriété de la boucle locale;	28° " accès dégroupé à la boucle locale " : la fourniture d'un accès totalement dégroupé ou d'un accès partagé à la boucle locale n'impliquant pas de changement en ce qui concerne la propriété de la boucle locale;
29° " colocalisation " : la fourniture d'un espace et des ressources techniques nécessaires à l'hébergement et à la connexion, dans des conditions raisonnables, des équipements pertinents d'un opérateur dans le cadre d'une offre de référence;	29° " colocalisation " : la fourniture d'un espace et des ressources techniques nécessaires à l'hébergement et à la connexion, dans des conditions raisonnables, des équipements pertinents d'un opérateur dans le cadre d'une offre de référence;
29/1° " gaine " : enveloppe servant à faire passer et protéger des câbles optiques, téléphoniques et/ou coaxiaux, et/ou ressources de réseau;	29/1° " gaine " : enveloppe servant à faire passer et protéger des câbles optiques, téléphoniques et/ou coaxiaux, et/ou ressources de réseau;
30° " ligne louée " : service de communications électroniques consistant en la fourniture d'un système de communications offrant une capacité de transmission transparente entre les points de terminaison de réseaux, à l'exclusion de la commutation sur demande;	30° " ligne louée " : service de communications électroniques consistant en la fourniture d'un système de communications offrant une capacité de transmission transparente entre les points de terminaison de réseaux, à l'exclusion de la commutation sur demande;
31° " ondes radioélectriques " : les ondes électromagnétiques se propageant dans l'espace sans guide artificiel, et dont la fréquence est inférieure à 3000 GHz;	31° " ondes radioélectriques " : les ondes électromagnétiques se propageant dans l'espace sans guide artificiel, et dont la fréquence est inférieure à 3000 GHz;
32° (abrogé)	32° (abrogé)
33° " spectre radioélectrique " : l'ensemble des ondes radioélectriques;	33° " spectre radioélectrique " : l'ensemble des ondes radioélectriques;
33/1° "attribution du spectre radioélectrique": la désignation d'une bande du spectre	33/1° "attribution du spectre radioélectrique": la désignation d'une bande du spectre

radioélectrique donnée, aux fins de son utilisation par un ou plusieurs types de services de radiocommunications, le cas échéant, selon des conditions définies;	radioélectrique donnée, aux fins de son utilisation par un ou plusieurs types de services de radiocommunications, le cas échéant, selon des conditions définies;
33/2° "plan national d'attribution des fréquences": document contenant pour chaque bande du spectre radioélectrique, les informations relatives aux attributions du spectre radioélectrique et aux applications autorisées;	33/2° "plan national d'attribution des fréquences": document contenant pour chaque bande du spectre radioélectrique, les informations relatives aux attributions du spectre radioélectrique et aux applications autorisées;
33/3° "spectre radioélectrique harmonisé": spectre radioélectrique dont les conditions harmonisées quant à sa disponibilité et son utilisation efficace ont été établies par la voie de mesures techniques d'application conformément à l'article 4 de la décision no 676/2002/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire pour la politique en matière de spectre radioélectrique dans la Communauté européenne, ci-après dénommée "décision spectre radioélectrique";	33/3° "spectre radioélectrique harmonisé": spectre radioélectrique dont les conditions harmonisées quant à sa disponibilité et son utilisation efficace ont été établies par la voie de mesures techniques d'application conformément à l'article 4 de la décision no 676/2002/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire pour la politique en matière de spectre radioélectrique dans la Communauté européenne, ci-après dénommée "décision spectre radioélectrique";
33/4° "utilisation partagée du spectre radioélectrique": l'accès par deux utilisateurs ou plus, en vue de leur utilisation, aux mêmes bandes du spectre radioélectrique dans le cadre d'un dispositif de partage défini, autorisé sur le fondement d'une autorisation générale, de droits d'utilisation du spectre radioélectrique ou d'une combinaison de ceux-ci, y compris des mécanismes de régulation tels que l'accès partagé sous licence destiné à faciliter l'utilisation partagée d'une bande du spectre radioélectrique, sous réserve d'un accord contraignant entre toutes les parties concernées, conformément aux règles de partage incluses dans leurs droits d'utilisation du spectre radioélectrique, afin de garantir à tous les utilisateurs des dispositifs de partage prévisibles et fiables, et sans préjudice de l'application du droit de la concurrence;	33/4° "utilisation partagée du spectre radioélectrique": l'accès par deux utilisateurs ou plus, en vue de leur utilisation, aux mêmes bandes du spectre radioélectrique dans le cadre d'un dispositif de partage défini, autorisé sur le fondement d'une autorisation générale, de droits d'utilisation du spectre radioélectrique ou d'une combinaison de ceux-ci, y compris des mécanismes de régulation tels que l'accès partagé sous licence destiné à faciliter l'utilisation partagée d'une bande du spectre radioélectrique, sous réserve d'un accord contraignant entre toutes les parties concernées, conformément aux règles de partage incluses dans leurs droits d'utilisation du spectre radioélectrique, afin de garantir à tous les utilisateurs des dispositifs de partage prévisibles et fiables, et sans préjudice de l'application du droit de la concurrence;
33/5° "droits d'utilisation du spectre radioélectrique": droits individuels d'utilisation du spectre radioélectrique utilisés entièrement ou partiellement pour la fourniture de réseaux publics de communications électroniques ou de	33/5° "droits d'utilisation du spectre radioélectrique": droits individuels d'utilisation du spectre radioélectrique utilisés entièrement ou partiellement pour la fourniture de réseaux publics de communications électroniques ou de

services de communications électroniques accessibles au public;	services de communications électroniques accessibles au public;
34° “radiocommunication”: toute communication au moyen d’ondes radioélectriques à l’exclusion de la transmission exclusive de signaux de services de médias audiovisuels et sonores ;	34° “radiocommunication”: toute communication au moyen d’ondes radioélectriques à l’exclusion de la transmission exclusive de signaux de services de médias audiovisuels et sonores ;
35° (abrogé)	35° (abrogé)
36° (abrogé)	36° (abrogé)
37° (abrogé)	37° (abrogé)
38° “station de radiocommunications”: un équipement hertzien, le cas échéant complété des antennes, ainsi que de tous les composants nécessaires au fonctionnement de l’ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication et/ou de radiorepérage;	38° “station de radiocommunications”: un équipement hertzien, le cas échéant complété des antennes, ainsi que de tous les composants nécessaires au fonctionnement de l’ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication et/ou de radiorepérage;
38/1° “réseau de radiocommunications”: ensemble formé par plusieurs stations de radiocommunications pouvant communiquer entre elles dans les limites d’une autorisation de radiocommunications privées ou d’un droit d’utilisation du spectre radioélectrique;	38/1° “réseau de radiocommunications”: ensemble formé par plusieurs stations de radiocommunications pouvant communiquer entre elles dans les limites d’une autorisation de radiocommunications privées ou d’un droit d’utilisation du spectre radioélectrique;
38/2° “autorisation de radiocommunications privées”: autorisation de pouvoir utiliser une station ou un réseau de radiocommunications à d’autres fins que la fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;	38/2° “autorisation de radiocommunications privées”: autorisation de pouvoir utiliser une station ou un réseau de radiocommunications à d’autres fins que la fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;
38/3° “station de radiodiffusion”: un équipement hertzien, le cas échéant complété des antennes associées, ainsi que de tous les composants nécessaires au fonctionnement de l’ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de fourniture de services de médias audiovisuels et sonores;	38/3° “station de radiodiffusion”: un équipement hertzien, le cas échéant complété des antennes associées, ainsi que de tous les composants nécessaires au fonctionnement de l’ensemble, qui émet ou reçoit intentionnellement des ondes radioélectriques à des fins de fourniture de services de médias audiovisuels et sonores;
38/4° “brouillage”: effet, sur la réception dans un système de radiocommunication, d’une énergie non désirée due à une émission, à un rayonnement ou à une induction (ou à une	38/4° “brouillage”: effet, sur la réception dans un système de radiocommunication, d’une énergie non désirée due à une émission, à un rayonnement ou à une induction (ou à une

combinaison de ces émissions, rayonnements ou inductions), se manifestant par une dégradation de la qualité de transmission, une déformation ou une perte de l'information que l'on aurait pu extraire en l'absence de cette énergie non désirée;	combinaison de ces émissions, rayonnements ou inductions), se manifestant par une dégradation de la qualité de transmission, une déformation ou une perte de l'information que l'on aurait pu extraire en l'absence de cette énergie non désirée;
39° " brouillage préjudiciable " : le brouillage qui compromet le fonctionnement d'un service de radionavigation ou d'autres services de sécurité ou qui altère gravement, entrave ou interrompt de façon répétée le fonctionnement d'un service de radiocommunications d'un service de fourniture de services de médias audiovisuels et sonores ou d'un service de communications électroniques opérant conformément à la réglementation applicable;	39° " brouillage préjudiciable " : le brouillage qui compromet le fonctionnement d'un service de radionavigation ou d'autres services de sécurité ou qui altère gravement, entrave ou interrompt de façon répétée le fonctionnement d'un service de radiocommunications d'un service de fourniture de services de médias audiovisuels et sonores ou d'un service de communications électroniques opérant conformément à la réglementation applicable;
40° " cryptographie " : l'ensemble des services mettant en oeuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée;	40° " cryptographie " : l'ensemble des services mettant en oeuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée;
41° "équipement terminal":	41° "équipement terminal":
a) tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de communications électroniques pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public;	a) tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de communications électroniques pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public;
b) les équipements de stations terrestres de satellites;	b) les équipements de stations terrestres de satellites;
42° "équipement hertzien" : un produit électrique ou électronique qui émet et/ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication, de fourniture de services de médias audiovisuels et sonores et/ou radiorepérage, ou un produit électrique ou électronique qui doit être complété d'un accessoire, tel qu'une antenne, pour émettre	42° "équipement hertzien" : un produit électrique ou électronique qui émet et/ou reçoit intentionnellement des ondes radioélectriques à des fins de radiocommunication, de fourniture de services de médias audiovisuels et sonores et/ou radiorepérage, ou un produit électrique ou électronique qui doit être complété d'un accessoire, tel qu'une antenne, pour émettre

et/ou recevoir intentionnellement des ondes radioélectriques à des fins de radiocommunication, de fourniture de services de médias audiovisuels et sonores et/ou de radiorepérage ;	et/ou recevoir intentionnellement des ondes radioélectriques à des fins de radiocommunication, de fourniture de services de médias audiovisuels et sonores et/ou de radiorepérage ;
43° " équipement " : tout produit qui est soit un équipement hertzien, soit un équipement terminal, soit les deux;	43° " équipement " : tout produit qui est soit un équipement hertzien, soit un équipement terminal, soit les deux;
44° " spécification technique " : la définition des caractéristiques de tous les services de communications électroniques fournis via le point de terminaison du réseau ou l'interface radio;	44° " spécification technique " : la définition des caractéristiques de tous les services de communications électroniques fournis via le point de terminaison du réseau ou l'interface radio;
45° " espace de numérotation " : l'ensemble des numéros, adresses et noms utilisés en vue d'identifier des opérateurs ou des utilisateurs;	45° " espace de numérotation " : l'ensemble des numéros, adresses et noms utilisés en vue d'identifier des opérateurs ou des utilisateurs;
46° " numéro géographique " : numéro du plan national de numérotation dont une partie de la structure numérique contient une signification géographique utilisée pour acheminer les appels vers le lieu physique du point de terminaison du réseau;	46° " numéro géographique " : numéro du plan national de numérotation dont une partie de la structure numérique contient une signification géographique utilisée pour acheminer les appels vers le lieu physique du point de terminaison du réseau;
47° " numéro non géographique " : numéro du plan national de numérotation qui n'est pas un numéro géographique; il s'agit entre autres des numéros d'appel mobiles, des numéros d'appel gratuits pour les appelants et des numéros à taux majoré;	47° " numéro non géographique " : numéro du plan national de numérotation qui n'est pas un numéro géographique; il s'agit entre autres des numéros d'appel mobiles, des numéros d'appel gratuits pour les appelants et des numéros à taux majoré;
48° " portabilité des numéros " : facilité permettant aux abonnés [...] de conserver leur numéro, quel que soit l'opérateur fournissant le service, dans une zone géographique déterminée dans le cas d'un numéro géographique et quel que soit l'endroit, dans le cas de numéros autres que géographiques; la facilité ne permet pas de conserver le numéro de téléphone national entre un opérateur de services téléphoniques accessibles au public en position déterminée et un opérateur de services téléphoniques accessibles au public sur un réseau de communications électroniques mobile;	48° " portabilité des numéros " : facilité permettant aux abonnés [...] de conserver leur numéro, quel que soit l'opérateur fournissant le service, dans une zone géographique déterminée dans le cas d'un numéro géographique et quel que soit l'endroit, dans le cas de numéros autres que géographiques; la facilité ne permet pas de conserver le numéro de téléphone national entre un opérateur de services téléphoniques accessibles au public en position déterminée et un opérateur de services téléphoniques accessibles au public sur un réseau de communications électroniques mobile;
48/1° " Bureau d'enregistrement de noms de domaine Internet " : une entité qui tient à jour	48/1° " Bureau d'enregistrement de noms de domaine Internet " : une entité qui tient à jour

un registre de noms de domaine et qui exploite un système de sorte que ces noms de domaine puissent être utilisés pour obtenir un accès à des adresses de protocole Internet ou d'autres informations via l'Internet;	un registre de noms de domaine et qui exploite un système de sorte que ces noms de domaine puissent être utilisés pour obtenir un accès à des adresses de protocole Internet ou d'autres informations via l'Internet;
48/2° " service universel " : un ensemble de services minimal défini à l'article 68 de qualité déterminée, disponible pour tous les utilisateurs quelle que soit leur situation géographique et compte tenu des conditions nationales spécifiques, d'un prix abordable;	48/2° " service universel " : un ensemble de services minimal défini à l'article 68 de qualité déterminée, disponible pour tous les utilisateurs quelle que soit leur situation géographique et compte tenu des conditions nationales spécifiques, d'un prix abordable;
49° " annuaire " : livre, liste ou fichier contenant principalement ou exclusivement des données concernant les abonnés d'un service téléphonique public et mis à la disposition du public en vue de permettre exclusivement ou principalement l'identification du numéro d'appel des utilisateurs finaux;	49° " annuaire " : livre, liste ou fichier contenant principalement ou exclusivement des données concernant les abonnés d'un service téléphonique public et mis à la disposition du public en vue de permettre exclusivement ou principalement l'identification du numéro d'appel des utilisateurs finaux;
50° (abrogé)	50° (abrogé)
51° " antenne " : un composant d'un appareil ou d'une station radio destiné au rayonnement et/ou à la captation d'ondes ;	51° " antenne " : un composant d'un appareil ou d'une station radio destiné au rayonnement et/ou à la captation d'ondes ;
52° " station de base " : une station de radiocommunication d'un réseau de communications électroniques installée et utilisée en un lieu déterminé, et destinée à assurer la couverture radioélectrique d'une zone géographique donnée;	52° " station de base " : une station de radiocommunication d'un réseau de communications électroniques installée et utilisée en un lieu déterminé, et destinée à assurer la couverture radioélectrique d'une zone géographique donnée;
53° " support " : une structure sur laquelle peuvent être placées les antennes de stations de base;	53° " support " : une structure sur laquelle peuvent être placées les antennes de stations de base;
54° " site d'antennes " : l'ensemble des constructions, comportant au moins un support, une antenne et des locaux pour les équipements électriques et électroniques, permettant l'installation et l'exploitation d'une ou plusieurs stations de base;	54° " site d'antennes " : l'ensemble des constructions, comportant au moins un support, une antenne et des locaux pour les équipements électriques et électroniques, permettant l'installation et l'exploitation d'une ou plusieurs stations de base;
55° " itinérance nationale " : la faculté pour un opérateur de permettre à ses clients d'accéder dans le même pays aux services de base offerts par un autre opérateur de réseau mobile de communications;	55° " itinérance nationale " : la faculté pour un opérateur de permettre à ses clients d'accéder dans le même pays aux services de base offerts par un autre opérateur de réseau mobile de communications;

56° " identification de la ligne " : numéro, signe ou ensemble de signes attribués à un abonné, à un utilisateur final, à un utilisateur ou à un terminal qui permet à celui-ci d'être joint par d'autres abonnés, utilisateurs finaux ou utilisateurs de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;	56° " identification de la ligne " : numéro, signe ou ensemble de signes attribués à un abonné, à un utilisateur final, à un utilisateur ou à un terminal qui permet à celui-ci d'être joint par d'autres abonnés, utilisateurs finaux ou utilisateurs de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public;
57° " identification de l'appelant " : toute donnée, disponible directement ou indirectement, dans les réseaux et services d'un opérateur, qui détermine le numéro d'appel du terminal, le nom de l'utilisateur final et l'endroit où l'équipement terminal se situe au moment de l'appel;	57° " identification de l'appelant " : toute donnée, disponible directement ou indirectement, dans les réseaux et services d'un opérateur, qui détermine le numéro d'appel du terminal, le nom de l'utilisateur final et l'endroit où l'équipement terminal se situe au moment de l'appel;
58° " service d'urgence " : tout service public ou d'intérêt public visé à l'article 107, § 1er, alinéa 1er, ou fixé par le Roi conformément à l'article 107, § 1er, alinéa 2, 1° ;	58° " service d'urgence " : tout service public ou d'intérêt public visé à l'article 107, § 1er, alinéa 1er, ou fixé par le Roi conformément à l'article 107, § 1er, alinéa 2, 1° ;
59° " numéro d'urgence " : numéro d'appel d'un service d'urgence fixé conformément à la procédure prévue à l'article 107, § 1er, alinéa 2, 2°de la présente loi;	59° " numéro d'urgence " : numéro d'appel d'un service d'urgence fixé conformément à la procédure prévue à l'article 107, § 1er, alinéa 2, 2°de la présente loi;
60° "communication d'urgence": une communication effectuée au moyen de services de communications interpersonnelles, entre un utilisateur final et un PSAP, dont le but est de recevoir de l'aide d'urgence de la part de services d'urgence;	60° "communication d'urgence": une communication effectuée au moyen de services de communications interpersonnelles, entre un utilisateur final et un PSAP, dont le but est de recevoir de l'aide d'urgence de la part de services d'urgence;
61° "PSAP" ("Public Safety Answering Point") ou "centre de gestion des appels d'urgence": un lieu physique où est réceptionnée initialement une communication d'urgence sous la responsabilité d'une autorité publique ou d'un organisme privé reconnu;	61° "PSAP" ("Public Safety Answering Point") ou "centre de gestion des appels d'urgence": un lieu physique où est réceptionnée initialement une communication d'urgence sous la responsabilité d'une autorité publique ou d'un organisme privé reconnu;
62° "zone d'activité d'un PSAP": zone géographique pour laquelle un PSAP gère toutes les communications d'urgence vers le service d'urgence, dénommée ci-après "zone d'activité" ;	62° "zone d'activité d'un PSAP": zone géographique pour laquelle un PSAP gère toutes les communications d'urgence vers le service d'urgence, dénommée ci-après "zone d'activité" ;
62/1° "PSAP le plus approprié": un PSAP établi par les autorités compétentes pour prendre en charge les communications d'urgence	62/1° "PSAP le plus approprié": un PSAP établi par les autorités compétentes pour prendre en charge les communications d'urgence

provenant d'une certaine zone ou les communications d'urgence d'un certain type;	provenant d'une certaine zone ou les communications d'urgence d'un certain type;
62/2° "sécurité des réseaux et services": la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services;	62/2° "sécurité des réseaux et services": la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services;
62/3° "incident de sécurité": tout événement ayant un effet négatif réel sur la sécurité des réseaux ou des services de communications électroniques;	62/3° "incident de sécurité": tout événement ayant un effet négatif réel sur la sécurité des réseaux ou des services de communications électroniques;
63° " réviseur agréé " : un réviseur d'entreprises inscrit au tableau de l'Institution des Réviseurs d'Entreprises;	63° " réviseur agréé " : un réviseur d'entreprises inscrit au tableau de l'Institution des Réviseurs d'Entreprises;
64° " hôpitaux " : les établissements de soins de santé visés à l'article 2 de la loi sur les hôpitaux, coordonnée le 7 août 1987;	64° " hôpitaux " : les établissements de soins de santé visés à l'article 2 de la loi sur les hôpitaux, coordonnée le 7 août 1987;
65° " écoles " : tout établissement d'enseignement primaire, secondaire ou supérieur appartenant au réseau d'une Communauté, d'une province, d'une commune ou à un réseau libre subventionné;	65° " écoles " : tout établissement d'enseignement primaire, secondaire ou supérieur appartenant au réseau d'une Communauté, d'une province, d'une commune ou à un réseau libre subventionné;
66° " bibliothèques publiques " : toute bibliothèque publique reconnue par l'Etat fédéral ou par une Communauté;	66° " bibliothèques publiques " : toute bibliothèque publique reconnue par l'Etat fédéral ou par une Communauté;
67° " bureau public de communications électroniques " : local ou dispositif accessible au public en vue de la mise à disposition temporaire contre rémunération, d'un équipement terminal permettant d'utiliser sur place un réseau ou un service de communications électroniques sans relation contractuelle avec le fournisseur du réseau ou du service ;	67° " bureau public de communications électroniques " : local ou dispositif accessible au public en vue de la mise à disposition temporaire contre rémunération, d'un équipement terminal permettant d'utiliser sur place un réseau ou un service de communications électroniques sans relation contractuelle avec le fournisseur du réseau ou du service ;
68° " violation de données à caractère personnel " : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la	68° " violation de données à caractère personnel " : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la

divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté;	divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté;
69° " ENISA " : Agence européenne chargée de la sécurité des réseaux et de l'information instituée par le Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information;	69° " ENISA " : Agence européenne chargée de la sécurité des réseaux et de l'information instituée par le Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information;
70° "ORECE": Organe des régulateurs européens des communications électroniques, en anglais "Body of European Regulators for Electronic Communications (BEREC)", institué par le Règlement (UE) n° 2018/1971 du Parlement européen et du Conseil du 11 décembre 2018 établissant l'Organe des régulateurs européens des communications électroniques (ORECE) et l'Agence de soutien à l'ORECE (Office ORECE) modifiant le règlement (UE) 2015/2120 et abrogeant le règlement (CE) n° 1211/200, ci-après dénommé "Règlement (UE) 2018/1971;	70° "ORECE": Organe des régulateurs européens des communications électroniques, en anglais "Body of European Regulators for Electronic Communications (BEREC)", institué par le Règlement (UE) n° 2018/1971 du Parlement européen et du Conseil du 11 décembre 2018 établissant l'Organe des régulateurs européens des communications électroniques (ORECE) et l'Agence de soutien à l'ORECE (Office ORECE) modifiant le règlement (UE) 2015/2120 et abrogeant le règlement (CE) n° 1211/200, ci-après dénommé "Règlement (UE) 2018/1971;
71° "Office": Agence de soutien à l'ORECE, instituée par le Règlement (UE) 2018/1971;	71° "Office": Agence de soutien à l'ORECE, instituée par le Règlement (UE) 2018/1971;
71/1° "RSPG": groupe pour la politique en matière de spectre radioélectrique, en anglais "Radio Spectrum Policy Group", institué par la décision de la Commission européenne du 11 juin 2019 instituant un groupe pour la politique en matière de spectre radioélectrique et abrogeant la décision 2002/622/CE;	71/1° "RSPG": groupe pour la politique en matière de spectre radioélectrique, en anglais "Radio Spectrum Policy Group", institué par la décision de la Commission européenne du 11 juin 2019 instituant un groupe pour la politique en matière de spectre radioélectrique et abrogeant la décision 2002/622/CE;
72° " Utilisateur prioritaire " : utilisateur de réseaux ou de services de communications électroniques qui par les tâches qu'il exerce et ses activités a une fonction sociétaire reconnue importante par les autorités et qui par un manque d'accès aux services ou réseaux de communications électroniques n'est plus en mesure d'exécuter de façon adéquate ses tâches ou activités, ce qui peut mener à une situation qui peut nuire à la sécurité publique, ou la sécurité civile et la protection civile, ou à la défense civile, ou à la planification de crise, ou à	72° " Utilisateur prioritaire " : utilisateur de réseaux ou de services de communications électroniques qui par les tâches qu'il exerce et ses activités a une fonction sociétaire reconnue importante par les autorités et qui par un manque d'accès aux services ou réseaux de communications électroniques n'est plus en mesure d'exécuter de façon adéquate ses tâches ou activités, ce qui peut mener à une situation qui peut nuire à la sécurité publique, ou la sécurité civile et la protection civile, ou à la défense civile, ou à la planification de crise, ou à

la sécurité ou à la protection du potentiel économique et scientifique du pays;	la sécurité ou à la protection du potentiel économique et scientifique du pays;
73° (abrogé)	73° (abrogé)
74° (annulé par la Cour constitutionnelle)	**74° « Appels infructueux » : toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau ;**
75° "radiorepérage" : la détermination de la position, de la vitesse et/ou d'autres caractéristiques d'un objet ou l'obtention d'informations relatives à ces paramètres, grâce aux propriétés de propagation des ondes radioélectriques ;	75° "radiorepérage" : la détermination de la position, de la vitesse et/ou d'autres caractéristiques d'un objet ou l'obtention d'informations relatives à ces paramètres, grâce aux propriétés de propagation des ondes radioélectriques ;
76° "mise à disposition sur le marché" : toute fourniture d'équipements hertziens destinés à être distribués, consommés ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;	76° "mise à disposition sur le marché" : toute fourniture d'équipements hertziens destinés à être distribués, consommés ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;
77° "mise sur le marché" : la première mise à disposition d'équipements hertziens sur le marché de l'Union;	77° "mise sur le marché" : la première mise à disposition d'équipements hertziens sur le marché de l'Union;
78° "mise en service" : la première utilisation des équipements hertziens au sein de l'Union par leur utilisateur final;	78° "mise en service" : la première utilisation des équipements hertziens au sein de l'Union par leur utilisateur final;
79° "fabricant" : toute personne physique ou morale qui fabrique des équipements hertziens ou fait concevoir ou fabriquer des équipements hertziens, et qui les commercialise sous son nom ou sa marque;	79° "fabricant" : toute personne physique ou morale qui fabrique des équipements hertziens ou fait concevoir ou fabriquer des équipements hertziens, et qui les commercialise sous son nom ou sa marque;
80° "importateur" : toute personne physique ou morale établie dans l'Union européenne qui met des équipements hertziens provenant d'un pays tiers sur le marché de l'Union européenne;	80° "importateur" : toute personne physique ou morale établie dans l'Union européenne qui met des équipements hertziens provenant d'un pays tiers sur le marché de l'Union européenne;
81° "distributeur" : toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met des équipements hertziens à disposition sur le marché;	81° "distributeur" : toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met des équipements hertziens à disposition sur le marché;

82° "rappel" : toute mesure visant à obtenir le retour d'équipements hertziens déjà mis à la disposition de l'utilisateur final;	82° "rappel" : toute mesure visant à obtenir le retour d'équipements hertziens déjà mis à la disposition de l'utilisateur final;
83° "retrait" : toute mesure visant à empêcher la mise à disposition sur le marché d'équipements hertziens présents dans la chaîne d'approvisionnement;	83° "retrait" : toute mesure visant à empêcher la mise à disposition sur le marché d'équipements hertziens présents dans la chaîne d'approvisionnement;
84° "interface radio" : les spécifications relatives à l'utilisation réglementée du spectre radioélectrique;	84° "interface radio" : les spécifications relatives à l'utilisation réglementée du spectre radioélectrique;
85° " prestataire de services " : personne dont le service ou le contenu fourni via un réseau de communications électroniques est porté en compte par un opérateur à l'utilisateur final;	85° " prestataire de services " : personne dont le service ou le contenu fourni via un réseau de communications électroniques est porté en compte par un opérateur à l'utilisateur final;
86° " opérateur facilitateur " : opérateur qui met à la disposition d'un prestataire de services des numéros ou d'autres moyens, de manière à permettre à ce dernier de faire percevoir, par voie de facturation par un opérateur ou par comptabilisation sur une carte prépayée d'un opérateur, une rémunération pour son service ou son contenu.	86° " opérateur facilitateur " : opérateur qui met à la disposition d'un prestataire de services des numéros ou d'autres moyens, de manière à permettre à ce dernier de faire percevoir, par voie de facturation par un opérateur ou par comptabilisation sur une carte prépayée d'un opérateur, une rémunération pour son service ou son contenu.
87° “infrastructure passive”: tout élément d’un réseau de communications électroniques qui est destiné à accueillir d’autres éléments d’un autre réseau de communications électroniques sans devenir lui-même un élément actif de ce dernier réseau, tel que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours ou poteaux;	87° “infrastructure passive”: tout élément d’un réseau de communications électroniques qui est destiné à accueillir d’autres éléments d’un autre réseau de communications électroniques sans devenir lui-même un élément actif de ce dernier réseau, tel que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours ou poteaux;
88° “point d’information unique”: le système d’information mis en place au sein de la plate-forme de l’ASBL “KLIM – CICC (Federaal Kabels en leidingen Informatie Meldpunt - Point de Contact fédéral Information Câbles et Conduites).	88° “point d’information unique”: le système d’information mis en place au sein de la plate-forme de l’ASBL “KLIM – CICC (Federaal Kabels en leidingen Informatie Meldpunt - Point de Contact fédéral Information Câbles et Conduites) ;
89° à venir	
90° à venir	
	91° « données de communications électroniques » : le contenu de

	communications électroniques et les métadonnées de communications électroniques ;
	92° «contenu de communications électroniques» : le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son ;
	93° «métadonnées de communications électroniques» : les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.
TITRE IV. La protection des intérêts de la société et des utilisateurs	TITRE IV. La protection des intérêts de la société et des utilisateurs
CHAPITRE II/1. - De la sécurité des communications électroniques	CHAPITRE II/1. - De la sécurité des communications électroniques
Art. 107/5	**Art. 107/5**
L'emploi de la cryptographie est libre.	**§ 1er. Afin de favoriser la sécurité numérique, l'utilisation de la cryptographie est libre dans les limites prévues aux §§ 2 à 4.**
La fourniture au public de services de cryptographie que le Roi détermine, après avis de l'Institut, est soumise à une déclaration préalable auprès de l'Institut.	**§ 2. Le recours à la cryptographie ne peut pas empêcher les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant.**
Le Roi arrête, après avis de l'Institut, le contenu et la forme de cette déclaration.	**§ 3. Le recours à la cryptographie, utilisé par un opérateur, visant à garantir la sécurité des communications, ne peut pas empêcher l'exécution d'une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et localiser des communications non accessibles au public.**

	§ 4. L'utilisation de la cryptographie par un opérateur étranger, dont l'utilisateur final ou l'abonné est situé sur le territoire belge, ne peut pas empêcher l'exécution d'une demande d'une autorité compétente telle que visée aux paragraphes 2 à 3.
	Toute clause contractuelle prise par les opérateurs faisant obstacle à l'exécution de cet alinéa est interdite et nulle de plein droit.
Sous-section 7. - Dispositions diverses.	Sous-section 7. - Dispositions diverses.
	Art. 121/8
	§ 1er. Sans prendre connaissance du contenu des communications, les opérateurs prennent les mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés.
	Le Roi peut préciser les mesures à prendre par les opérateurs en vertu de l'alinéa 1er.
	L'Institut a le pouvoir de donner des instructions contraignantes, y compris des instructions concernant les dates limites de mise en œuvre, en vue de l'application du présent paragraphe.
	§ 2. Lorsque cela se justifie au regard de la gravité des circonstances, qui doivent être examinées au cas par cas, les mesures appropriées visées au paragraphe 1er, alinéa 1er, peuvent comprendre notamment :
	- Des mesures au niveau du réseau, tels que le blocage des numéros, de services, des URLs, de noms de domaine, d'adresses IP ou de tout autre élément d'identification de la communication électronique ;
	- Des mesures au niveau de l'utilisateur final, telles que la désactivation complète ou partielle de certains services ou équipements.

CHAPITRE III. - Protection des utilisateurs finaux	CHAPITRE III. - Protection des utilisateurs finaux
Section 2. - Secret des communications, traitement des données et protection de la vie privée.	Section 2. - Secret des communications, traitement des données et protection de la vie privée.
Art. 122	**Art. 122**
§ 1er. Les opérateurs suppriment les données de trafic concernant les abonnés ou les utilisateurs finaux de leurs données de trafic ou rendent ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication.	§ 1er. Les opérateurs suppriment les données de trafic concernant les abonnés ou les utilisateurs finaux de leurs données de trafic ou rendent ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication.
L'alinéa 1er s'applique sans préjudice du respect des obligations de coopération, prévues par ou en vertu de la loi, avec :	
1° les autorités compétentes pour la recherche ou la poursuite d'infractions pénales;	
2° le service de médiation pour les télécommunications pour la recherche de l'identité de toute personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques.	
3° les services de renseignement et de sécurité dans le cadre de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	
§ 2. Par dérogation au § 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs stockent et traitent les données suivantes :	**§2. Par dérogation au paragraphe 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs peuvent conserver et traiter les données de trafic nécessaires à cette fin.**
1° l'identification de la ligne appelante;	
2° les adresses relatives à l'abonné et au lieu de raccordement, ainsi que le type d'équipement terminal;	
3° le nombre total d'unités à facturer pour la période de facturation;	
4° l'identification de la ligne appelée;	

5° le type d'appel, l'heure à laquelle l'appel a commencé, la durée de l'appel ou la quantité de données transmises;	
6° la date de la communication ou du service;	
7° d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.	
Sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, l'opérateur informe, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent :	Sans préjudice de l'application **du RGPD et de la loi du 30 juillet 2018**, l'opérateur informe, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent :
1° des types de données de trafic traitées;	1° des types de données de trafic traitées;
2° des objectifs précis du traitement;	2° des objectifs précis du traitement;
3° de la durée du traitement.	3° de la durée du traitement.
Le traitement des données énumérées à alinéa 1er, est seulement autorisé jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.	Le traitement des données **visées** à alinéa 1er, est seulement autorisé jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.
§ 3. Par dérogation au § 1er et dans le seul but d'assurer le marketing des services de communications électroniques propres et d'établir le profil d'utilisation visé à l'article 110, § 4, alinéa premier, article 110/1 et article 111, § 3, alinéa 2, ou des services à données de trafic ou de localisation, les opérateurs ne peuvent traiter les données visées au § 1er qu'aux conditions suivantes :	§ 3. Par dérogation au § 1er et dans le seul but d'assurer le marketing des services de communications électroniques propres et d'établir le profil d'utilisation visé à l'article 110, § 4, alinéa premier, article 110/1 et article 111, § 3, alinéa 2, ou des services à données de trafic ou de localisation, les opérateurs ne peuvent traiter les données visées au § 1er qu'aux conditions suivantes :
1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci en vue du traitement :	1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci en vue du traitement :
a) des types de données de trafic traitées;	a) des types de données de trafic traitées;
b) des objectifs précis du traitement;	b) des objectifs précis du traitement;

c) de la durée du traitement.	c) de la durée du traitement.
2° L'abonné ou, le cas échéant, l'utilisateur final, a, préalablement au traitement, donné son consentement pour le traitement.	2° L'abonné ou, le cas échéant, l'utilisateur final, a, préalablement au traitement, donné son consentement pour le traitement.
Par consentement pour le traitement au sens du présent article, on entend la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées.	Par consentement pour le traitement au sens du présent article, on entend **le consentement au sens de l'article 4 du RGPD**.
3° L'opérateur concerné offre gratuitement à ses abonnés ou ses utilisateurs finaux la possibilité de retirer le consentement donné de manière simple.	3° L'opérateur concerné offre gratuitement à ses abonnés ou ses utilisateurs finaux **la possibilité de retirer le consentement donné facilement et à tout moment.**
4° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question pour l'établissement du plan d'utilisation visé à l'article 110, § 4, alinéa 1er, article 110/1 et article 111, § 3, alinéa 2 ou pour l'action de marketing en question.	4° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question pour l'établissement du plan d'utilisation visé à l'article 110, § 4, alinéa 1er, article 110/1 et article 111, § 3, alinéa 2 ou pour l'action de marketing en question.
Ces conditions sont d'application sous réserve des conditions complémentaires découlant de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.	Ces conditions sont d'application sous réserve des conditions complémentaires découlant de l'application **du RGPD et de la loi du 30 juillet 2018.**
§ 4. Par dérogation au § 1er, les données peuvent être traitées pour déceler des fraudes éventuelles.	**§ 4. Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, l'opérateur :**
Les données sont communiquées aux autorités compétentes en cas de délit.	
	1° conserve les données reprises dans le « Call detail record » (CDR) ou dans un registre fonctionnellement équivalent, ainsi que les données de localisation de l'auteur de la fraude présumée ou de l'utilisation malveillante

	présumée du réseau lorsqu'elles sont disponibles, 4 mois à partir de la date de la communication ;
	2° conserve pendant 12 mois à partir de la date de la communication les données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles ;
	3° conserve les données visées au 1° et qui sont relatives à une fraude spécifique identifiée ou une utilisation malveillante du réseau spécifique identifiée le temps nécessaire à son analyse et à sa résolution, le cas échéant au-delà du délai de 4 mois visé au 1° ;
	4° conserve les données de trafic visées au 2° et relatives à une utilisation malveillante spécifique du réseau, le temps nécessaire au traitement de cette dernière, le cas échéant au-delà du délai de 12 mois visé au 2° ;
	5° traite les données de trafic nécessaires à ces fins, en ce compris, lorsque c'est nécessaire, les données visées au paragraphe 2.
	Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service, d'identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées nécessaires à ces fins.
	Le Roi peut préciser et étendre, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de l'Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire pour la poursuite des finalités prévues au présent paragraphe.
	En cas de fraude présumée ou d'utilisation malveillante présumée, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec la fraude présumée ou l'utilisation malveillante présumée.

	§ 4/1. Par dérogation au paragraphe 1er, les opérateurs peuvent conserver et traiter les données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.
	Ils peuvent les conserver pour une durée de douze mois à partir de la date de la communication.
	Ils peuvent conserver les données visées à l'alinéa 1er relatives à une atteinte spécifique à la sécurité du réseau pendant la durée nécessaire pour la traiter, le cas échéant au-delà du délai de 12 mois visé à l'alinéa 2.
	En cas d'atteinte à la sécurité de leurs réseaux et services de communications électroniques, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec l'atteinte à la sécurité de leurs réseaux et services de communications électroniques.
	§ 4/2. Par dérogation au paragraphe 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation imposée par une norme législative formelle, pour la durée requise à cette fin.
§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des clients, de détecter les fraudes, du marketing des services de communications électroniques propres ou de la fourniture de services à données de trafic ou de localisation.	**§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination.**
Le traitement est limité à ce qui est strictement nécessaire à l'exercice de telles activités.	

§ 6. L'Institut, l'Autorité belge de la concurrence, les juridictions de l'ordre judiciaire et le Conseil d'Etat peuvent, dans le cadre de leurs compétences, être informés des données de trafic et de facture pertinentes en vue du règlement de litiges, parmi lesquels des litiges relatifs à l'interconnexion et la facturation.	§ 6. **L'Institut, le Service de médiation pour les télécommunications,** l'Autorité belge de la concurrence, les juridictions de l'ordre judiciaire et le Conseil d'Etat peuvent, dans le cadre de leurs compétences, être informés des données de trafic et de facture pertinentes en vue du règlement de litiges, parmi lesquels des litiges relatifs à l'interconnexion et la facturation.
Art. 123	**Art. 123**
§ 1er. Sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les opérateurs de réseaux mobiles ne peuvent traiter de données de localisation se rapportant à un abonné ou un utilisateur final que lorsqu'elles ont été rendues anonymes ou que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation.	**§ 1er. Sans préjudice de l'application du RGPD et de la loi du 30 juillet 2018, les opérateurs de réseaux mobiles ne peuvent conserver et traiter de données de localisation autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final que dans les cas suivants :**
	1° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées maximum 12 mois à partir de la date de la communication, sauf en cas d'atteinte spécifique à la sécurité du réseau nécessitant de prolonger la conservation des données concernées au-delà de ce délai ;
	2° lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau, les données étant conservées maximum 4 mois à partir de la date de la communication, sauf en cas de fraude ou d'utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai ;
	3° lorsque les données ont été rendues anonymes ;
	4° lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service qui fait usage de données de trafic ou de localisation ;
	5° lorsque le traitement est nécessaire pour répondre à une obligation imposée par une norme législative formelle.

§ 2. Le traitement dans le cadre de la fourniture d'un service à données de trafic ou de localisation est soumis aux conditions suivantes :	§ 2. Le traitement dans le cadre de la fourniture d'un service à données de trafic ou de localisation est soumis aux conditions suivantes :
1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci pour le traitement :	1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci pour le traitement :
a) des types de données de localisation traites;	a) des types de données de localisation traites;
b) des objectifs précis du traitement;	b) des objectifs précis du traitement;
c) de la durée du traitement;	c) de la durée du traitement;
d) des tiers éventuels auxquels ces données seront transmises;	d) des tiers éventuels auxquels ces données seront transmises;
e) de la possibilité de retirer à tout moment, définitivement ou temporairement, le consentement donné pour le traitement.	e) de la possibilité de retirer à tout moment, définitivement ou temporairement, le consentement donné pour le traitement.
2° L'abonné ou, le cas échéant, l'utilisateur final, a préalablement au traitement, donné son consentement pour le traitement.	2° L'abonné ou, le cas échéant, l'utilisateur final, a préalablement au traitement, donné son consentement pour le traitement.
Par consentement pour le traitement au sens du présent article, on entend la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données de localisation se rapportant à lui soient traitées.	Par consentement pour le traitement au sens du présent article, on entend **le consentement au sens de l'article 4 du RGPD.**
3° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question.	3° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question.
4° L'opérateur concerné offre gratuitement à ses abonnés ou à ses utilisateurs finaux la possibilité de retirer le consentement donné, facilement et à tout moment, définitivement ou temporairement.	4° L'opérateur concerné offre gratuitement à ses abonnés ou à ses utilisateurs finaux la possibilité de retirer le consentement donné, facilement et à tout moment, définitivement ou temporairement.
§ 4. Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit les données de trafic et de localisation au service.	**§ 4. Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit le service qui fait usage de données de trafic ou de localisation, ou par la**

	Cellule de coordination de l'opérateur visée à l'article 127/3.
Le traitement est limité à ce qui est strictement nécessaire pour pouvoir fournir au service concerné les données de trafic ou de localisation.	Le traitement est limité à ce qui est strictement nécessaire pour pouvoir fournir au service concerné les données de trafic ou de localisation.
§ 5. En cas d'appel d'urgence aux centrales de gestion des services d'urgence offrant de l'aide sur place, les opérateurs annulent, pour autant que cela soit techniquement possible, en vue de permettre le traitement de l'appel d'urgence par les centrales de gestion concernées, le refus temporaire ou l'absence de consentement de l'abonné ou de l'utilisateur final concernant le traitement de données de localisation par ligne distincte.	§ 5. En cas d'appel d'urgence aux centrales de gestion des services d'urgence offrant de l'aide sur place, les opérateurs annulent, pour autant que cela soit techniquement possible, en vue de permettre le traitement de l'appel d'urgence par les centrales de gestion concernées, le refus temporaire ou l'absence de consentement de l'abonné ou de l'utilisateur final concernant le traitement de données de localisation par ligne distincte.
Cette annulation est gratuite.	Cette annulation est gratuite.
Art. 125	**Art. 125**
§ 1er. Les dispositions de l'article 124 de la présente loi et les articles 259bis et 314bis du Code pénal ne sont pas applicables :	§ 1er. Les dispositions de l'article 124 de la présente loi et les articles 259bis et 314bis du Code pénal ne sont pas applicables :
1° lorsque la loi permet ou impose l'accomplissement des actes visés;	1° lorsque la loi permet ou impose l'accomplissement des actes visés;
2° lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques;	2° lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques;
3° lorsque les actes sont accomplis en vue de permettre l'intervention des services de secours et d'urgence en réponse aux demandes d'aide qui leur sont adressées;	3° lorsque les actes sont accomplis en vue de permettre l'intervention des services de secours et d'urgence en réponse aux demandes d'aide qui leur sont adressées;
4° lorsque les actes sont accomplis par l'Institut sur ordre d'un juge d'instruction, du procureur du Roi, à la demande du dirigeant du service visé à l'article 3, 8°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, ou de l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale dans le cadre de ses missions, et/ou dans le cadre de sa mission générale de surveillance et de contrôle;	4° lorsque les actes sont accomplis par l'Institut sur ordre d'un juge d'instruction, du procureur du Roi, à la demande du dirigeant du service visé à l'article 3, 8°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, ou de l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale dans le cadre de ses missions, et/ou dans le cadre de sa mission générale de surveillance et de contrôle;

5° lorsque les actes sont accomplis par le service de médiation pour les télécommunications ou à la demande de celui-ci dans le cadre de ses missions légales de recherche et ne concernent pas l'écoute de communications;	5° lorsque les actes sont accomplis par le service de médiation pour les télécommunications ou à la demande de celui-ci dans le cadre de ses missions légales de recherche et ne concernent pas l'écoute de communications;
5° /1 : lorsque les actes sont accomplis par les agents habilités par le ministre qui a l'économie dans ses attributions, dans le cadre de leurs missions légales de recherche et ne concernent pas l'écoute de communications;	5° /1 : lorsque les actes sont accomplis par les agents habilités par le ministre qui a l'économie dans ses attributions, dans le cadre de leurs missions légales de recherche et ne concernent pas l'écoute de communications;
5° /2 (abrogé)	5° /2 (abrogé)
6° lorsque les actes sont accomplis dans le seul but d'offrir des services à l'utilisateur final consistant à empêcher la réception de communications électroniques non souhaitées, à condition d'avoir reçu l'autorisation de l'utilisateur final à cet effet.	6° lorsque les actes sont accomplis dans le seul but d'offrir des services à l'utilisateur final consistant à empêcher la réception de communications électroniques non souhaitées, à condition d'avoir reçu l'autorisation de l'utilisateur final à cet effet.
7° lorsque les actes sont accomplis par les opérateurs dans le but exclusif de combattre la fraude commise au moyen de messages utilisant des numéros de téléphone, comme des messages SMS ou MMS, et aux conditions suivantes:	7° lorsque les actes sont accomplis par les opérateurs dans le but exclusif de combattre la fraude commise au moyen de messages utilisant des numéros de téléphone, comme des messages SMS ou MMS, et aux conditions suivantes:
a) les actes restent limités à l'examen mécanique des messages afin d'établir la fraude; l'intervention humaine est autorisée exclusivement pour vérifier le bon fonctionnement des algorithmes informatiques;	a) les actes restent limités à l'examen mécanique des messages afin d'établir la fraude; l'intervention humaine est autorisée exclusivement pour vérifier le bon fonctionnement des algorithmes informatiques;
b) les opérateurs sont transparents vis-à-vis des utilisateurs finaux, afin qu'il soit clair pour eux que les messages sont susceptibles d'être examinés mécaniquement dans le cadre de la lutte contre la fraude;	b) les opérateurs sont transparents vis-à-vis des utilisateurs finaux, afin qu'il soit clair pour eux que les messages sont susceptibles d'être examinés mécaniquement dans le cadre de la lutte contre la fraude;
c) les données concernées ne peuvent être traitées que par des personnes chargées par l'opérateur de lutter contre la fraude;	c) les données concernées ne peuvent être traitées que par des personnes chargées par l'opérateur de lutter contre la fraude;
d) le traitement des données concernées est limité aux actes et à la durée nécessaires pour lutter contre la fraude ou jusqu'à la fin de la période durant laquelle une action en justice est possible.	d) le traitement des données concernées est limité aux actes et à la durée nécessaires pour lutter contre la fraude ou jusqu'à la fin de la période durant laquelle une action en justice est possible.

Si l'examen visé à l'alinéa 1er, 7°, *a)*, révèle une fraude, les opérateurs prennent des mesures concrètes pour lutter contre la fraude, comme le blocage des messages ou le remplacement dans les messages des URL renvoyant à un site Internet frauduleux par un message d'avertissement ou une URL avec un message d'avertissement.	Si l'examen visé à l'alinéa 1er, 7°, *a)*, révèle une fraude, les opérateurs prennent des mesures concrètes pour lutter contre la fraude, comme le blocage des messages ou le remplacement dans les messages des URL renvoyant à un site Internet frauduleux par un message d'avertissement ou une URL avec un message d'avertissement.
Avant le 1er février, les opérateurs fournissent à l'Institut un rapport annuel reprenant au moins les mesures qu'ils ont prises au cours de l'année écoulée pour lutter contre la fraude, leur efficacité ainsi que l'évolution de la fraude.	Avant le 1er février, les opérateurs fournissent à l'Institut un rapport annuel reprenant au moins les mesures qu'ils ont prises au cours de l'année écoulée pour lutter contre la fraude, leur efficacité ainsi que l'évolution de la fraude.
§ 2. Le Roi fixe, après avis de la Commission de la protection de la vie privée et de l'Institut, par arrêté délibéré en Conseil des ministres, les modalités et les moyens à mettre en oeuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques *L'abrogation de ce paragraphe par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, a été annulée par la Cour Constitutionnelle.*	
Art. 126	**Art. 126**
Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques.	**§ 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, conservent les données énumérées par le Roi, l'arrêté étant pris après avis de l'Autorité de protection des données et de l'Institut.**
Les données à conserver ainsi que la durée de la conservation, qui en matière de service	**Cet arrêté ne peut comprendre que des données de souscription de l'abonné au service**

téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.	**ainsi que des données qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé. Il ne porte pas sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication ou sur la localisation de l'équipement terminal.**
Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique.	**Par données de souscription, on entend les produits auxquels l'abonné a souscrit, le début et la fin du service ainsi que les identifiants et différents numéros qui lui sont attribués lors de la souscription au service.**
	Les opérateurs ne conservent les données visées à l'alinéa 1er que pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture des réseaux ou services de communications électroniques concernés.
	§ 2. Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.
	Par dérogation à l'alinéa 1er, les opérateurs conservent les adresses IP à la source de la connexion, autres que celle qui a été utilisée pour souscrire au service, ainsi que les autres données techniques d'identification des utilisateurs finaux, des équipements terminaux ou du service de communications électroniques utilisé, dont la liste est fixée par le Roi, jusqu'à douze mois après la fin de la session.
	§ 3. Le Roi fixe, après avis de l'Autorité de protection des données et de l'Institut, les exigences auxquelles les données visées au paragraphe 1er, alinéa 1er, doivent répondre.
Remarque : *les modifications que la loi du 1er septembre 2016 a apportées* ***à l'article 127*** *ont été annulées par la Cour constitutionnelle dans son arrêt du n° 158/2021 du 18 novembre 2021. Dans cet arrêt, la Cour maintient cependant les*	

effets des modifications annulées jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus.	
Art. 126/1	**Art. 126/1**
Remarque : *par son arrêt n° 57/2021 du 22 avril 2021 (M.B. 28/06/2021, p. 65587), la Cour constitutionnelle a annulé le présent article.*	**§ 1er. Sans préjudice du RGDP et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées au paragraphe 2, pour les zones géographiques visées au paragraphe 3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans le présent article.**
	Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communication électroniques concernés.
	Ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.
	§ 2. Les données visées au paragraphe 1er sont les données fixées par le Roi, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, et qui ressortent de la catégorie suivante :
	Les métadonnées de communications électroniques, en ce compris l'origine et la destination de la communication, la localisation de l'équipement terminal lors de la communication et les métadonnées des appels infructueux, pour autant que ces dernières données soient, dans le cadre de la fourniture des services de communications électroniques concernés :

	i° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs ; ou
	ii° en ce qui concerne les données de l'internet, journalisées par ces opérateurs.
	Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les exigences auxquelles ces données doivent répondre.
	§ 3. Les zones géographiques dans lesquelles sont conservées les données visées au paragraphe 2 sont les suivantes :
	1° la zone géographique composée des :
	- arrondissements judiciaires dans lesquels au moins 3 infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1000 habitants par an ont été constatées durant l'année sur une moyenne des trois années calendriers qui précèdent celle en cours ;
	- zones de police, dans lesquelles, au moins 3 infractions visées à l'article 90ter, §§ 2 à 4, du Code d'instruction criminelle par 1000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précèdent celle en cours, moins de 3 infractions visées à l'article 90ter §§ 2 à 4, du Code d'instruction criminelle par 1000 habitants par an sur une moyenne de trois années qui précèdent celle en cours ont été constatées.
	Dans l'hypothèse visée au 1er tiret, le délai de conservation des données visées au paragraphe 2 est de :

	a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90ter, §§ 2 à 4 du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois dernières années calendriers qui précèdent celle en cours ;
	b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90ter, §§ 2 à 4 du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours ;
	c) 12 mois, s'il y a 7 ou plus de 7 d'infractions visées à l'article 90ter §§ 2 à 4 du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.
	Dans l'hypothèse visée au deuxième tiret, le délai de conservation des données visées au paragraphe 2 est de :
	a) 6 mois, s'il y a 3 ou 4 infractions visées à l'article 90ter §§ 2 à 4 du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois dernières années calendriers qui précèdent celle en cours;
	b) 9 mois, s'il y a 5 ou 6 infractions visées à l'article 90ter §§ 2 à 4 du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;
	c) 12 mois, s'il y a 7 ou plus de 7 infractions visées à l'article 90ter§§ 2 à 4 du Code d'instruction criminelle par an par 1000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours
	Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non 5.
	Les statistiques relatives au nombre d'infractions visées à l'article 90ter §§ 2 à 4 du Code d'instruction criminelle par an par 1000

	habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police.
	Les périmètres des arrondissements judiciaires visés au 1° sont fixés par l'article 4 de l'annexe au Code judiciaire.
	Les périmètres des zones de police visées au 1° sont celles fixés à l'annexe de l'arrêté royal 24 octobre 2001 portant la dénomination des zones de police.
	La direction, visée à l'article 44/11 de la loi sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
	Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.
	Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que leur durée de conservation.
	Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation, ainsi que leur durée de conservation aux opérateurs.

	2° Toutes les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.
	Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin qu'il prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées au § 2 sur l'ensemble du territoire.
	L'obligation de conservation visée à l'alinéa précédent est confirmée par arrêté royal sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal publié dans le mois de la décision visée à l'alinéa précédent, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.
	3° Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave, à savoir :
	a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2., 3°, 4° et 5° de la Code de la Navigation ;
	b) les gares au sens de l'article 2, 5° de la loi du 27 avril 2018 sur la police des chemins de fer ;
	c) les stations de métro et de pré-métro ;
	d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement

	européen et du Conseil, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports ;
	e) les bâtiments affectés à l'administration des douanes et accises ;
	f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement ;
	g) les armuriers et les stands de tir au sens de l'article 2, points 1 et 19 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes ;
	h) les établissements visés à l'article 3.1.a) de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants ;
	i) les établissements SEVESO visés dans l'accord de coopération du 16 février 2016 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses ;
	j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et ses arrêtés d'exécution ; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

	k) le siège social de la S.A. Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace ;
	l) les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de service essentiels désignés sur base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;
	m) le cas échéant sans préjudice du § 6 alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave fixées par arrêté royal.
	4° Les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir :
	a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution et les cabinets ministériels ;
	b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'Etat et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité ;
	c) pour le transport, les autoroutes et les parkings publics attenants ;

	d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances :
	i) les assemblées législatives au sens de l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution ;
	ii) les maisons communales et les hôtels de ville ;
	iii) le palais royal ;
	iv) les domaines royaux ;
	v) les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du Titre III de la Constitution ;
	vi) les communes dans lesquelles se trouvent des domaines militaires ;
	vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'Etat ;
	e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;
	f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale :
	i) les hôpitaux au sens de l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soin ;
	ii) la Banque nationale de Belgique ;
	g) le cas échéant, sans préjudice du § 6 alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.
	5° Les zones où il y a une menace potentielle grave pour les intérêts des institutions

	internationales établies sur le territoire national, à savoir :
	a) les ambassades et les représentations diplomatiques ;
	b) les bâtiments affectés à l'Union Européenne ;
	c) les bâtiments et infrastructures affectés à l'OTAN ;
	d) les institutions de l'Espace économique européen ;
	e) les institutions des Nations Unies ;
	f) le cas échéant, sans préjudice du § 6 alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.
	Pour chaque catégorie de zone visée à l'alinéa 1er, 3° à 5° inclus, le Roi détermine l'étendue du périmètre de la zone.
	Chaque autorité compétente dans l'une des matières visées à l'alinéa 1er, points 3° à 5°, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.
	Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée au paragraphe 1er dans cette zone.
	A l'exception de la liste des lieux visés à l'alinéa 1er, point 4°, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences la liste actualisée des zones visées à l'alinéa 1er, 3° à 5°

	inclus, où une conservation de données est obligatoire.
	L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées à l'alinéa 1er, 3° à 5° inclus, soient retirées de la liste.
	Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa précédent, le ministre de la Défense, le ministre de la Justice, et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.
	L'arrêté ministériel visé à l'alinéa précédent est publié par voie de mention au Moniteur belge.
	Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.
	Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.
	§ 4. Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone.
	Lorsque, compte tenu de la technologie utilisée par l'opérateur, celui-ci n'est pas en mesure de localiser l'équipement terminal ayant participé à la communication, y compris l'appel infructueux, de façon plus précise que sa

	localisation sur le territoire national, l'opérateur conserve les données visées au paragraphe 2 pour la durée la plus courte fixée en exécution du présent article, à la condition qu'en exécution du présent article l'ensemble du territoire national soit soumis à une obligation de conservation. Lorsque cette condition n'est pas remplie, l'opérateur concerné par le présent alinéa ne conserve pas de données en exécution du présent article.
	Lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur conserve les données de trafic pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone visée au paragraphe 3.
	Les opérateurs conservent les données relatives à la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, énumérées dans l'arrêté royal visé au paragraphe 2, alinéa 2, lorsque cet équipement se trouve dans une zone visée au paragraphe 3.
	Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée au paragraphe 3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent, si disponible, à cet effet la localisation satellitaire d'un équipement terminal.
	Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données à une zone visée au paragraphe 3, il conserve les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.
	Lorsqu'un point d'agrégation de l'opérateur, telle une antenne, couvre plusieurs zones géographiques visées au paragraphe 3 qui sont soumises à des durées de conservation différentes, l'opérateur conserve les données pour ce point d'agrégation pendant la durée de conservation la plus courte.

	Lorsqu'en application du présent article, différentes durées de conservation sont applicables à des mêmes données, les opérateurs conservent les données pendant la durée la plus courte.
	§ 5. Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, et après avis des autorités de protection des données compétentes et de l'Institut, les éléments suivants :
	- les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées au paragraphe 3 ;
	- la liste des différentes autorités compétentes dans les matières visées au paragraphe 3, alinéa 1er, points 2° à 5° ;
	- les modalités de communication des informations par les autorités compétentes vers le service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er ;
	- s'il y échet, les zones géographiques additionnelles visées au paragraphe 3, alinéa 1er, points 3°, m), 4°, g) et 5°, f).
	L'arrêté royal visé à l'alinéa 1er, 4ème tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1er en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal.
	§ 6. Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et de la Sécurité, et de l'Institut et des autorités de protection des données

	compétentes, un rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 5, afin de vérifier si des dispositions doivent être adaptées.
	Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 5 répondent toujours aux critères visés au paragraphe 3, alinéa 1er, points 3° à 5° et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.
	Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.
	Le rapport d'évaluation comprend également le pourcentage du territoire national auquel s'applique l'obligation de conservation des données en vertu du présent article.
	Ce rapport est envoyé à l'Organe de contrôle de l'information policière et au Comité permanent R.
Art. 127.	**Art. 127.**
§ 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs, aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ou aux utilisateurs finaux, en vue de permettre :	§ 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs, aux canaux de vente de services de communications électroniques, aux entreprises fournissant un service d'identification ou aux utilisateurs finaux, en vue de permettre :
1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence;	1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence;
2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des	2° l'identification de l'utilisateur final, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des

communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.
Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.	Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.	Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.
Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.	Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.
Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.	Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.
Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.	Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.
L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.	L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er.	Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er.
Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, aux opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.	Le Roi fixe, après l'avis de l'Institut, les tarifs rétribuant la collaboration des opérateurs aux opérations visées à l'alinéa 1er, 2° ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.
§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.	§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, **à l'exception de systèmes d'encryptage, qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements, qui font l'objet de règles particulières prévues à l'article 107/5**.
§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.	§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.
Les utilisateurs finaux non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, qui sont définis par cet arrêté royal, s'identifient dans le délai fixé par l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, ce délai ne pouvant excéder six mois après la publication de l'arrêté royal visé au paragraphe 1er. L'interdiction visée au paragraphe 2 ne s'applique qu'après la fin du délai accordé à l'utilisateur final pour s'identifier.	Les utilisateurs finaux non identifiés de cartes prépayées achetées avant l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, qui sont définis par cet arrêté royal, s'identifient dans le délai fixé par l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, ce délai ne pouvant excéder six mois après la publication de l'arrêté royal visé au paragraphe 1er. L'interdiction visée au paragraphe 2 ne s'applique qu'après la fin du délai accordé à l'utilisateur final pour s'identifier.
§ 4. Si un opérateur ou un fournisseur visé à l'article 126, § 1er, alinéa 1er, ne respecte pas les mesures techniques et administratives qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.	§ 4. Si un opérateur ou un fournisseur visé à l'article 126, § 1er, alinéa 1er, ne respecte pas les mesures techniques et administratives qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.
§ 5. Les opérateurs et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, déconnectent les utilisateurs finaux qui ne respectent pas les mesures techniques et administratives qui leur	§ 5. Les opérateurs et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, déconnectent les utilisateurs finaux qui ne respectent pas les mesures techniques et administratives qui leur

sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion.	sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion.
[...]	[...]
§ 6. [...] (abrogation annulée par la Cour constitutionnelle)	§ 6. Chaque opérateur établit, sur la base du paragraphe 1er, une procédure interne permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition de l'Institut des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.
	Art. 127/1
	§ 1er. Pour l'application du présent article, la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux :
	1° qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88bis, alinéa 1er, du Code d'instruction criminelle ;
	2° qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 au sens de l'article XV.70 du Code de droit économique ;
	3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) ou aux dispositions prises sur la base ou en exécution de ces articles.
	§ 2. Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle :

	1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;
	2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique ;
	3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques ;
	4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information ;
	5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques ;
	6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave ;
	7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ;
	8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave ;
	9° l'Institut dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle ;
	10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques.

	§ 3. Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.
	Seules les autorités visées au paragraphe 2, peuvent obtenir d'un opérateur des données conservées en vertu des articles 126 et 127 pour les finalités prévues dans ce même paragraphe, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.
	Par dérogation à l'alinéa 2, les autorités visées au paragraphe 2, 10°, ne peuvent pas obtenir d'un opérateur des adresses IP attribuées à la source de la connexion.
	Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.
	§ 4. Les données conservées en vertu de l'article 126/1 le sont pour les autorités et finalités visées au paragraphe 2, 1°, 2°, 3° et 6°.
	Seules les autorités visées au paragraphe 2, 1°, 2°, 3°, 6° et 9° peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu de l'article 126/1, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.
	§ 5. La norme législative formelle de droit belge visée aux paragraphes 2 à 4 précise :
	- **la ou les catégories d'entreprises auxquelles l'autorité peut demander des données ;**

	- **les catégories de données qui peuvent être demandées ;**
	- **les finalités poursuivies ;**
	- **les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.**
	Le ministre fait publier au Moniteur belge une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1 et 127.
	A la demande du ministre ou de l'Institut, les autorités belges visées aux paragraphes 2 à 4 fournissent les informations nécessaires pour la rédaction de cette circulaire.
	§ 6. Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1 ou 127 comprennent les mentions minimales suivantes :
	1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service ;
	2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central ;
	3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité ;
	4° le délai de réponse souhaité.
	§ 7. L'Institut transmet annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de

	données conservées en vertu des articles 122, 123, 126, 126/1 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants.
	Ces statistiques comprennent notamment :
	1° les cas dans lesquels des données conservées ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;
	2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ;
	3° les cas dans lesquels des demandes de données conservées n'ont pu être satisfaites.
	Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l'information confidentielle.
	Les données qui concernent l'application de l'alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.
	L'Institut demande aux opérateurs et au service désigné par le Roi les informations qui lui permettent de remplir l'obligation visée à l'alinéa 1er.
	Art. 127/2
	§ 1er. Les opérateurs veillent à garantir la qualité des métadonnées de communications électroniques conservées et, pour ce qui concerne les données conservées pour les autorités, à ce qu'elles soient de la même qualité que les données traitées dans le cadre de la fourniture du réseau ou du service de communications électroniques.
	Les opérateurs mettent tout en œuvre pour établir les liens techniques entre les données conservées pour les autorités qui sont nécessaires pour répondre à leurs demandes.

	§ 2. Pour ce qui concerne les données d'identification de l'abonné et les métadonnées de communications électroniques, conservées pour les autorités, les opérateurs :
	1° garantissent que les données conservées sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ou traitées par le service ;
	2° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès ;
	3° ne peuvent utiliser les données conservées pour d'autres finalités que la fourniture de ces données aux autorités, sauf lorsqu'ils obtiennent le consentement des abonnés concernés conformément à l'article 4 du RGDP et sans préjudice d'autres dispositions légales.
	§ 3. Pour ce qui concerne les données d'identification de l'abonné et les métadonnées de communications électroniques, les opérateurs :
	1° conservent les données sur le territoire de l'Union européenne et fournissent en Belgique les données demandées par une autorité belge;
	2° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données ou rendent ces données anonymes ;
	3° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, conformément à l'article 105/1 ;
	4° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités n'est effectué que par un ou plusieurs

	membres de la Cellule de coordination visée à l'article 127/3, § 1er, de manière manuelle ou automatisée ;
	5° assurent une traçabilité de l'exploitation des données conservées.
	§ 4. La traçabilité visée au paragraphe 3, alinéa 1er, 5°, s'effectue à l'aide d'un journal.
	L'opérateur prend les mesures nécessaires pour que chaque consultation des données qu'il conserve pour les autorités génère de manière automatisée un enregistrement dans le journal des données suivantes : l'identité de la personne ayant consulté les données, le moment de la consultation et les données consultées.
	Ce journal comprend également les informations et documents suivants, qui, le cas échéant, y sont introduits de manière manuelle :
	1° l'identité de l'autorité demanderesse, l'objet, la date et l'heure de la demande, une copie de la demande ou un lien vers cette dernière ;
	2° pour ce qui concerne la réponse de l'opérateur à la demande de l'autorité : l'identité de son destinataire, la date et l'heure de son envoi ainsi que le moyen de communication utilisé pour l'envoyer.
	Le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte.
	Les données de ce journal sont conservées pendant une période de dix ans. A l'échéance de la période de conservation, les données du journal sont détruites.
	L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal. Toute modification des données reprises dans le

	journal est interdite. Toute consultation du journal est journalisée.
	Le Roi peut préciser, après avis de l'Autorité de protection des données et de l'Institut, les exigences à respecter par les opérateurs concernant le journal.
	Dans le cadre du contrôle de l'opérateur, l'Institut et l'Autorité de protection des données peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.
	§ 5. Si l'Institut dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2, 3 ou 4, il peut l'obliger à se soumettre à un contrôle de sécurité effectué par un organisme qualifié indépendant, proposé par l'opérateur à l'Institut pour accord.
	Cet organisme ne prend pas connaissance des demandes des autorités envers les opérateurs, en ce compris le journal visé au paragraphe 4.
	Le rapport et les résultats de ce contrôle de sécurité sont communiqués à l'Institut. Le coût du contrôle est à la charge de l'opérateur.
	Art. 127/3
	§ 1er. Auprès de chaque opérateur est constituée une Cellule de coordination, chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques.
	Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l'alinéa 1er. Ils peuvent cependant, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur.
	Ces autorités adressent leurs demandes à cette cellule.
	Le cas échéant, plusieurs opérateurs peuvent créer une Cellule de coordination commune. En pareil cas, chaque opérateur prend les mesures nécessaires pour que cette Cellule de

	coordination commune soit en mesure de répondre aux demandes qui lui sont adressées.
	Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité.
	§ 2. Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel. Ces membres ne communiquent aux préposés que les données strictement nécessaires pour obtenir cette aide.
	Chaque opérateur veille à la confidentialité des données traitées par la Cellule de coordination.
	Les membres de la Cellule de coordination disposent d'un avis de sécurité positif et non périmé, visé à l'article 22quinquies/1 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.
	Un avis de sécurité a une durée de validité de maximum 5 ans.
	L'autorité administrative compétente pour le traitement des avis est le ministre de la Justice.
	Le Roi définit des mesures de sécurité alternatives à un avis de sécurité, qui sont adaptées aux personnes pour lesquelles un avis de sécurité ne peut être rendu, à défaut d'informations suffisantes les concernant.
	Par dérogation à l'alinéa 3, une personne visée à l'alinéa 6 peut faire partie de la Cellule de coordination, en respectant ces mesures de sécurité alternatives et sans disposer d'un avis de sécurité.
	Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut :
	1° pour les opérateurs autres que ceux qui disposent déjà d'un officier de sécurité en

	raison d'autres activités que la Cellule de coordination, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un tel officier en fonction du nombre de demandes reçues de la part des autorités judiciaires, ainsi que les règles qui s'appliquent en l'absence d'un tel officier ;
	2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en particulier en matière d'emploi des langues ;
	3° les règles permettant l'accès des autorités belges habilitées aux coordonnées de la Cellule de coordination et de ses membres.
	§ 3. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs finaux. Il met, sur demande, à la disposition de l'Institut, des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.
	Chaque opérateur est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur base des articles 122, 123, 126, 126/1 et 127.
	§ 4. Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles. Sont déterminés, entre autres, les éléments suivants, le cas échéant et par autorité concernée :
	a) le mode de transfert, la forme et le contenu des demandes et des réponses ;
	b) le degré d'urgence de traitement des demandes ;
	c) le délai de réponse ;
	d) la disponibilité requise du service ;
	e) les modalités de test de la collaboration ;

	f) les tarifs de rétribution de cette collaboration.
	Si nécessaire et pour l'application du présent article, le Roi peut prévoir des règles différentes selon différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et la fourniture ou non d'un réseau de communications électroniques en Belgique.
TITRE V. - Dispositions procédurales et pénales.	TITRE V. - Dispositions procédurales et pénales.
CHAPITRE IV. - Dispositions Pénales.	CHAPITRE IV. - Dispositions Pénales.
Art. 145	**Art. 145**
§ 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 124, 126, 126/1, 127, 133 et les arrêtés pris en exécution des articles 32, 39, § 3, 47, 106/2, 126, 126/1 et 127.)	**§ 1er. Est punie d'une amende de 50 à 100 000 EUR, la personne qui enfreint les articles 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 107/5, 124, 126 à 127/3, 133 et les arrêtés pris en exécution des articles 9, § 7, 32, 39, § 3, 47, 106/2, 126, 126/1, 127, 127/2 et 127/3.**
§ 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 13/1, § 1er, et les arrêtés pris en exécution de l'article 16.	§ 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 13/1, § 1er, et les arrêtés pris en exécution de l'article 16.
§ 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement :	§ 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement :
1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite;	1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite;
2° (abrogé)	2° (abrogé)
3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci.	3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci.
§ 3bis. Est punie d'une amende de 50 EUR à 300 EUR et d'un emprisonnement de quinze jours à	§ 3bis. Est punie d'une amende de 50 EUR à 300 EUR et d'un emprisonnement de quinze jours à

deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.	deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.
§ 3ter. (Annulé par la Cour constitutionnelle).	**§ 3ter. Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement :**
	1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données conservées par l'opérateur pour les autorités ;
	2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1°, les détient, les révèle à une autre personne, les divulgue ou en fait un usage quelconque.
§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée.	§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée.
CHAPITRE 3 - Modifications à la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques	
Art. 8	**Art. 8**
L'autorité sectorielle notifie à l'exploitant la décision motivée de la désignation de son infrastructure comme infrastructure critique et communique une copie de cette décision avec mention de la date de notification à la DGCC.	L'autorité sectorielle notifie à l'exploitant la décision motivée de la désignation de son infrastructure comme infrastructure critique et communique une copie de cette décision avec mention de la date de notification à la DGCC.
La DGCC communique également à l'OCAM les informations utiles pour l'accomplissement de l'analyse de la menace visée à l'article 10, en ce compris la date à laquelle la notification a eu lieu.	La DGCC communique également à l'OCAM les informations utiles pour l'accomplissement de l'analyse de la menace visée à l'article 10, en ce compris la date à laquelle la notification a eu lieu.

La DGCC informe le bourgmestre de la commune sur le territoire de laquelle se trouve l'infrastructure critique de cette désignation.	La DGCC informe le bourgmestre de la commune sur le territoire de laquelle se trouve l'infrastructure critique de cette désignation.
Dans les cas visés à l'article 13, § 7, la DGCC informe de cette désignation le gouverneur de la province sur le territoire de laquelle se situe l'infrastructure critique ou, lorsque cette dernière se situe sur le territoire de l'agglomération bruxelloise, l'autorité compétente en vertu de l'article 48 de la loi spéciale du 12 janvier 1989 relative aux Institutions bruxelloises.	Dans les cas visés à l'article 13, § 7, la DGCC informe de cette désignation le gouverneur de la province sur le territoire de laquelle se situe l'infrastructure critique ou, lorsque cette dernière se situe sur le territoire de l'agglomération bruxelloise, l'autorité compétente en vertu de l'article 48 de la loi spéciale du 12 janvier 1989 relative aux Institutions bruxelloises.
	Dans le cadre de l'application de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, après la désignation d'une infrastructure critique et au moins annuellement, la DGCC fournit au service désigné par le Roi, la commune dans laquelle l'infrastructure critique est située ou, le cas échéant, une liste des communes dans lesquelles les infrastructures critiques sont situées.
CHAPITRE 4 - Modifications à la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	
CHAPITRE I. - Généralités	CHAPITRE I. - Généralités
Art. 2	**Art. 2**
Dans la présente loi, il faut entendre par :	Dans la présente loi, il faut entendre par :
1° loi du 21 mars 1991 : loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;	1° loi du 21 mars 1991 : loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;
2° (abrogé)	2° (abrogé)
3° Institut : l'Institut belge des services postaux et des télécommunications, en abrégé IBPT;	3° Institut : l'Institut belge des services postaux et des télécommunications, en abrégé IBPT;
4° Ministre : le ministre ou secrétaire d'Etat qui a les services postaux ou les télécommunications dans ses attributions.	4° Ministre : le ministre ou secrétaire d'Etat qui a les services postaux ou les télécommunications dans ses attributions.
Les termes utilisés dans la présente loi ont la même signification que celle qui en est donnée dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques,	Les termes utilisés dans la présente loi ont la même signification que celle qui en est donnée dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques,

dans la loi du 13 juin 2005 relative aux communications électroniques, dans la loi du 26 janvier 2018 relative aux services postaux, ainsi que dans leurs arrêtés d'exécution.	dans la loi du 13 juin 2005 relative aux communications électroniques, dans la loi du 26 janvier 2018 relative aux services postaux, ainsi que dans leurs arrêtés d'exécution.
	5° « Données relatives à l'utilisateur final ou à l'abonné » :
	- **les données de souscription de l'abonné au service ;**
	- **les données visant à établir l'identité civile de l'abonné ou de l'utilisateur final, en ce compris les données de paiement ;**
	- **les données techniques d'identification de l'utilisateur final, de l'équipement terminal ou du service de communications électroniques, sans que ces données ne puissent donner des informations sur le destinataire de la communication, en ce compris les adresses IP du destinataire de la communication ou sur la localisation précise de l'équipement terminal ;**
	- **les données visant à déterminer le moment de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement au réseau en raison de l'extinction de cet équipement.**
CHAPITRE III. - L'Institut	CHAPITRE III. - L'Institut
Section 2. - Compétences et Missions	Section 2. - Compétences et Missions
Art. 14	**Art. 14**
§ 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes	§ 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes

d'information d'intérêt général pour la sécurité publique, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes :	d'information d'intérêt général pour la sécurité publique, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes :
1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants;	1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants;
2° la prise de décisions administratives;	2° la prise de décisions administratives;
3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :	3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :
a) la loi du 13 juin 2005 relative aux communications électroniques ;	a) la loi du 13 juin 2005 relative aux communications électroniques ;
b) le Titre Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;	b) le Titre Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;
c) la loi du 26 janvier 2018 relative aux services postaux ;	c) la loi du 26 janvier 2018 relative aux services postaux ;
d) les articles 14, § 2, 2°, et 21, §§ 5 à 7, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges ;	**d) les articles 14, § 2, 2° et 2°/1, 21, §§ 5 à 7, 25, §§ 8 à 10 et 28/1 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges ;**
e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;	e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;
f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;	f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;
g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;	g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;

h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ;	h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ;
i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.	i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.
j) tout acte juridique contraignant en droit de l'Union européenne, qui attribue des missions à l'autorité réglementaire nationale dans le secteur des postes ou des communications électroniques.	j) tout acte juridique contraignant en droit de l'Union européenne, qui attribue des missions à l'autorité réglementaire nationale dans le secteur des postes ou des communications électroniques.
Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques. Le Roi peut fixer les modalités pratiques des inspections pour ce secteur, après avis de l'Institut.	Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques. Le Roi peut fixer les modalités pratiques des inspections pour ce secteur, après avis de l'Institut.
4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, (ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale),la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure;	4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, (ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale),la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure;
4° /1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications	4° /1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications

électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, la prise de décision administrative sur base de l'article 4 ou 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;	électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, la prise de décision administrative sur base de l'article 4 ou 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;
5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications.	5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications.
6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat dans le secteur postal et dans le secteur des communications électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1erbis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion.	6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat dans le secteur postal et dans le secteur des communications électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1erbis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion.
§ 2. Dans le cadre de ses compétences, l'Institut :	§ 2. Dans le cadre de ses compétences, l'Institut :
1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques ; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des	1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques ; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des

consommateurs en matière de communications électroniques sont dûment pris en compte;	consommateurs en matière de communications électroniques sont dûment pris en compte;
2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;	2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;
	2°/1 peut exiger d'un opérateur des données relatives à l'utilisateur final ou à l'abonné ou d'autres métadonnées de communications électroniques, qui sont nécessaires à l'accomplissement de l'une de ses missions d'application et de contrôle des dispositions prévues à l'article 14, paragraphe 1er, 3°, a) et g) à i), aux conditions prévues aux articles 25, §§ 8 à 9 et 28/1, §§ 1er et 2 ;
	2°/2 peut exiger d'un opérateur de lui permettre de consulter une base de données contenant les données dont la conservation est prévue par ou en vertu des articles 122, 123, 126, 126/1 et 127 de la loi du 13 juin 2005 relative aux communications, pour le contrôle du respect par un opérateur de ces articles ou de leurs arrêtés d'exécution, aux conditions prévues aux articles 25, § 10 et 28/1, § 3.
3° coopère avec et communique de l'information à :	3° coopère avec et communique de l'information à :
a) la Commission européenne, l'ENISA, l'Office et à l'ORECE;	a) la Commission européenne, l'ENISA, l'Office et à l'ORECE;
b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;	b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;
c) les autorités de régulation des autres secteurs économiques;	c) les autorités de régulation des autres secteurs économiques;
d) les services publics fédéraux en charge de la protection des consommateurs;	d) les services publics fédéraux en charge de la protection des consommateurs;
e) les autorités belges en charge de la concurrence;	e) les autorités belges en charge de la concurrence;
Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation	Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation

et de l'échange d'informations entre ces instances et l'Institut;	et de l'échange d'informations entre ces instances et l'Institut;
f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;	f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;
g) les services publics qui ont une compétence en matière de sécurité publique, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;	g) les services publics qui ont une compétence en matière de sécurité publique, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;
h) l'Autorité de protection des données;	h) l'Autorité de protection des données;
i) le Service public fédéral chargé des statistiques et de l'information économique.	i) le Service public fédéral chargé des statistiques et de l'information économique.
4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993;	4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993;
5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques.	5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques.
6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés à l'article 6 de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 35 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ne sont plus réalisés.	6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés à l'article 6 de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 35 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ne sont plus réalisés.
L'Institut peut procéder à une même réfection lorsque la décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés :	L'Institut peut procéder à une même réfection lorsque la décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés :

- veiller à la qualité et à la pérennité du service universel	- veiller à la qualité et à la pérennité du service universel
- veiller aux intérêts des utilisateurs des services postaux;	- veiller aux intérêts des utilisateurs des services postaux;
- contribuer au développement d'un marché intérieur des services postaux ;	- contribuer au développement d'un marché intérieur des services postaux ;
- promouvoir la concurrence dans le secteur postal.	- promouvoir la concurrence dans le secteur postal.
7° peut, en sa qualité de service d'inspection, exiger à tout moment la communication du plan de sécurité de l'exploitant, en dérogation à l'article 25, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	7° peut, en sa qualité de service d'inspection, exiger à tout moment la communication du plan de sécurité de l'exploitant, en dérogation à l'article 25, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.
§ 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités.	§ 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités.
Section 4. - Les membres du personnel de l'Institut	Section 4. - Les membres du personnel de l'Institut
Sous-section 1. - Officiers de police judiciaire	Sous-section 1. - Officiers de police judiciaire
Art. 25	**Art. 25**
§ 1er. Dans le cadre du contrôle de l'utilisation du spectre, de la lutte contre les perturbations, ainsi que du contrôle du respect de la législation en matière de compatibilité électromagnétique et la conformité des équipements, les membres du personnel visés à l'article 24 peuvent, dans l'exercice de leur mission de police judiciaire :	§ 1er. Dans le cadre du contrôle de l'utilisation du spectre, de la lutte contre les perturbations, ainsi que du contrôle du respect de la législation en matière de compatibilité électromagnétique et la conformité des équipements, les membres du personnel visés à l'article 24 peuvent, dans l'exercice de leur mission de police judiciaire :
1° pénétrer à tout moment, lorsque l'accomplissement de leur mission le requiert, dans tout moyen de transport, bâtiment ou dépendance, à l'exception d'un domicile au sens de l'article 15 de la Constitution;	1° pénétrer à tout moment, lorsque l'accomplissement de leur mission le requiert, dans tout moyen de transport, bâtiment ou dépendance, à l'exception d'un domicile au sens de l'article 15 de la Constitution;

1°/1 pénétrer, munis d'un mandat du juge d'instruction, dans un domicile au sens de l'article 15 de la Constitution, dans le respect de la loi du 7 juin 1969 fixant le temps pendant lequel il ne peut être procédé à des perquisitions, visites domiciliaires ou arrestations;	1°/1 pénétrer, munis d'un mandat du juge d'instruction, dans un domicile au sens de l'article 15 de la Constitution, dans le respect de la loi du 7 juin 1969 fixant le temps pendant lequel il ne peut être procédé à des perquisitions, visites domiciliaires ou arrestations;
2° effectuer toutes les constatations utiles, se faire produire et saisir tous les documents, pièces, livres et objets nécessaires à l'instruction et à la constatation des infractions;	2° effectuer toutes les constatations utiles, se faire produire et saisir tous les documents, pièces, livres et objets nécessaires à l'instruction et à la constatation des infractions;
3° saisir tous les documents, pièces, livres et objets, pour autant que cela soit nécessaire pour mettre fin au manquement;	3° saisir tous les documents, pièces, livres et objets, pour autant que cela soit nécessaire pour mettre fin au manquement;
4° recueillir tous renseignements, recevoir toutes dépositions ou tous témoignages écrits ou oraux;	4° recueillir tous renseignements, recevoir toutes dépositions ou tous témoignages écrits ou oraux;
5° prêter leur assistance dans le cadre de l'exécution des décisions de l'Institut.	5° prêter leur assistance dans le cadre de l'exécution des décisions de l'Institut.
Lorsque ces actes ont le caractère d'une perquisition, ils ne peuvent être posés qu'en application des articles 87 à 90 du Code d'instruction criminelle.	Lorsque ces actes ont le caractère d'une perquisition, ils ne peuvent être posés qu'en application des articles 87 à 90 du Code d'instruction criminelle.
§ 2. Dans le cadre du contrôle du respect de la législation en matière de compatibilité électromagnétique et de la conformité des équipements, les membres du personnel de l'Institut visés à l'article 24 peuvent procéder à la prise d'échantillons et faire procéder à leur analyse. Le Roi, sur avis de l'Institut, en détermine les modalités.	§ 2. Dans le cadre du contrôle du respect de la législation en matière de compatibilité électromagnétique et de la conformité des équipements, les membres du personnel de l'Institut visés à l'article 24 peuvent procéder à la prise d'échantillons et faire procéder à leur analyse. Le Roi, sur avis de l'Institut, en détermine les modalités.
§ 3. A l'exception des cas visés au § 1er, les membres du personnel visés à l'article 24 peuvent, en leur qualité d'officier de police judiciaire, procéder à toutes les constatations, rassembler des informations, prendre des déclarations, se faire présenter des documents, pièces, livres et objets et saisir ceux qui sont nécessaires à la recherche ou à la constatation ou nécessaires pour pouvoir mettre fin au manquement. Ils peuvent procéder à des perquisitions ou entreprendre toutes les actions nécessaires pour constater une infraction à la législation dont ils contrôlent le respect.	§ 3. A l'exception des cas visés au § 1er, les membres du personnel visés à l'article 24 peuvent, en leur qualité d'officier de police judiciaire, procéder à toutes les constatations, rassembler des informations, prendre des déclarations, se faire présenter des documents, pièces, livres et objets et saisir ceux qui sont nécessaires à la recherche ou à la constatation ou nécessaires pour pouvoir mettre fin au manquement. Ils peuvent procéder à des perquisitions ou entreprendre toutes les actions nécessaires pour constater une infraction à la législation dont ils contrôlent le respect.

Toute perquisition se fait dans le respect des dispositions du Code d'instruction criminelle.	Toute perquisition se fait dans le respect des dispositions du Code d'instruction criminelle.
L'accord du juge d'instruction est nécessaire pour procéder à une perquisition :	L'accord du juge d'instruction est nécessaire pour procéder à une perquisition :
1° au domicile des chefs d'entreprises, administrateurs, gérants, directeurs et autres membres du personnel de l'entreprise concernée ainsi qu'au domicile et dans les locaux utilisés à des fins professionnelles de personnes physiques et morales, internes ou externes, chargées des la gestion commerciale, comptable, administrative, fiscale et financière de cette entreprise;	1° au domicile des chefs d'entreprises, administrateurs, gérants, directeurs et autres membres du personnel de l'entreprise concernée ainsi qu'au domicile et dans les locaux utilisés à des fins professionnelles de personnes physiques et morales, internes ou externes, chargées des la gestion commerciale, comptable, administrative, fiscale et financière de cette entreprise;
2° au siège social ou d'exploitation de l'entreprise concernée.	2° au siège social ou d'exploitation de l'entreprise concernée.
§ 4. Les procès-verbaux des officiers de police judiciaire font foi jusqu'à preuve du contraire.	§ 4. Les procès-verbaux des officiers de police judiciaire font foi jusqu'à preuve du contraire.
§ 5. Dans l'exercice de leurs missions de recherche ou de constatation d'infractions, les officiers de police judiciaire sont soumis à la surveillance du procureur général.	§ 5. Dans l'exercice de leurs missions de recherche ou de constatation d'infractions, les officiers de police judiciaire sont soumis à la surveillance du procureur général.
§ 6. Les officiers de police judiciaire peuvent, pour les besoins de l'accomplissement de leurs missions, requérir la force publique et bénéficier de tous les moyens reconnus aux agents de la force publique.	§ 6. Les officiers de police judiciaire peuvent, pour les besoins de l'accomplissement de leurs missions, requérir la force publique et bénéficier de tous les moyens reconnus aux agents de la force publique.
§ 7. Sans préjudice des lois particulières qui garantissent le secret des déclarations, les administrations publiques sont tenues de prêter leur concours aux officiers de police judiciaire dans l'exécution de leurs missions.	§ 7. Sans préjudice des lois particulières qui garantissent le secret des déclarations, les administrations publiques sont tenues de prêter leur concours aux officiers de police judiciaire dans l'exécution de leurs missions.
	§ 8. Pour les besoins de l'accomplissement de leurs missions, les officiers de police judiciaire de l'Institut peuvent exiger d'un opérateur de leur fournir des données relatives à l'utilisateur final ou à l'abonné conservées par l'opérateur, qui sont nécessaires afin de rechercher, de constater ou de poursuivre une infraction à une loi visée à l'article 24, lorsque celle-ci est commise au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications au

	sens de la loi du 13 juin 2005 relative aux communications électroniques.
	L'officier de police judiciaire soumet sa demande motivée à l'autorisation préalable de son supérieur hiérarchique.
	§ 9. Pour les besoins de l'accomplissement de leurs missions, les officiers de police judiciaire de l'Institut peuvent exiger d'un opérateur de leur fournir des métadonnées de communications électroniques autres que les données relatives à l'utilisateur final ou à l'abonné, qui sont nécessaires afin de rechercher, de constater ou de poursuivre une infraction à une loi visée à l'article 24, lorsque celle-ci est commise au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications au sens de la loi du 13 juin 2005 relative aux communications électroniques.
	L'officier de police judiciaire soumet sa demande motivée à l'autorisation préalable du juge d'instruction, sauf cas d'urgence dûment justifié.
	En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction la demande envoyée à l'opérateur sans délai après cet envoi. Un contrôle ultérieur est effectué par le juge d'instruction.
	§ 10. Par dérogation aux paragraphes 8 et 9, à la demande d'un officier de police judiciaire de l'Institut et après autorisation du Conseil de l'Institut, un opérateur permet à cet officier de consulter ses bases de données qui mettent en œuvre les articles 126, 126/1 et 127 de la loi du 13 juin 2005 relative aux communications électroniques, afin de contrôler le respect de ces articles et de leurs arrêtés d'exécution.
	Ces officiers ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

	§ 11. Les officiers de police judiciaire de l'Institut consignent les demandes visées aux paragraphes 8, 9 et 10 dans un inventaire.
	Art. 28/1
	§ 1er. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), les membres du personnel de l'Institut, qui n'agissent pas dans un cadre pénal, peuvent exiger d'un opérateur de leur fournir des données relatives à l'utilisateur final ou à l'abonné conservées par l'opérateur.
	Le membre du personnel soumet sa demande motivée à l'autorisation préalable de son supérieur hiérarchique.
	§ 2. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), les membres du personnel de l'Institut, qui n'agissent pas dans un cadre pénal, peuvent exiger d'un opérateur de leur fournir des métadonnées de communications électroniques conservées par l'opérateur, autres que les données relatives à l'utilisateur final ou à l'abonné.
	Il soumet préalablement sa demande motivée à l'approbation de l'Autorité de protection des données, sauf cas d'urgence dûment justifié. En cas d'urgence dûment justifiée, il communique à l'Autorité de protection des données, la demande envoyée à l'opérateur sans délai après cet envoi. Un contrôle ultérieur est effectué par l'Autorité de protection des données.
	§ 3. L'alinéa 2 du paragraphe 2 n'est pas applicable lorsque l'Institut contrôle le respect par un opérateur des articles 122 et 123 de la loi du 13 juin 2005 relative aux communications électroniques, en consultant si nécessaire les bases de données qui mettent en œuvre ces articles.
	§ 4. Les demandes qui sont formulées conformément aux paragraphes 1er, 2 et 3 sont consignées dans un inventaire tenu auprès de l'Institut.

CHAPITRE 5 – Modifications au Code d'instruction criminelle	
Art. 88bis	**Art. 88bis**
§ 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder:	§ 1er. S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder:
1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;	1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;
2° à la localisation de l'origine ou de la destination de communications électroniques.	2° à la localisation de l'origine ou de la destination de communications électroniques.
Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:	Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:
- de l'opérateur d'un réseau de communications électroniques; et	- de l'opérateur d'un réseau de communications électroniques; et
- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.	- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.
Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.	Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.	Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.
Il précise également la durée durant laquelle la mesure pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2.	Il précise également la durée durant laquelle la mesure pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2.
En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.	En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.
S'il s'agit toutefois de l'infraction visée à l'article 137, 347bis, 434 ou 470 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire.	S'il s'agit toutefois de l'infraction visée à l'article 137, 347bis, 434 ou 470 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire.
S'il s'agit de l'infraction visée à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut en outre ordonner la mesure dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction soit nécessaire.	S'il s'agit de l'infraction visée à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut en outre ordonner la mesure dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction soit nécessaire.
Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques.	Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3bis de la loi du 13 juin 2005 relative aux communications électroniques.
En cas d'urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 4 et 5.	En cas d'urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 4 et 5.
§ 2. (annulé par la Cour Constitutionnelle)	**§ 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées**

	sur la base de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent :
	- pour une infraction visée au livre II, titre Iter, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;
	- pour une autre infraction visée à l'article 90ter, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;
	- pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.
§ 3. (partiellement annulé par la Cour Constitutionnelle)	§ 3. **La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.**
Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.	**La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.**
§ 4. Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en	§ 4. Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en

temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.	temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.
Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.	Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.
Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à dix mille euros.]	Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de vingt-six euros à dix mille euros.]
CHAPITRE 6 - Modifications à la loi du 5 août 1992 sur la fonction de police	
Art. 42	**Art. 42**
Lorsqu'il est mis en danger dans l'exercice de sa mission ou lorsque des personnes sont en danger, tout membre du cadre opérationnel peut requérir l'aide ou l'assistance des personnes présentes sur place. En cas d'absolue nécessité, il peut de même requérir l'aide ou l'assistance de toute autre personne utile.	***§ 1er.*** Lorsqu'il est mis en danger dans l'exercice de sa mission ou lorsque des personnes sont en danger, tout membre du cadre opérationnel peut requérir l'aide ou l'assistance des personnes présentes sur place. En cas d'absolue nécessité, il peut de même requérir l'aide ou l'assistance de toute autre personne utile.
L'aide ou l'assistance requise ne peut mettre en danger la personne qui la prête.	L'aide ou l'assistance requise ne peut mettre en danger la personne qui la prête.
	§ 2. Un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue.
	Seules les données visant à identifier l'utilisateur ou l'abonné et les moyens de

	communication et relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, concernant la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données, sont communiquées.
	La réquisition est adressée par l'officier de police judiciaire visé à paragraphe 2, alinéa 1er, à :
	- **l'opérateur d'un réseau de communications électroniques ; ou**
	- **toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.**
	§ 3. La réquisition et sa justification sont notifiées par la Cellule Personnes Disparues à l'Organe de contrôle, au plus tard dans les 48 heures après la réquisition.
	Si l'Organe de contrôle estime que les conditions pour effectuer cette réquisition ne sont pas remplies, il ordonne, de manière motivée, l'interdiction d'exploiter les données obtenues par ce moyen et l'effacement des données.
	Cette décision motivée est notifiée dans les meilleurs délais possibles par l'Organe de contrôle à la Cellule Personnes Disparues.
CHAPITRE 7 - Modifications à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité	
Article 3	**Article 3**
La présente loi entend par :	La présente loi entend par :

1° "Conseil national de sécurité" : le Conseil créé au sein du Gouvernement, qui est chargé des tâches de sécurité nationale déterminées par le Roi ;	1° "Conseil national de sécurité" : le Conseil créé au sein du Gouvernement, qui est chargé des tâches de sécurité nationale déterminées par le Roi ;
2° "agent": tout membre du personnel statutaire ou contractuel et tout militaire exerçant ses fonctions au sein des services de renseignement et de sécurité visés à l'article 2 ;	2° "agent": tout membre du personnel statutaire ou contractuel et tout militaire exerçant ses fonctions au sein des services de renseignement et de sécurité visés à l'article 2 ;
3° "membre de l'équipe d'intervention" :	3° "membre de l'équipe d'intervention" :
a) pour la Sûreté de l'Etat, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens de la Sûreté de l'Etat ;	a) pour la Sûreté de l'Etat, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens de la Sûreté de l'Etat ;
b) pour le Service Général du Renseignement et de la Sécurité, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens du Service Général du Renseignement et de la Sécurité ;	b) pour le Service Général du Renseignement et de la Sécurité, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens du Service Général du Renseignement et de la Sécurité ;
4° "Service Général du Renseignement et de la Sécurité" : le Service Général du Renseignement et de la Sécurité.	4° "Service Général du Renseignement et de la Sécurité" : le Service Général du Renseignement et de la Sécurité.
5° "le Ministre" : le Ministre de la Justice en ce qui concerne la Sûreté de l'Etat, et le Ministre de la Défense en ce qui concerne le Service Général du Renseignement et de la Sécurité ;	5° "le Ministre" : le Ministre de la Justice en ce qui concerne la Sûreté de l'Etat, et le Ministre de la Défense en ce qui concerne le Service Général du Renseignement et de la Sécurité ;
6° "la commission" : la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, créée par l'article 43/1 ;	6° "la commission" : la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, créée par l'article 43/1 ;
7° "le Comité permanent R" : le Comité permanent de contrôle des services de renseignement visé dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace ;	7° "le Comité permanent R" : le Comité permanent de contrôle des services de renseignement visé dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace ;
8° "le dirigeant du service" : d'une part, l'administrateur général de la Sûreté de l'Etat ou, en cas d'empêchement, l'administrateur général faisant fonction et, d'autre part, le chef du Service Général du Renseignement et de la	8° "le dirigeant du service" : d'une part, l'administrateur général de la Sûreté de l'Etat ou, en cas d'empêchement, l'administrateur général faisant fonction et, d'autre part, le chef du Service Général du Renseignement et de la

Sécurité ou, en cas d'empêchement, le chef faisant fonction ;	Sécurité ou, en cas d'empêchement, le chef faisant fonction ;
9° "l'officier de renseignement" :	9° "l'officier de renseignement" :
a) pour la Sûreté de l'Etat, l'agent revêtu au moins du grade de commissaire ;	a) pour la Sûreté de l'Etat, l'agent revêtu au moins du grade de commissaire ;
b) pour le Service Général du Renseignement et de la Sécurité, l'officier affecté à ce service, ainsi que l'agent civil revêtu au moins du grade de commissaire ;	b) pour le Service Général du Renseignement et de la Sécurité, l'officier affecté à ce service, ainsi que l'agent civil revêtu au moins du grade de commissaire ;
10° "communications" : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radio-électricité, signalisation optique ou un autre système électromagnétique; les communications par téléphone, GSM, mobilophone, télex, télécopieur ou la transmission électronique de données par ordinateur ou réseau informatique, ainsi que toute autre communication privée ;	10° "communications" : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radio-électricité, signalisation optique ou un autre système électromagnétique; les communications par téléphone, GSM, mobilophone, télex, télécopieur ou la transmission électronique de données par ordinateur ou réseau informatique, ainsi que toute autre communication privée**, quelle que soit la nature de l'émetteur ou du récepteur** ;
11° "réseaux de communications électroniques" : les réseaux de communications électroniques visés à l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques ;	11° "réseaux de communications électroniques" : les réseaux de communications électroniques visés à l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques ;
11° /1 "fournisseur d'un service de communications électroniques" : quiconque qui, de quelque manière que ce soit, met à disposition ou offre, sur le territoire belge, un service qui consiste en la transmission de signaux via des réseaux de communications électroniques ou qui permet aux utilisateurs, via un réseau de communications électroniques, d'obtenir, de recevoir ou de diffuser des informations ;	11° /1 "fournisseur d'un service de communications électroniques" : quiconque qui, de quelque manière que ce soit, met à disposition ou offre, sur le territoire belge, un service qui consiste en la transmission de signaux via des réseaux de communications électroniques ou qui permet aux utilisateurs, via un réseau de communications électroniques, d'obtenir, de recevoir ou de diffuser des informations ;
12° "lieu accessible au public" : tout lieu, public ou privé, auquel le public peut avoir accès ;	12° "lieu accessible au public" : tout lieu, public ou privé, auquel le public peut avoir accès ;
12° /1 "lieu non accessible au public non soustrait à la vue" : tout lieu auquel le public n'a pas accès et qui est visible de tous à partir de la voie publique sans moyen ou artifice, à	12° /1 "lieu non accessible au public non soustrait à la vue" : tout lieu auquel le public n'a pas accès et qui est visible de tous à partir de la voie publique sans moyen ou artifice, à

l'exception de l'intérieur des bâtiments non accessibles au public ;	l'exception de l'intérieur des bâtiments non accessibles au public ;
13° "courrier" : l'envoi postal tel qu'il est défini à l'article 131, 6°, 7° et 11°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;	13° "courrier" : l'envoi postal tel qu'il est défini à l'article 131, 6°, 7° et 11°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;
14° " moyen technique " : une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception d' :	14° " moyen technique " : une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception d' :
a) un appareil utilisé pour la prise de photographies ;	a) un appareil utilisé pour la prise de photographies ;
b) un appareil mobile utilisé pour la prise d'images animées lorsque la prise de photographies ne permet pas de garantir la discrétion et la sécurité des agents et à la condition que cette utilisation ait été préalablement autorisée par le dirigeant du service ou son délégué. Seules les images fixes jugées pertinentes sont conservées. Les autres images sont détruites dans le mois qui suit le jour de l'enregistrement ;	b) un appareil mobile utilisé pour la prise d'images animées lorsque la prise de photographies ne permet pas de garantir la discrétion et la sécurité des agents et à la condition que cette utilisation ait été préalablement autorisée par le dirigeant du service ou son délégué. Seules les images fixes jugées pertinentes sont conservées. Les autres images sont détruites dans le mois qui suit le jour de l'enregistrement ;
15° "processus de radicalisation" : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ;	15° "processus de radicalisation" : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ;
16° "journaliste" : le journaliste admis à porter le titre de journaliste professionnel conformément à la loi du 30 décembre 1963 relative à la reconnaissance et à la protection du titre de journaliste professionnel ;	16° "journaliste" : le journaliste admis à porter le titre de journaliste professionnel conformément à la loi du 30 décembre 1963 relative à la reconnaissance et à la protection du titre de journaliste professionnel ;
17° "secret des sources" : le secret tel qu'il est défini dans la loi du 7 avril 2005 relative à la protection des sources journalistes ;	17° "secret des sources" : le secret tel qu'il est défini dans la loi du 7 avril 2005 relative à la protection des sources journalistes ;
18° "Directeur des Opérations de la Sûreté de l'Etat" : l'agent des services extérieurs de la Sûreté de l'Etat revêtu du grade de commissaire général qui est chargé de la direction des services extérieurs de la Sûreté de l'Etat ;	18° "Directeur des Opérations de la Sûreté de l'Etat" : l'agent des services extérieurs de la Sûreté de l'Etat revêtu du grade de commissaire général qui est chargé de la direction des services extérieurs de la Sûreté de l'Etat ;
19° "objet verrouillé" : un objet dont l'ouverture nécessite une fausse clé ou une effraction ;	19° "objet verrouillé" : un objet dont l'ouverture nécessite une fausse clé ou une effraction ;

20° "observation" : la surveillance d'une ou de plusieurs personnes, de leur présence ou de leur comportement, de choses, lieux ou événements ;	20° "observation" : la surveillance d'une ou de plusieurs personnes, de leur présence ou de leur comportement, de choses, lieux ou événements ;
21° "inspection" : la pénétration, l'examen et la fouille d'un lieu ainsi que l'examen et la fouille d'un objet.	21° "inspection" : la pénétration, l'examen et la fouille d'un lieu ainsi que l'examen et la fouille d'un objet.
Article 7	**Article 7**
La Sûreté de l'Etat a pour mission :	La Sûreté de l'Etat**, chargée de la sécurité nationale,** a pour mission :
1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité]1, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité ;	1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité]1, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité ;
2° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Conseil national de sécurité ;	2° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Conseil national de sécurité ;
3° […]	3° […]
3° /1 de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge ;	3° /1 de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge ;
4° d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi.	4° d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi.
Article 11	**Article 11**
§1er. Le Service Général du Renseignement et de la Sécurité a pour mission :	§1er. Le Service Général du Renseignement et de la Sécurité **, chargé de la sécurité nationale,** a pour mission :
1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les	1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les

Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer :	Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer :
a) l'intégrité du territoire national ou la population,	a) l'intégrité du territoire national ou la population,
b) les plans de défense militaires,	b) les plans de défense militaires,
c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,	c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,
d) l'accomplissement des missions des Forces armées,	d) l'accomplissement des missions des Forces armées,
e) la sécurité des ressortissants belges à l'étranger,	e) la sécurité des ressortissants belges à l'étranger,
f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité ;	f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité ;
et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense ;	et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense ;
2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre	2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre

cyberattaque, dans le respect des dispositions du droit des conflits armés ;	cyberattaque, dans le respect des dispositions du droit des conflits armés ;
3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère ;	3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère ;
4° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Conseil national de sécurité.	4° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Conseil national de sécurité.
5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge.	5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge.
§ 2. Pour l'application du § 1er, on entend par :	§ 2. Pour l'application du § 1er, on entend par :
1° "activité qui menace ou pourrait menacer l'intégrité du territoire national ou la population" : toute manifestation de l'intention de, par des moyens de nature militaire, saisir, occuper ou agresser tout ou partie du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale, ou porter atteinte à la protection ou à la survie de tout ou partie de la population, au patrimoine national ou au potentiel économique du pays ;	1° "activité qui menace ou pourrait menacer l'intégrité du territoire national ou la population" : toute manifestation de l'intention de, par des moyens de nature militaire, saisir, occuper ou agresser tout ou partie du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale, ou porter atteinte à la protection ou à la survie de tout ou partie de la population, au patrimoine national ou au potentiel économique du pays ;
2° "activité qui menace ou pourrait menacer les plans de défense militaires" : toute manifestation de l'intention de prendre connaissance par voie illicite des plans relatifs à la défense militaire du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale et des intérêts vitaux de l'Etat, ou à la défense militaire commune dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale ;	2° "activité qui menace ou pourrait menacer les plans de défense militaires" : toute manifestation de l'intention de prendre connaissance par voie illicite des plans relatifs à la défense militaire du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale et des intérêts vitaux de l'Etat, ou à la défense militaire commune dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale ;
2°/1 "activité qui menace ou pourrait menacer le potentiel scientifique et économique en rapport avec les acteurs, tant personnes	2°/1 "activité qui menace ou pourrait menacer le potentiel scientifique et économique en rapport avec les acteurs, tant personnes

physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du Ministre de la Justice et du Ministre de la Défense" : toute manifestation de l'intention de porter atteinte aux éléments essentiels du potentiel scientifique et économique de ces acteurs ;	physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du Ministre de la Justice et du Ministre de la Défense" : toute manifestation de l'intention de porter atteinte aux éléments essentiels du potentiel scientifique et économique de ces acteurs ;
3° "activité qui menace ou pourrait menacer l'accomplissement des missions des Forces armées" : toute manifestation de l'intention de neutraliser, d'entraver, de saboter, de porter atteinte ou d'empêcher la mise en condition, la mobilisation et la mise en œuvre des Forces armées belges, des Forces armées alliées ou des organismes de défense interalliés lors de missions, actions ou opérations dans le cadre national, dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale ;	3° "activité qui menace ou pourrait menacer l'accomplissement des missions des Forces armées" : toute manifestation de l'intention de neutraliser, d'entraver, de saboter, de porter atteinte ou d'empêcher la mise en condition, la mobilisation et la mise en œuvre des Forces armées belges, des Forces armées alliées ou des organismes de défense interalliés lors de missions, actions ou opérations dans le cadre national, dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale ;
4° "activité qui menace ou pourrait menacer la sécurité des ressortissants belges à l'étranger" : toute manifestation de l'intention de porter collectivement atteinte à la vie ou à l'intégrité physique de ressortissants belges à l'étranger et des membres de leur famille.	4° "activité qui menace ou pourrait menacer la sécurité des ressortissants belges à l'étranger" : toute manifestation de l'intention de porter collectivement atteinte à la vie ou à l'intégrité physique de ressortissants belges à l'étranger et des membres de leur famille.
§ 3. A la requête du Service Général du Renseignement et de la Sécurité, la Sûreté de l'Etat prête son concours pour recueillir le renseignement lorsque des personnes qui ne relèvent pas du Ministre de la Défense nationale ou qui ne relèvent pas d'entreprises qui exécutent des contrats conclus avec lui, avec des organisations militaires internationales ou avec des pays tiers en matière militaire, ou qui participent à une procédure de passation de marché public lancée par ceux-ci, sont impliquées dans les activités visées au paragraphe 1er, 1°, 2°, 3° et 5°.	§ 3. A la requête du Service Général du Renseignement et de la Sécurité, la Sûreté de l'Etat prête son concours pour recueillir le renseignement lorsque des personnes qui ne relèvent pas du Ministre de la Défense nationale ou qui ne relèvent pas d'entreprises qui exécutent des contrats conclus avec lui, avec des organisations militaires internationales ou avec des pays tiers en matière militaire, ou qui participent à une procédure de passation de marché public lancée par ceux-ci, sont impliquées dans les activités visées au paragraphe 1er, 1°, 2°, 3° et 5°.
Les mesures de protection industrielle ne seront prises qu'à la demande du Ministre de la Défense nationale, de pays tiers ou des organisations avec lesquelles la Belgique est liée par traité, convention ou contrat.	Les mesures de protection industrielle ne seront prises qu'à la demande du Ministre de la Défense nationale, de pays tiers ou des organisations avec lesquelles la Belgique est liée par traité, convention ou contrat.
	Section 3/1 - Réquisitions de conservation

	Article 13/6
	§1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :
	1° la conservation des données de trafic et de localisation de moyens de communications électroniques qui sont à sa disposition au moment de la réquisition;
	2° la conservation des données de trafic et de localisation qu'il génère et traite à partir de la réquisition.
	La réquisition visée à l'alinéa 1er repose sur une décision écrite et motivée du dirigeant du service ou de son délégué.
	§2. La réquisition est adressée à l'opérateur ou au fournisseur visé au §1er, alinéa 1er et mentionne :
	1° la nature des données de trafic et de localisation qui doivent être conservées ;
	2° les personnes, les groupements, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation doivent être conservées ;
	3° pour la mesure visée au §1er, alinéa 1er, 1°, le délai de conservation des données qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure ;
	4° pour la mesure visée au §1er, alinéa 1er, 2° :
	- la durée de la mesure qui ne peut excéder six mois à compter de la date de la réquisition sans préjudice de la possibilité de prolongation en suivant la même procédure ;
	- le délai de conservation qui ne peut excéder six mois à compter de la date de la

	communication sans préjudice de la possibilité de prolongation en suivant la même procédure ;
	5° la date de la réquisition ;
	6° la signature du dirigeant du service ou de son délégué ;
	§3. En cas d'urgence, le dirigeant du service ou son délégué peut requérir la conservation verbalement. Cette réquisition verbale est confirmée par écrit au plus tard le premier jour ouvrable qui suit.
	§4. Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.
	Chaque décision de réquisition est notifiée avec sa motivation au Comité permanent R. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la réquisition.
	Lorsqu'il est mis fin prématurément à la réquisition, l'opérateur d'un réseau de communications électroniques ou le fournisseur d'un service de communications électroniques requis en est averti le plus rapidement possible.
	§5. Pour l'exécution de la réquisition, le dirigeant du service ou son délégué peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale.
	§6. Toute personne qui refuse de prêter son concours aux réquisitions visées aux § § 1er et 5 est punie d'une amende de vingt-six euros à vingt mille euros.
	§7. Le Roi peut déterminer, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs et des fournisseurs.

	Article 13/7
	§1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs d'un réseau de communications électroniques et des fournisseurs d'un service de communications électroniques afin de procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traitées par eux.
	§2. La réquisition visée au § 1er ne peut avoir lieu qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.
	§3. La demande du dirigeant du service de requérir la conservation mentionne, sous peine d'illégalité :
	1° la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible ;
	2° les circonstances de fait qui justifient la conservation généralisée et indifférenciée des données de trafic et de localisation ;
	3° la nature des données de trafic et de localisation qui doivent être conservées ;
	4° la durée de la mesure de conservation qui ne peut excéder six mois à compter de la date de la réquisition. Elle peut être prolongée en suivant la même procédure ;
	5° le délai de conservation des données qui ne peut excéder six mois à compter de la date de la communication. Elle peut être prolongée en suivant la même procédure ;
	6° le cas échéant, les motifs qui justifient l'extrême urgence visée au § 5 ;

	7° la date de la demande ;
	8° la signature du dirigeant du service.
	§4. La réquisition est adressée aux opérateurs et aux fournisseurs visés au §1er et mentionne :
	1° la date de l'accord de la Commission ;
	2° la nature des données de trafic et de localisation qui doivent être conservées ;
	3° la durée de la mesure et le délai de conservation des données ;
	4° la date de la réquisition ;
	5° la signature du dirigeant du service ou de son délégué.
	§5. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, en cas d'indisponibilité, d'un autre membre de la Commission. L'auteur de l'accord en informe immédiatement les autres membres de la Commission. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant l'accord. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.
	§6. La réquisition de conservation généralisée et indifférenciée est confirmée par arrêté royal.
	L'arrêté royal ne mentionne que :
	1° la date de l'accord de la Commission ;
	2° la date de la réquisition ;
	3° la nature des données de trafic et de localisation qui doivent être conservées ;
	4° la durée de la mesure et le délai de conservation des données ;

	En l'absence de confirmation par arrêté royal dans le mois de la réquisition, cette réquisition prend fin.
	Les opérateurs d'un réseau de communications électroniques et les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.
	§7. Pour l'exécution de la réquisition, le dirigeant du service peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale et l'accord de la Commission.
	§8. Toute personne qui refuse de prêter son concours aux réquisitions visées aux § § 1er et 7 est punie d'une amende de vingt-six euros à vingt mille euros.
	§9. La Commission transmet sans délai la demande du dirigeant du service et son accord au Comité permanent R.
	§10. Le service de renseignement et de sécurité fait rapport à la Commission toutes les deux semaines sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.
	§11. Le dirigeant du service met fin à la réquisition, nonobstant la confirmation par arrêté royal, lorsque la conservation n'est plus utile pour lutter contre la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, lorsque cette menace a disparu ou lorsqu'il constate une illégalité.
	Lorsque la Commission ou le Comité permanent R constate une illégalité, il est mis fin à la réquisition nonobstant la confirmation par arrêté royal.
	Lorsqu'il est mis fin prématurément à la réquisition, les opérateurs d'un réseau de communications électroniques ou les

	fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.
	§12. Le Roi détermine, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs et des fournisseurs.
Article 18/7	**Article 18/7**
§ 1er. Dans l'intérêt de l'exercice des missions, le dirigeant du service peut, par une décision écrite, procéder ou faire procéder à :	§1er. **Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions**, procéder ou faire procéder à :
1° l'identification ou la localisation, à l'aide d'un moyen technique, des services et des moyens de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée ;	1° l'identification ou la localisation, à l'aide d'un moyen technique, des services et des moyens de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée ;
2° la réquisition de l'opérateur d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, l'identification du moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques. Un service de renseignement et de sécurité peut également obtenir les données visées au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur du service.	2° la réquisition de l'opérateur d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques afin d'obtenir **la communication des factures afférentes aux abonnements identifiés,** les données relatives à la méthode de paiement, l'identification du moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques. Un service de renseignement et de sécurité peut également obtenir les données visées au moyen d'un accès aux fichiers des clients de l'opérateur ou du fournisseur du service.
§ 2. [...]	§ 2. [...]
§3. Tout opérateur d'un réseau de communications et tout fournisseur d'un service de communications qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et suivant les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les	§3. Tout opérateur d'un réseau de communications et tout fournisseur d'un service de communications qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et suivant les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les

communications électroniques dans ses attributions.	communications électroniques dans ses attributions.
Le Roi fixe, sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les communications électroniques dans ses attributions, les conditions auxquelles l'accès visé au § 1er est possible pour le dirigeant du service.	Le Roi fixe, sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les communications électroniques dans ses attributions, les conditions auxquelles l'accès visé au § 1er est possible pour **le service concerné**.
Toute personne visée à l'alinéa 1er qui refuse de communiquer les données ainsi demandées est punie d'une amende de vingt-six euros à vingt mille euros.	Toute personne visée à l'alinéa 1er qui refuse de communiquer les données ainsi demandées est punie d'une amende de vingt-six euros à vingt mille euros.
Article 18/8	**Article 18/8**
§1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique, procéder ou faire procéder :	§1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique, procéder ou faire procéder :
1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées ;	1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées ;
2° à la localisation de l'origine ou de la destination de communications électroniques.	2° à la localisation de l'origine ou de la destination de communications électroniques.
Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les [données de trafic] sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.	Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les [données de trafic] sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.
La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.	La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.
§2. Pour ce qui concerne l'application de la méthode visée au paragraphe 1er aux données conservées sur la base de l'article 126 de la loi	**§2. [Annulé par la Cour Constitutionnelle]**

du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent :	
1° pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut dans sa décision requérir les données que pour une période de six mois préalable à la décision ;	
2° pour une menace potentielle autre que celles visées sous le 1° et le 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision ;	
3° pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision	
§3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les Communications électroniques dans ses attributions.	§3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au § 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du Ministre de la Justice, du Ministre de la Défense et du Ministre qui a les Communications électroniques dans ses attributions.
Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à vingt mille euros.	Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à vingt mille euros.
§4. […]	§4. […]
Article 18/14	**Article 18/14**
§1er. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent ouvrir un courrier confié ou non à un opérateur postal et prendre connaissance de son contenu.	§1er. **Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions,** ouvrir un courrier confié ou non à un opérateur postal et prendre connaissance de son contenu.

L'opérateur postal visé à l'alinéa 1er est tenu de remettre le courrier auquel l'autorisation se rapporte, contre récépissé, à un agent du service, sur présentation de sa carte de légitimation et d'une demande écrite du dirigeant du service. Cette demande mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.	L'opérateur postal visé à l'alinéa 1er est tenu de remettre le courrier auquel l'autorisation se rapporte, contre récépissé, à un agent du service, sur présentation de sa carte de légitimation et d'une demande écrite du dirigeant du service. Cette demande mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.
§2. Les services veillent à ce qu'un envoi postal remis par un opérateur postal soit rendu sans délai, après son examen, à l'opérateur de la poste pour expédition ultérieure.	§2. Les services veillent à ce qu'un envoi postal remis par un opérateur postal soit rendu sans délai, après son examen, à l'opérateur de la poste pour expédition ultérieure.
§3. L'opérateur postal qui refuse de prêter le concours visé aux § § 1er et 2 est puni d'une amende de vingt-six euros à vingt mille euros.	§3. L'opérateur postal qui refuse de prêter le concours visé aux § § 1er et 2 est puni d'une amende de vingt-six euros à vingt mille euros.
§4. L'Etat est civilement responsable vis-à-vis de l'opérateur postal en cas de dommage causé au courrier qui lui a été confié.	§4. L'Etat est civilement responsable vis-à-vis de l'opérateur postal en cas de dommage causé au courrier qui lui a été confié.
Article 18/17	**Article 18/17**
§1er. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent intercepter des communications, en prendre connaissance et les enregistrer.	§1er. **Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions** intercepter des communications, en prendre connaissance et les enregistrer.
§2. A cet effet, les services de renseignement et de sécurité peuvent pénétrer, à tout moment, à l'insu du propriétaire ou de son ayant droit ou sans le consentement de ceux-ci, dans des lieux accessibles ou non au public afin d' :	§2. A cet effet, les services de renseignement et de sécurité peuvent pénétrer, à tout moment, à l'insu du propriétaire ou de son ayant droit ou sans le consentement de ceux-ci, dans des lieux accessibles ou non au public afin d' :
1° installer un moyen technique, intervenir sur ce moyen ou le retirer ;	1° installer un moyen technique, intervenir sur ce moyen ou le retirer ;
2° ouvrir un objet verrouillé pour y placer un moyen technique ;	2° ouvrir un objet verrouillé pour y placer un moyen technique ;
3° emporter l'objet sur lequel sera installé le moyen technique, intervenir sur cet objet et le replacer.	3° emporter l'objet sur lequel sera installé le moyen technique, intervenir sur cet objet et le replacer.
Le moyen technique est retiré ou l'objet emporté est remis en place le plus rapidement possible à l'échéance de l'interception, à moins	Le moyen technique est retiré ou l'objet emporté est remis en place le plus rapidement possible à l'échéance de l'interception, à moins

que cela n'entrave le bon déroulement de la mission.	que cela n'entrave le bon déroulement de la mission.
§3. Si une opération sur un réseau de communications électroniques est nécessaire, l'opérateur du réseau ou le fournisseur d'une service de communications électroniques est saisi d'une demande écrite du dirigeant du service et est tenu de prêter son concours technique à la suite de cette demande. Cette demande mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.	§3. Si une opération sur un réseau de communications électroniques est nécessaire, l'opérateur du réseau ou le fournisseur d'une service de communications électroniques est saisi d'une demande écrite du dirigeant du service et est tenu de prêter son concours technique à la suite de cette demande. Cette demande mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.
Toute personne qui refuse de prêter son concours technique aux réquisitions visées à l'alinéa 1er est punie d'une amende de vingt-six euros à vingt mille euros. Les modalités et délais de ce concours technique sont déterminés par le Roi, sur la proposition des Ministres de la Justice et de la Défense et du Ministre qui a les Communications électroniques dans ses attributions.	Toute personne qui refuse de prêter son concours technique aux réquisitions visées à l'alinéa 1er est punie d'une amende de vingt-six euros à vingt mille euros. Les modalités et délais de ce concours technique sont déterminés par le Roi, sur la proposition des Ministres de la Justice et de la Défense et du Ministre qui a les Communications électroniques dans ses attributions.
§4. Les communications recueillies grâce à la méthode exceptionnelle visée au § 1er sont enregistrées. L'objet de la méthode exceptionnelle ainsi que les jours et heures où celle-ci a été exécutée sont enregistrés au début et à la fin de chaque enregistrement qui s'y rapporte.	§4. Les communications recueillies grâce à la méthode exceptionnelle visée au § 1er sont enregistrées. L'objet de la méthode exceptionnelle ainsi que les jours et heures où celle-ci a été exécutée sont enregistrés au début et à la fin de chaque enregistrement qui s'y rapporte.
Seules les parties d'enregistrement des communications estimées pertinentes par le dirigeant du service ou, selon le cas, en son nom, par le directeur des opérations ou la personne qu'il a désignée à cet effet pour la Sûreté de l'Etat, ou l'officier ou l'agent civil, ayant au moins le grade de commissaire de sécurité pour le Service Général du Renseignement et de la Sécurité, peuvent faire l'objet d'une transcription.	Seules les parties d'enregistrement des communications estimées pertinentes par le dirigeant du service ou, selon le cas, en son nom, par le directeur des opérations ou la personne qu'il a désignée à cet effet pour la Sûreté de l'Etat, ou l'officier ou l'agent civil, ayant au moins le grade de commissaire de sécurité pour le Service Général du Renseignement et de la Sécurité, peuvent faire l'objet d'une transcription.
Toute note prise dans le cadre de l'exécution de la méthode exceptionnelle par les personnes commises à cette fin et qui n'est pas consignée dans un rapport est détruite par les personnes visées à l'alinéa 2 ou par la personne qu'elles délèguent à cette fin. Cette destruction fait	Toute note prise dans le cadre de l'exécution de la méthode exceptionnelle par les personnes commises à cette fin et qui n'est pas consignée dans un rapport est détruite par les personnes visées à l'alinéa 2 ou par la personne qu'elles délèguent à cette fin. Cette destruction fait

l'objet d'une mention dans le registre spécial prévu au § 6.	l'objet d'une mention dans le registre spécial prévu au § 6.
§5. Les enregistrements accompagnés de la transcription éventuelle des communications jugées pertinentes ou de la traduction éventuelle sont conservés, dans un lieu sécurisé désigné par le dirigeant du service conformément aux exigences de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.	§5. Les enregistrements accompagnés de la transcription éventuelle des communications jugées pertinentes ou de la traduction éventuelle sont conservés, dans un lieu sécurisé désigné par le dirigeant du service conformément aux exigences de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.
§6. Un registre spécial tenu régulièrement à jour contient un relevé de chacune des mesures visées aux §§ 1er et 2.	§6. Un registre spécial tenu régulièrement à jour contient un relevé de chacune des mesures visées aux §§ 1er et 2.
Le relevé mentionne la date et l'heure auxquelles la mesure a commencé et celles auxquelles elle s'est terminée.	Le relevé mentionne la date et l'heure auxquelles la mesure a commencé et celles auxquelles elle s'est terminée.
§7. Les enregistrements des communications sont détruits, suivant les modalités fixées par le Roi et sous le contrôle de la Commission et d'un agent désigné à cet effet par le dirigeant du service, dans un délai de cinq ans qui débute le jour de l'enregistrement. Avec l'accord écrit préalable de la Commission, le dirigeant du service peut décider de prolonger la durée de conservation lorsque l'enregistrement est encore nécessaire dans le cadre d'une enquête de renseignement ou d'une procédure judiciaire. La durée totale de conservation ne peut pas dépasser dix ans, sauf lorsqu'un enregistrement est encore nécessaire dans le cadre d'une procédure judiciaire. La destruction est mentionnée dans le registre spécial visé au paragraphe 6.	§7. Les enregistrements des communications sont détruits, suivant les modalités fixées par le Roi et sous le contrôle de la Commission et d'un agent désigné à cet effet par le dirigeant du service, dans un délai de cinq ans qui débute le jour de l'enregistrement. Avec l'accord écrit préalable de la Commission, le dirigeant du service peut décider de prolonger la durée de conservation lorsque l'enregistrement est encore nécessaire dans le cadre d'une enquête de renseignement ou d'une procédure judiciaire. La durée totale de conservation ne peut pas dépasser dix ans, sauf lorsqu'un enregistrement est encore nécessaire dans le cadre d'une procédure judiciaire. La destruction est mentionnée dans le registre spécial visé au paragraphe 6.
Les transcriptions des communications estimées pertinentes et les traductions éventuelles sont conservées et détruites conformément à l'article 21.	Les transcriptions des communications estimées pertinentes et les traductions éventuelles sont conservées et détruites conformément à l'article 21.
CHAPITRE 8 – Modifications à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	
Art. 84	**Art. 84**
§ 1er. Aux fins visées à l'article 82, 2°, et moyennant l'autorisation préalable d'un juge d'instruction, l'auditeur ou, en son absence	§ 1er. Aux fins visées à l'article 82, 2°, et moyennant l'autorisation préalable d'un juge d'instruction, l'auditeur ou, en son absence

l'auditeur adjoint, peut, lorsqu'il estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, faire procéder :	l'auditeur adjoint, peut, lorsqu'il estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, faire procéder :
1° au repérage des données de trafic de moyens de communications électroniques à partir desquels ou vers lesquels des communications électroniques ont été faites;	1° au repérage des données de trafic de moyens de communications électroniques à partir desquels ou vers lesquels des communications électroniques ont été faites;
2° à la localisation de l'origine ou de la destination de communications électroniques, y compris les numéros de téléphone et les adresses réseau.	2° à la localisation de l'origine ou de la destination de communications électroniques, y compris les numéros de téléphone et les adresses réseau.
3° à la demande des détails de paiement des services de communications électroniques.	3° à la demande des détails de paiement des services de communications électroniques.
Pour ce faire, il peut requérir la collaboration:	Pour ce faire, il peut requérir la collaboration:
1° de l'opérateur d'un réseau de communications électroniques;	1° de l'opérateur d'un réseau de communications électroniques;
2° de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.	2° de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.
Dans les cas visés à l'alinéa 1er, pour chaque moyen de communications électroniques dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.	Dans les cas visés à l'alinéa 1er, pour chaque moyen de communications électroniques dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.
L'auditeur ou, en son absence l'auditeur adjoint, indique dans sa décision les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver sa décision, des principes de proportionnalité et de subsidiarité.	L'auditeur ou, en son absence l'auditeur adjoint, indique dans sa décision les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver sa décision, des principes de proportionnalité et de subsidiarité.

Il mentionne également la période du passé sur laquelle porte la demande des données conformément au paragraphe 1er*bis*.	Il mentionne également la période du passé sur laquelle porte la demande des données conformément au paragraphe 1er*bis*.
§ 1er*bis*. Les données visées au paragraphe 1er, alinéa 1er, peuvent être requises pour une période de douze mois préalable à la décision de l'auditeur ou, en son absence, de l'auditeur adjoint, dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, et pour une période de six mois dans le cas d'autres infractions pour lesquelles l'auditeur peut requérir ces données.	§ 1er*bis*. Les données visées au paragraphe 1er, alinéa 1er, peuvent être requises pour une période de douze mois préalable à la décision de l'auditeur ou, en son absence, de l'auditeur adjoint, dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, et pour une période de six mois dans le cas d'autres infractions pour lesquelles l'auditeur peut requérir ces données.
	§ 1erbis/1. Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1er, alinéa 2, de conserver les données visées au paragraphe 1er, alinéa 1er, qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.
	Les paragraphes 1er, alinéas 4 et 5, et 3 s'appliquent par analogie à l'ordre visé à l'alinéa 1er.
	Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soient garanties et à ce que les données soient conservées de manière sécurisée.
	L'auditeur ou, en son absence, l'auditeur adjoint demande sans délai l'autorisation préalable d'un juge d'instruction pour requérir la communication des données visées au paragraphe 1er, alinéa 1er, qui font l'objet d'un ordre de conservation visé à l'alinéa 1er et fait part de cet ordre au juge d'instruction. Si le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre de conservation ou s'il estime que cet ordre n'était pas légitime ou justifié, cet ordre devient caduc. Dans ce cas, l'auditeur ou, en son absence, l'auditeur adjoint fait sans délai savoir au destinataire de

	l'ordre de conservation que celui-ci est devenu caduc.
§ 1er*ter*. La mesure ne peut porter sur les moyens de communications électroniques d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction pour laquelle l'auditeur peut requérir les données visées au paragraphe 1er, alinéa 1er, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une telle infraction utilisent ses moyens de communications électroniques.	§ 1er*ter*. La mesure ne peut porter sur les moyens de communications électroniques d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction pour laquelle l'auditeur peut requérir les données visées au paragraphe 1er, alinéa 1er, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une telle infraction utilisent ses moyens de communications électroniques.
La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par l'auditeur ou, en son absence, par l'auditeur adjoint des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas utilisés.	La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par l'auditeur ou, en son absence, par l'auditeur adjoint des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas utilisés.
§ 2. Après réception de la demande visée au § 1er, les acteurs visés au § 1er, alinéa 2, communiquent sans délai à l'auditeur ou, en son absence l'auditeur adjoint, une estimation du coût des informations demandées et du délai nécessaire pour rassembler ces informations.	§ 2. Après réception de la demande visée au § 1er, les acteurs visés au § 1er, alinéa 2, communiquent sans délai à l'auditeur ou, en son absence l'auditeur adjoint, une estimation du coût des informations demandées et du délai nécessaire pour rassembler ces informations.
Après réception de la confirmation de la demande de l'auditeur ou, en son absence l'auditeur adjoint, les acteurs visés à l'alinéa 1er communiquent les données demandées dans le délai fixé par l'auditeur ou, en son absence l'auditeur adjoint.	Après réception de la confirmation de la demande de l'auditeur ou, en son absence l'auditeur adjoint, les acteurs visés à l'alinéa 1er communiquent les données demandées dans le délai fixé par l'auditeur ou, en son absence l'auditeur adjoint.
§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.	§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.
CHAPITRE 9 – Modifications à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (« loi NIS »)	
Art. 62	**Art. 62**

§ 1er. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 60 et 61. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.	**§ 1er. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 60 et 61. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination.**
	§ 2. Lorsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, le CSIRT national peut obtenir d'un opérateur, au sens de l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques, des données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 91° de la loi du 13 juin 2005 relative aux communications électroniques conservées par celui-ci.
	Les finalités poursuivies par les tâches précitées sont :
	- la prévention de menaces graves contre la sécurité publique ;
	- l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information ;
	- la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave.
	Lorsque le CSIRT national adresse à un opérateur une demande de données relatives à l'utilisateur ou à l'abonné visées à l'article 2, 5° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, cette demande est autorisée par le supérieur hiérarchique.
	Lorsque le CSIRT national adresse à un opérateur une demande de métadonnées de

	communications électroniques au sens de l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques autres que celles visées à l'alinéa précédent, cette demande doit faire l'objet d'un contrôle préalable par l'Autorité de protection des données créé par la loi du 3 décembre 2017.
	En cas de situation urgente dûment justifiée, le CSIRT national peut se passer du contrôle préalable visée à l'alinéa précédent et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa précédent pour permettre un contrôle ultérieur.
	Le directeur du CSIRT national désigne expressément les personnes habilitées à traiter ces données de communications électroniques.
	Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées.
§ 3. Pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.	**§ 3. Pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.**
§ 4**.** Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.	**§ 4. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.**
Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.	**Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.**
Art. 65	**Art. 65**

§ 1er. Conformément à l'article 5.1.c) du Règlement UE 2016/679, lors du traitement de données à caractère personnel dans le cadre de l'exécution de la présente loi, le responsable de traitement veille à limiter le traitement au minimum nécessaire et de manière proportionnée à la finalité poursuivie.	§ 1er. Conformément à l'article 5.1.c) du Règlement UE 2016/679, lors du traitement de données à caractère personnel dans le cadre de l'exécution de la présente loi, le responsable de traitement veille à limiter le traitement au minimum nécessaire et de manière proportionnée à la finalité poursuivie.
§ 2. Dans le respect de ce principe, les données personnelles traitées peuvent être des données de tout type en rapport avec la sécurité des réseaux et systèmes d'information, à savoir le cas échéant des informations nominatives, des données concernant les collaborateurs d'une organisation ou des personnes extérieures, des données ou des identifiants de connexion, des données de géolocalisation, des données d'identification ou d'authentification, le cas échéant au moyen de dispositifs sécurisés.	§ 2. Dans le respect de ce principe, les données personnelles traitées peuvent être des données de tout type en rapport avec la sécurité des réseaux et systèmes d'information, à savoir le cas échéant des informations nominatives, des données concernant les collaborateurs d'une organisation ou des personnes extérieures, des données ou des identifiants de connexion, **des données de communications électroniques,** des données de géolocalisation, des données d'identification ou d'authentification, le cas échéant au moyen de dispositifs sécurisés.
§ 3. Les principaux traitements de données personnelles dans le cadre de la présente loi peuvent être regroupés comme suit :	§ 3. Les principaux traitements de données personnelles dans le cadre de la présente loi peuvent être regroupés comme suit :
- l'échange général d'informations entre les opérateurs de services essentiels et les fournisseurs de services numériques, d'une part, et les autorités visées à l'article 7, d'autre part ;	- l'échange général d'informations entre les opérateurs de services essentiels et les fournisseurs de services numériques, d'une part, et les autorités visées à l'article 7, d'autre part ;
- le traitement d'informations spécifiques entre les entités visées au premier tiret dans le cadre des notifications d'incidents ou d'autres échanges ponctuels ;	- le traitement d'informations spécifiques entre les entités visées au premier tiret dans le cadre des notifications d'incidents ou d'autres échanges ponctuels ;
- le traitement par les services d'inspection conformément au titre 4 ;	- le traitement par les services d'inspection conformément au titre 4 ;
- le traitement par les cours et tribunaux ou les autorités sectorielles dans le cadre de la mise en oeuvre de la loi et particulièrement de la recherche, la poursuite et la répression d'infractions ;	- le traitement par les cours et tribunaux ou les autorités sectorielles dans le cadre de la mise en oeuvre de la loi et particulièrement de la recherche, la poursuite et la répression d'infractions ;
- les échanges et autres traitements d'informations par le CSIRT national et par le CSIRT sectoriel pour leurs missions visées respectivement aux articles 60 à 62 et 63 et 64.	- les échanges et autres traitements d'informations par le CSIRT national et par le CSIRT sectoriel pour leurs missions visées respectivement aux articles 60 à 62 et 63 et 64.

CHAPITRE 10 – Modifications à la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits	
Art. 11	**Art. 11**
§ 1er. Sans préjudice des attributions des officiers de police judiciaire, les membres du personnel statutaire ou contractuel du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement désignés à cette fin par le Roi surveillent l'exécution des dispositions de la présente loi et de ses arrêtés d'exécution ainsi que des règlements de l'Union européenne et qui relèvent des compétences du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement en effectuant des inspections inopinées, munis de pièces justificatives de leurs fonctions qui sont établies par le Roi.	§ 1er. Sans préjudice des attributions des officiers de police judiciaire, les membres du personnel statutaire ou contractuel du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement désignés à cette fin par le Roi surveillent l'exécution des dispositions de la présente loi et de ses arrêtés d'exécution ainsi que des règlements de l'Union européenne et qui relèvent des compétences du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement en effectuant des inspections inopinées, munis de pièces justificatives de leurs fonctions qui sont établies par le Roi.
Les membres du personnel contractuel prêtent serment, préalablement à l'exercice de leurs fonctions, entre les mains du ministre ou de son délégué.	Les membres du personnel contractuel prêtent serment, préalablement à l'exercice de leurs fonctions, entre les mains du ministre ou de son délégué.
Les membres du personnel statutaire ou contractuel du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et l'Environnement désignés par le Roi pour la surveillance de l'application de la présente loi et des arrêtés pris en exécution de celle-ci peuvent, dans les limites de l'exécution de leur compétence, pénétrer, sans avertissement préalable, en tous lieux affectés au commerce des denrées alimentaires ou autres produits visés par la présente loi et dans les dépôts attenant à ces lieux et autres lieux soumis à leur contrôle ou dans lesquels ils peuvent avoir un motif raisonnable de supposer qu'il existe des infractions aux dispositions des législations dont ils exercent la surveillance. Ils peuvent les fouiller, même si ceux-ci ne sont pas accessibles au public.	Les membres du personnel statutaire ou contractuel du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et l'Environnement désignés par le Roi pour la surveillance de l'application de la présente loi et des arrêtés pris en exécution de celle-ci peuvent, dans les limites de l'exécution de leur compétence, pénétrer, sans avertissement préalable, en tous lieux affectés au commerce des denrées alimentaires ou autres produits visés par la présente loi et dans les dépôts attenant à ces lieux et autres lieux soumis à leur contrôle ou dans lesquels ils peuvent avoir un motif raisonnable de supposer qu'il existe des infractions aux dispositions des législations dont ils exercent la surveillance. Ils peuvent les fouiller, même si ceux-ci ne sont pas accessibles au public.
Ils peuvent pénétrer sans avertissement préalable, à tout moment, dans les lieux qui servent à la fabrication des denrées alimentaires ou autres produits visés par la présente loi et destinés au commerce, ainsi que dans les lieux où ils sont entreposés.	Ils peuvent pénétrer sans avertissement préalable, à tout moment, dans les lieux qui servent à la fabrication des denrées alimentaires ou autres produits visés par la présente loi et destinés au commerce, ainsi que dans les lieux où ils sont entreposés.

La visite des lieux servant exclusivement d'habitation n'est permise qu'entre 5 heures du matin et 9 heures du soir et il ne peut y être procédé qu'avec l'autorisation du juge.	La visite des lieux servant exclusivement d'habitation n'est permise qu'entre 5 heures du matin et 9 heures du soir et il ne peut y être procédé qu'avec l'autorisation du juge.
Ils peuvent exiger la production de tous écrits et documents commerciaux relatifs aux denrées alimentaires et autres produits visés par la présente loi et de tous documents imposés par les arrêtés pris en exécution de la présente loi.	Ils peuvent exiger la production de tous écrits et documents commerciaux relatifs aux denrées alimentaires et autres produits visés par la présente loi et de tous documents imposés par les arrêtés pris en exécution de la présente loi.
Ils peuvent procéder au contrôle des transports, transport en commun et des moyens de transports.	Ils peuvent procéder au contrôle des transports, transport en commun et des moyens de transports.
	Ils peuvent identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique.
	À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification à :
	1° l'opérateur d'un réseau de communications électroniques ; et
	2° toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.
	Sans préjudice d'une éventuelle délégation, chaque demande d'identification doit être approuvée au préalable, par écrit, par le chef du service Inspection produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement.
§ 2. Ils constatent les infractions aux lois et arrêtés sur la matière dans les procès-verbaux faisant foi jusqu'à preuve du contraire.	§ 2. Ils constatent les infractions aux lois et arrêtés sur la matière dans les procès-verbaux faisant foi jusqu'à preuve du contraire.
Ils peuvent procéder à l'audition du contrevenant et à toute autre audition utile.	Ils peuvent procéder à l'audition du contrevenant et à toute autre audition utile.

Une copie du procès-verbal est transmise au contrevenant dans les trente jours de la constatation de l'infraction.	Une copie du procès-verbal est transmise au contrevenant dans les trente jours de la constatation de l'infraction.
Ils peuvent requérir, dans l'exercice de leurs missions, l'assistance des forces de police.	Ils peuvent requérir, dans l'exercice de leurs missions, l'assistance des forces de police.
Ils peuvent procéder au scellage d'appareils automatiques de distribution qui ne sont pas conforme à l'article 6, §§ 4 et 6. Les conditions à cet effet sont élaborées par le ministre.	Ils peuvent procéder au scellage d'appareils automatiques de distribution qui ne sont pas conforme à l'article 6, §§ 4 et 6. Les conditions à cet effet sont élaborées par le ministre.
Ils peuvent procéder à tout examen, contrôle et audition et recueillir toutes informations qu'ils estiment nécessaires pour s'assurer que les dispositions des législations dont ils exercent la surveillance sont effectivement observées et notamment prendre l'identité de toute personne dont ils estiment l'audition nécessaire pour l'exercice de la surveillance.	Ils peuvent procéder à tout examen, contrôle et audition et recueillir toutes informations qu'ils estiment nécessaires pour s'assurer que les dispositions des législations dont ils exercent la surveillance sont effectivement observées et notamment prendre l'identité de toute personne dont ils estiment l'audition nécessaire pour l'exercice de la surveillance.
§ 3. Le procès-verbal constatant les infractions visées à l'article 19 et rédigé par les personnes visées au § 1er chargés de la surveillance désignés par le Roi, est transmis au fonctionnaire désigné en application de l'article 19. Au cas où le procès-verbal aurait été dressé par le bourgmestre ou son délégué, il peut également être envoyé au fonctionnaire précité.	§ 3. Le procès-verbal constatant les infractions visées à l'article 19 et rédigé par les personnes visées au § 1er chargés de la surveillance désignés par le Roi, est transmis au fonctionnaire désigné en application de l'article 19. Au cas où le procès-verbal aurait été dressé par le bourgmestre ou son délégué, il peut également être envoyé au fonctionnaire précité.
En cas d'application de l'article 11bis, le procès-verbal n'est transmis au procureur du Roi que lorsqu'il n'a pas été donné suite à l'avertissement.	En cas d'application de l'article 11bis, le procès-verbal n'est transmis au procureur du Roi que lorsqu'il n'a pas été donné suite à l'avertissement.
§ 4. Le Roi peut fixer d'autres modalités de contrôle et d'inspection, afin de satisfaire aux obligations résultant des traités internationaux et des actes internationaux pris en vertu de ceux-ci.	§ 4. Le Roi peut fixer d'autres modalités de contrôle et d'inspection, afin de satisfaire aux obligations résultant des traités internationaux et des actes internationaux pris en vertu de ceux-ci.
§ 5. Les dispositions du présent article ne s'appliquent pas aux contrôles effectués en application de la loi du 4 février 2000 relative à la création de l'Agence fédérale pour la Sécurité de la Chaîne alimentaire.	§ 5. Les dispositions du présent article ne s'appliquent pas aux contrôles effectués en application de la loi du 4 février 2000 relative à la création de l'Agence fédérale pour la Sécurité de la Chaîne alimentaire.

COÖRDINATIE VAN DE ARTIKELEN	
BASISTEKST	**TEKST AANGEPAST AAN HET WETSONTWERP**
HOOFDSTUK 2. Wijzigingen aan de wet van 13 juni 2005 betreffende de elektronische communicatie.	
TITEL I. - Definities en algemene principes.	TITEL I. - Definities en algemene principes.
HOOFDSTUK I. - Algemeen.	HOOFDSTUK I. - Algemeen.
Art. 2	**Art. 2**
Voor de toepassing van deze wet wordt verstaan onder :	Voor de toepassing van deze wet wordt verstaan onder :
1° " Instituut " : Het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	1° " Instituut " : Het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
2° " minister " : de ministers of staatssecretaris die bevoegd zijn voor de aangelegenheden die de elektronische communicatie betreffen als bedoeld in deze wet;	2° " minister " : de ministers of staatssecretaris die bevoegd zijn voor de aangelegenheden die de elektronische communicatie betreffen als bedoeld in deze wet;
3° “elektronische-communicatienetwerk”: de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van andere signalen dan die voor audiovisuele en auditieve mediadiensten worden gebruikt;	3° “elektronische-communicatienetwerk”: de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van andere signalen dan die voor audiovisuele en auditieve mediadiensten worden gebruikt;
3/1° “netwerk met zeer hoge capaciteit”: hetzij een netwerk voor elektronische communicatie dat ten minste tot aan het distributiepunt volledig uit optische-vezelelementen bestaat, hetzij een elektronischecommunicatienetwerk	3/1° “netwerk met zeer hoge capaciteit”: hetzij een netwerk voor elektronische communicatie dat ten minste tot aan het distributiepunt volledig uit optische-vezelelementen bestaat, hetzij een elektronischecommunicatienetwerk

dat, in gebruikelijke piekomstandigheden, in staat is om soortgelijke netwerkprestaties te bieden wat betreft downlink- en uplinkbandbreedte, veerkrachtigheid van het netwerk, parameters met betrekking tot fouten, latentietijden en de veranderingen daarin; de netwerkprestaties kunnen ook als vergelijkbaar worden beschouwd als de eindgebruiker een andere gebruikservaring heeft vanwege de inherent verschillende kenmerken van het medium dat op het netwerk wordt aangesloten;	dat, in gebruikelijke piekomstandigheden, in staat is om soortgelijke netwerkprestaties te bieden wat betreft downlink- en uplinkbandbreedte, veerkrachtigheid van het netwerk, parameters met betrekking tot fouten, latentietijden en de veranderingen daarin; de netwerkprestaties kunnen ook als vergelijkbaar worden beschouwd als de eindgebruiker een andere gebruikservaring heeft vanwege de inherent verschillende kenmerken van het medium dat op het netwerk wordt aangesloten;
4° " aanbieden van een elektronische-communicatienetwerk " : het bouwen, exploiteren, toezicht houden op of beschikbaar stellen van een elektronisch communicatienetwerk;	4° " aanbieden van een elektronische-communicatienetwerk " : het bouwen, exploiteren, toezicht houden op of beschikbaar stellen van een elektronisch communicatienetwerk;
5° “elektronische-communicatiedienst”: een gewoonlijk tegen vergoeding via elektronische-communicatienetwerken aangeboden dienst, die, met uitzondering van diensten waarbij met behulp van elektronischecommunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd en met uitzondering van audiovisuele en auditieve mediadiensten, de volgende soorten diensten omvat:	5° “elektronische-communicatiedienst”: een gewoonlijk tegen vergoeding via elektronische-communicatienetwerken aangeboden dienst, die, met uitzondering van diensten waarbij met behulp van elektronischecommunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd en met uitzondering van audiovisuele en auditieve mediadiensten, de volgende soorten diensten omvat:
a) internettoegangsdienst;	a) internettoegangsdienst;
b) interpersoonlijke communicatiedienst; en	b) interpersoonlijke communicatiedienst; en
c) diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt;	c) diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt;
5/1° “internettoegangsdienst”: een voor het publiek beschikbare elektronische-communicatiedienst die toegang tot het internet biedt en derhalve connectiviteit met vrijwel alle eindpunten van het internet, ongeacht de gebruikte netwerktechnologie en eindapparatuur;	5/1° “internettoegangsdienst”: een voor het publiek beschikbare elektronische-communicatiedienst die toegang tot het internet biedt en derhalve connectiviteit met vrijwel alle eindpunten van het internet, ongeacht de gebruikte netwerktechnologie en eindapparatuur;
5/2° “interpersoonlijke communicatiedienst”: een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve	5/2° “interpersoonlijke communicatiedienst”: een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve

uitwisseling van informatie via elektronische-communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;	uitwisseling van informatie via elektronische-communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;
5/3° "nummergebaseerde interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;	5/3° "nummergebaseerde interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;
5/4° "nummeronafhankelijke interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die geen verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die geen communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;	5/4° "nummeronafhankelijke interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die geen verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die geen communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;
	5/5°: "fraude": een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten nadele van de operator of eindgebruiker, via het gebruik van een elektronische-communicatiedienst;
	5/6°: "kwaadwillig gebruik van het netwerk of van de dienst": gebruik van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen;
6° " verkeersgegeven " : gegeven dat wordt verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor het factureren van een dergelijke communicatie;	6° " verkeersgegeven " : gegeven dat wordt verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor het factureren van een dergelijke communicatie;

7° “informatie over de locatie van de oproeper”: in een openbaar mobiel netwerk, de verwerkte gegevens, afkomstig van netwerkinfrastructuur of van handsets, waaruit de geografische positie van de mobiele eindapparatuur van een eindgebruiker blijkt en, in een openbaar vast netwerk, de gegevens over het fysieke adres van het netwerkaansluitpunt;	7° “informatie over de locatie van de oproeper”: in een openbaar mobiel netwerk, de verwerkte gegevens, afkomstig van netwerkinfrastructuur of van handsets, waaruit de geografische positie van de mobiele eindapparatuur van een eindgebruiker blijkt en, in een openbaar vast netwerk, de gegevens over het fysieke adres van het netwerkaansluitpunt;
8° " dienst met verkeersgegevens " : een dienst die een bijzondere behandeling van de verkeersgegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;	8° " dienst met verkeersgegevens " : een dienst die een bijzondere behandeling van de verkeersgegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;
9° " dienst met locatiegegevens " : een dienst die een bijzondere behandeling van de locatiegegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;	9° " dienst met locatiegegevens " : een dienst die een bijzondere behandeling van de locatiegegevens vereist die verder gaat dan wat strikt noodzakelijk is voor het versturen of aanrekenen van de communicatie;
10° " openbaar elektronische-communicatienetwerk " : een elektronische-communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om voor het publiek beschikbare elektronische-communicatiediensten [...] aan te bieden ter ondersteuning van de overdracht van informatie tussen netwerkaansluitpunten;	10° " openbaar elektronische-communicatienetwerk " : een elektronische-communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om voor het publiek beschikbare elektronische-communicatiediensten [...] aan te bieden ter ondersteuning van de overdracht van informatie tussen netwerkaansluitpunten;
10/1° "elektronische-communicatienetwerk met hoge snelheid" : een elektronische-communicatienetwerk dat breedbandtoegangsdiensten kan leveren met snelheden van minstens 30 Mbps;	10/1° "elektronische-communicatienetwerk met hoge snelheid" : een elektronische-communicatienetwerk dat breedbandtoegangsdiensten kan leveren met snelheden van minstens 30 Mbps;
11° “operator”: persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt;	11° “operator”: persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt;
11/1° “beheerder van passieve infrastructuren”: een economische speler die, enerzijds, een dienst levert van productie, transport of distributie van gas, van elektriciteit (straatverlichting inbegrepen) of van water (de verwijdering of verwerking en zuivering van afval- en rioolwater, en drainagesystemen inbegrepen); van verwarming; of die	11/1° “beheerder van passieve infrastructuren”: een economische speler die, enerzijds, een dienst levert van productie, transport of distributie van gas, van elektriciteit (straatverlichting inbegrepen) of van water (de verwijdering of verwerking en zuivering van afval- en rioolwater, en drainagesystemen inbegrepen); van verwarming; of die

transportdiensten verstrekt (met inbegrip van spoorwegen, wegen, havens en luchthavens), en die anderzijds elementen van zijn netwerk ter beschikking stelt zonder dat deze zelf actieve elementen van een elektronische-communicatienetwerk worden;	transportdiensten verstrekt (met inbegrip van spoorwegen, wegen, havens en luchthavens), en die anderzijds elementen van zijn netwerk ter beschikking stelt zonder dat deze zelf actieve elementen van een elektronische-communicatienetwerk worden;
11/2° “algemene machtiging”: regelgeving waarbij rechten worden verleend voor het aanbieden van elektronische communicatienetwerken of -diensten en specifieke sectorgebonden verplichtingen worden vastgesteld die kunnen gelden voor alle of voor specifieke soorten elektronische-communicatienetwerken en -diensten;	11/2° “algemene machtiging”: regelgeving waarbij rechten worden verleend voor het aanbieden van elektronische communicatienetwerken of -diensten en specifieke sectorgebonden verplichtingen worden vastgesteld die kunnen gelden voor alle of voor specifieke soorten elektronische-communicatienetwerken en -diensten;
12° " gebruiker " : een natuurlijke of rechtspersoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst;	12° " gebruiker " : een natuurlijke of rechtspersoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst;
13° " eindgebruiker " : een gebruiker die geen openbaar elektronische-communicatienetwerk of voor het publiek beschikbare elektronische-communicatiediensten aanbiedt;	13° " eindgebruiker " : een gebruiker die geen openbaar elektronische-communicatienetwerk of voor het publiek beschikbare elektronische-communicatiediensten aanbiedt;
14° " consument " : een natuurlijke persoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst voor “andere doeleinden dan deze in het kader van zijn bedrijfs- of beroepsdoeleinden;	14° " consument " : een natuurlijke persoon die gebruik maakt van of verzoekt om een voor het publiek beschikbare elektronische-communicatiedienst voor “andere doeleinden dan deze in het kader van zijn bedrijfs- of beroepsdoeleinden;
14/1° “micro-onderneming”: onderneming die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;	14/1° “micro-onderneming”: onderneming die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;
14/2° “kleine onderneming”: onderneming die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;	14/2° “kleine onderneming”: onderneming die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;
14/3° “middelgrote onderneming”: onderneming die het jaargemiddelde van 249 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;	14/3° “middelgrote onderneming”: onderneming die het jaargemiddelde van 249 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:24 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;

14/4° “micro-organisatie zonder winstoogmerk”: vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;	14/4° “micro-organisatie zonder winstoogmerk”: vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;
14/5° “kleine organisatie zonder winstoogmerk”: vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;	14/5° “kleine organisatie zonder winstoogmerk”: vereniging zonder winstoogmerk, internationale vereniging zonder winstoogmerk of stichting die het jaargemiddelde van 49 tewerkgestelde werknemers, berekend overeenkomstig artikel 1:28 van het Wetboek van vennootschappen en verenigingen, niet overschrijdt;
15° " abonnee " : een natuurlijke of rechtspersoon [...] die geen operator is en die partij is bij een overeenkomst met een operator, die voor het publiek beschikbare elektronische-communicatiediensten aanbiedt voor de levering van die diensten;	15° " abonnee " : een natuurlijke of rechtspersoon [...] die geen operator is en die partij is bij een overeenkomst met een operator, die voor het publiek beschikbare elektronische-communicatiediensten aanbiedt voor de levering van die diensten;
15/1° “abonnee met maximum 9 werknemers”: abonnee die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig, naar gelang het geval, artikel 1:24 of 1:28 van hetWetboek van vennootschappen en verenigingen, niet overschrijdt;	15/1° “abonnee met maximum 9 werknemers”: abonnee die het jaargemiddelde van 9 tewerkgestelde werknemers, berekend overeenkomstig, naar gelang het geval, artikel 1:24 of 1:28 van hetWetboek van vennootschappen en verenigingen, niet overschrijdt;
16° “netwerkaansluitpunt”: het fysieke punt waarop een eindgebruiker de toegang tot een openbaar elektronische-communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het netwerkaansluitpunt bepaald door middel van een specifiek netwerkadres dat met een nummer of naam van een eindgebruiker kan zijn verbonden;	16° “netwerkaansluitpunt”: het fysieke punt waarop een eindgebruiker de toegang tot een openbaar elektronische-communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het netwerkaansluitpunt bepaald door middel van een specifiek netwerkadres dat met een nummer of naam van een eindgebruiker kan zijn verbonden;
16/1° "toegangspunt" : een in of buiten het gebouw gelegen fysiek punt dat toegankelijk is voor operatoren, waar het netwerk kan worden aangesloten op de voor hoge snelheid bestemde fysieke binnenhuisinfrastructuur;	16/1° "toegangspunt" : een in of buiten het gebouw gelegen fysiek punt dat toegankelijk is voor operatoren, waar het netwerk kan worden aangesloten op de voor hoge snelheid bestemde fysieke binnenhuisinfrastructuur;

17° “bijbehorende faciliteiten”: de bij een elektronischecommunicatienetwerk of een elektronische-communicatiedienst behorende diensten, fysieke infrastructuren en andere faciliteiten of elementen die het aanbieden van diensten via dat netwerk of dienst mogelijk maken of ondersteunen of het potentieel hiertoe bezitten en onder meer gebouwen of toegangen tot gebouwen, bekabeling van gebouwen, antennes, torens en andere ondersteunende constructies, kabelgoten, kabelbuizen, masten, mangaten en straatkasten omvatten;	17° “bijbehorende faciliteiten”: de bij een elektronischecommunicatienetwerk of een elektronische-communicatiedienst behorende diensten, fysieke infrastructuren en andere faciliteiten of elementen die het aanbieden van diensten via dat netwerk of dienst mogelijk maken of ondersteunen of het potentieel hiertoe bezitten en onder meer gebouwen of toegangen tot gebouwen, bekabeling van gebouwen, antennes, torens en andere ondersteunende constructies, kabelgoten, kabelbuizen, masten, mangaten en straatkasten omvatten;
17/1° “bijbehorende dienst”: een bij een elektronischecommunicatienetwerk of een elektronische-communicatiedienst behorende dienst die het aanbieden, het zelf verstrekken of het geautomatiseerd aanbieden van diensten via dat netwerk of dienst mogelijk maakt of ondersteunt of het potentieel hiertoe bezit en onder meer nummervertaalsystemen of systemen met soortgelijke functies en voorwaardelijke-toegangssystemen en elektronische programmagidsen, kort “EPG’s”, alsmede andere diensten zoals identiteit, locatie en presentie-informatiediensten omvat (met uitzondering van diensten en systemen die uitsluitend worden gebruikt voor audiovisuele of auditieve mediadiensten);	17/1° “bijbehorende dienst”: een bij een elektronischecommunicatienetwerk of een elektronische-communicatiedienst behorende dienst die het aanbieden, het zelf verstrekken of het geautomatiseerd aanbieden van diensten via dat netwerk of dienst mogelijk maakt of ondersteunt of het potentieel hiertoe bezit en onder meer nummervertaalsystemen of systemen met soortgelijke functies en voorwaardelijke-toegangssystemen en elektronische programmagidsen, kort “EPG’s”, alsmede andere diensten zoals identiteit, locatie en presentie-informatiediensten omvat (met uitzondering van diensten en systemen die uitsluitend worden gebruikt voor audiovisuele of auditieve mediadiensten);
17/2° "fysieke binnenhuisinfrastructuur" : elk element van een netwerk, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens en palen (buiten kabels, met inbegrip van ongebruikte glasvezels (dark fibre)), alsook installaties op de locatie van de eindgebruiker, met inbegrip van elementen die gemeenschappelijk eigendom zijn, die bestemd zijn om elementen van vaste of draadloze toegangsnetwerken onder te brengen zonder dat ze zelf een actief element van het netwerk worden, voor zover die netwerken elektronische-communicatiediensten kunnen leveren en het toegangspunt van het gebouw kunnen aansluiten op het aansluitpunt van het netwerk;	17/2° "fysieke binnenhuisinfrastructuur" : elk element van een netwerk, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens en palen (buiten kabels, met inbegrip van ongebruikte glasvezels (dark fibre)), alsook installaties op de locatie van de eindgebruiker, met inbegrip van elementen die gemeenschappelijk eigendom zijn, die bestemd zijn om elementen van vaste of draadloze toegangsnetwerken onder te brengen zonder dat ze zelf een actief element van het netwerk worden, voor zover die netwerken elektronische-communicatiediensten kunnen leveren en het toegangspunt van het gebouw kunnen aansluiten op het aansluitpunt van het netwerk;
17/3° "nomadiciteit": eigenschap van een elektronische-communicatiedienst waardoor	17/3° "nomadiciteit": eigenschap van een elektronische-communicatiedienst waardoor

deze dienst gebruikt kan worden vanuit potentieel om het even welke aansluiting op een elektronische-communicatienetwerk;	deze dienst gebruikt kan worden vanuit potentieel om het even welke aansluiting op een elektronische-communicatienetwerk;
18° " toegang " : het beschikbaar stellen aan een operator van faciliteiten en/of diensten onder uitdrukkelijke voorwaarden, hetzij op exclusieve hetzij op niet-exclusieve basis, met het oog op het aanbieden van elektronische-communicatiediensten of het aanbieden van diensten van de informatiemaatschappij. Deze term omvat met name toegang tot netwerkelementen en verwante faciliteiten waarbij eventueel apparatuur kan worden verbonden met vaste of niet-vaste middelen (dit houdt met name toegang in tot het aansluitnet en tot faciliteiten en diensten die noodzakelijk zijn om diensten te kunnen aanbieden via het aansluitnet); toegang tot materiële infrastructuur waaronder gebouwen, kabelgoten en masten; toegang tot relevante programmatuursystemen waaronder operationele ondersteuningssystemen; toegang tot informatiesystemen of databases voor reservering, levering, bestelling, onderhouds- en herstelverzoeken en facturering; toegang tot nummervertaling of systemen met vergelijkbare functionaliteit; toegang tot vaste en mobiele netwerken, met name voor roaming; toegang tot virtuele netwerkdiensten;	18° " toegang " : het beschikbaar stellen aan een operator van faciliteiten en/of diensten onder uitdrukkelijke voorwaarden, hetzij op exclusieve hetzij op niet-exclusieve basis, met het oog op het aanbieden van elektronische-communicatiediensten of het aanbieden van diensten van de informatiemaatschappij. Deze term omvat met name toegang tot netwerkelementen en verwante faciliteiten waarbij eventueel apparatuur kan worden verbonden met vaste of niet-vaste middelen (dit houdt met name toegang in tot het aansluitnet en tot faciliteiten en diensten die noodzakelijk zijn om diensten te kunnen aanbieden via het aansluitnet); toegang tot materiële infrastructuur waaronder gebouwen, kabelgoten en masten; toegang tot relevante programmatuursystemen waaronder operationele ondersteuningssystemen; toegang tot informatiesystemen of databases voor reservering, levering, bestelling, onderhouds- en herstelverzoeken en facturering; toegang tot nummervertaling of systemen met vergelijkbare functionaliteit; toegang tot vaste en mobiele netwerken, met name voor roaming; toegang tot virtuele netwerkdiensten;
19° “interconnectie”: een specifiek type toegang dat tussen operatoren van openbare netwerken wordt gerealiseerd door het fysiek en logisch verbinden van openbare elektronische-communicatienetwerken die door dezelfde of een andere onderneming worden gebruikt om het de gebruikers van een onderneming mogelijk te maken te communiceren met die van dezelfde of van een andere onderneming of toegang te hebben tot diensten die door een andere onderneming worden aangeboden, wanneer die diensten worden aangeboden door de betrokken partijen of andere partijen die toegang hebben tot het netwerk;	19° “interconnectie”: een specifiek type toegang dat tussen operatoren van openbare netwerken wordt gerealiseerd door het fysiek en logisch verbinden van openbare elektronische-communicatienetwerken die door dezelfde of een andere onderneming worden gebruikt om het de gebruikers van een onderneming mogelijk te maken te communiceren met die van dezelfde of van een andere onderneming of toegang te hebben tot diensten die door een andere onderneming worden aangeboden, wanneer die diensten worden aangeboden door de betrokken partijen of andere partijen die toegang hebben tot het netwerk;
20° " interface " : een netwerkaansluitpunt en/of een radio-interface en de bijhorende technische specificaties;	20° " interface " : een netwerkaansluitpunt en/of een radio-interface en de bijhorende technische specificaties;
21° [...];	21° [...];

22° “spraakcommunicatiedienst”: een voor het publiek beschikbare elektronische-communicatiedienst voor direct of indirect uitgaande en binnenkomende nationale of nationale en internationale gesprekken, met behulp van een nummer of een aantal nummers in een nationaal of internationaal nummerplan;	22° “spraakcommunicatiedienst”: een voor het publiek beschikbare elektronische-communicatiedienst voor direct of indirect uitgaande en binnenkomende nationale of nationale en internationale gesprekken, met behulp van een nummer of een aantal nummers in een nationaal of internationaal nummerplan;
22/1° oproep " : door middel van een voor het publiek beschikbare interpersoonlijke communicatiedienst tot stand gebrachte verbinding die tweewegspraak-communicatie mogelijk maakt;	22/1° oproep " : door middel van een voor het publiek beschikbare interpersoonlijke communicatiedienst tot stand gebrachte verbinding die tweewegspraak-communicatie mogelijk maakt;
22/2° “dienst voor totale conversatie”: een multimediale dienst voor in werkelijke tijd conversatie die bidirectionele symmetrische in werkelijke tijd overdracht van videofilm, realtime tekst en stem tussen gebruikers in twee of meer locaties biedt;	22/2° “dienst voor totale conversatie”: een multimediale dienst voor in werkelijke tijd conversatie die bidirectionele symmetrische in werkelijke tijd overdracht van videofilm, realtime tekst en stem tussen gebruikers in twee of meer locaties biedt;
23° " aansluitnetwerk " : een fysiek pad dat door elektronischecommunicatiesignalen wordt gebruikt en het netwerkaansluitpunt verbindt met een verdeler of een soortgelijke voorziening in het vaste voor het publiek beschikbare elektronische-communicatienetwerk;	23° " aansluitnetwerk " : een fysiek pad dat door elektronischecommunicatiesignalen wordt gebruikt en het netwerkaansluitpunt verbindt met een verdeler of een soortgelijke voorziening in het vaste voor het publiek beschikbare elektronische-communicatienetwerk;
24° subnetwerk : gedeelte van een aansluitnetwerk dat het netwerkaansluitpunt verbindt met een concentratiepunt of een ander bepaald tussenliggend aansluitpunt gelegen in het vaste openbare elektronische-communicatienetwerk;	24° subnetwerk : gedeelte van een aansluitnetwerk dat het netwerkaansluitpunt verbindt met een concentratiepunt of een ander bepaald tussenliggend aansluitpunt gelegen in het vaste openbare elektronische-communicatienetwerk;
25° " volledig ontbundelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van de volledige capaciteit van netwerkinfrastructuur;	25° " volledig ontbundelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van de volledige capaciteit van netwerkinfrastructuur;
26° " toegang tot binair debiet " : toegang die bestaat uit het verlenen van transportcapaciteit met de bijbehorende schakeling naar een gebruiker waarbij de toegangsleverancier de interface bij de gebruiker vastlegt;	26° " toegang tot binair debiet " : toegang die bestaat uit het verlenen van transportcapaciteit met de bijbehorende schakeling naar een gebruiker waarbij de toegangsleverancier de interface bij de gebruiker vastlegt;

27° " gedeelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van een gespecificeerd deel van de capaciteit van de netwerkinfrastructuur, zoals een deel van de frequentie of iets gelijkwaardigs;	27° " gedeelde toegang tot het aansluitnetwerk " : het verlenen van toegang tot het aansluitnetwerk of het subnetwerk van een onderneming met aanmerkelijke marktmacht op een relevante markt, waarbij toestemming wordt verleend voor het gebruik van een gespecificeerd deel van de capaciteit van de netwerkinfrastructuur, zoals een deel van de frequentie of iets gelijkwaardigs;
28° " ontbundelde toegang tot het aansluitnetwerk " : het verlenen van volledig ontbundelde toegang of gedeelde toegang tot het aansluitnetwerk, wat geen verandering behelst in de eigendom van het aansluitnetwerk;	28° " ontbundelde toegang tot het aansluitnetwerk " : het verlenen van volledig ontbundelde toegang of gedeelde toegang tot het aansluitnetwerk, wat geen verandering behelst in de eigendom van het aansluitnetwerk;
29° " co-locatie " : het leveren van fysieke ruimte en technische faciliteiten, nodig om het installeren en aansluiten van apparatuur van een operator onder redelijke voorwaarden mogelijk te maken in het kader van een referentieaanbod;	29° " co-locatie " : het leveren van fysieke ruimte en technische faciliteiten, nodig om het installeren en aansluiten van apparatuur van een operator onder redelijke voorwaarden mogelijk te maken in het kader van een referentieaanbod;
29/1° " kabelgoot " : omhulsel dat dient om glasvezel-, telefoon- en/of coaxkabels en/of netwerkfaciliteiten te laten passeren en te beschermen;	29/1° " kabelgoot " : omhulsel dat dient om glasvezel-, telefoon- en/of coaxkabels en/of netwerkfaciliteiten te laten passeren en te beschermen;
30° " huurlijn " : elektronische-communicatiedienst bestaande uit de levering van communicatiefaciliteiten met behulp waarvan transparante transmissiecapaciteit tussen netwerkaansluitpunten wordt geboden, met uitzondering van de schakeling op aanvraag;	30° " huurlijn " : elektronische-communicatiedienst bestaande uit de levering van communicatiefaciliteiten met behulp waarvan transparante transmissiecapaciteit tussen netwerkaansluitpunten wordt geboden, met uitzondering van de schakeling op aanvraag;
31° " radiogolven " : elektromagnetische golven die zich in de ruimte voortplanten zonder kunstmatige geleider, en waarvan de frequentie onder 3000 GHz ligt;	31° " radiogolven " : elektromagnetische golven die zich in de ruimte voortplanten zonder kunstmatige geleider, en waarvan de frequentie onder 3000 GHz ligt;
32° (opgeheven)	32° (opgeheven)
33° " radiospectrum " : het geheel van de radiogolven;	33° " radiospectrum " : het geheel van de radiogolven;
33/1° “radiospectrumtoewijzing”: de aanwijzing van een specifieke radiospectrumband voor gebruik door een of meer soorten	33/1° “radiospectrumtoewijzing”: de aanwijzing van een specifieke radiospectrumband voor gebruik door een of meer soorten

radiocommunicatiediensten, in voorkomend geval onder duidelijk omschreven voorwaarden;	radiocommunicatiediensten, in voorkomend geval onder duidelijk omschreven voorwaarden;
33/2° "nationaal frequentietoewijzingsplan": document dat voor elke band van het radiospectrum de informatie bevat in verband met de toewijzingen van het radiospectrum en de toegestane toepassingen;	33/2° "nationaal frequentietoewijzingsplan": document dat voor elke band van het radiospectrum de informatie bevat in verband met de toewijzingen van het radiospectrum en de toegestane toepassingen;
33/3° "geharmoniseerd radiospectrum": radiospectrum waarvoor geharmoniseerde voorwaarden in verband met de beschikbaarheid en het doelmatig gebruik ervan zijn vastgesteld door middel van technische uitvoeringsmaatregelen overeenkomstig artikel 4 van Beschikking nr. 676/2002/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een regelgevingskader voor het radiospectrumbeleid in de Europese Gemeenschap, hierna te noemen "Radiospectrumbeschikking";	33/3° "geharmoniseerd radiospectrum": radiospectrum waarvoor geharmoniseerde voorwaarden in verband met de beschikbaarheid en het doelmatig gebruik ervan zijn vastgesteld door middel van technische uitvoeringsmaatregelen overeenkomstig artikel 4 van Beschikking nr. 676/2002/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een regelgevingskader voor het radiospectrumbeleid in de Europese Gemeenschap, hierna te noemen "Radiospectrumbeschikking";
33/4° "gedeeld gebruik van radiospectrum": toegang door twee of meer gebruikers om gebruik te maken van dezelfde radiospectrumbanden in het kader van een bepaalde regeling inzake gedeeld gebruik, toegestaan op basis van een algemene machtiging, gebruiksrechten voor radiospectrum of een combinatie daarvan, met inbegrip van regelgevingsbenaderingen, zoals vergunningsplichtige gedeelde toegang, die als doel hebben het gedeeld gebruik van een radiospectrumband te vergemakkelijken, en onderworpen aan een bindende overeenkomst tussen alle betrokken partijen, overeenkomstig de regels inzake gedeeld gebruik die zijn opgenomen in hun gebruiksrechten voor radiospectrum, zodat aan alle gebruikers voorspelbare en betrouwbare regelingen inzake delen kunnen worden gewaarborgd, en zonder afbreuk te doen aan de toepassing van het mededingingsrecht;	33/4° "gedeeld gebruik van radiospectrum": toegang door twee of meer gebruikers om gebruik te maken van dezelfde radiospectrumbanden in het kader van een bepaalde regeling inzake gedeeld gebruik, toegestaan op basis van een algemene machtiging, gebruiksrechten voor radiospectrum of een combinatie daarvan, met inbegrip van regelgevingsbenaderingen, zoals vergunningsplichtige gedeelde toegang, die als doel hebben het gedeeld gebruik van een radiospectrumband te vergemakkelijken, en onderworpen aan een bindende overeenkomst tussen alle betrokken partijen, overeenkomstig de regels inzake gedeeld gebruik die zijn opgenomen in hun gebruiksrechten voor radiospectrum, zodat aan alle gebruikers voorspelbare en betrouwbare regelingen inzake delen kunnen worden gewaarborgd, en zonder afbreuk te doen aan de toepassing van het mededingingsrecht;
33/5° "gebruiksrechten voor radiospectrum": individuele gebruiksrechten voor radiospectrum die geheel of gedeeltelijk gebruikt worden voor het aanbieden van openbare elektronische communicatienetwerken of voor het publiek	33/5° "gebruiksrechten voor radiospectrum": individuele gebruiksrechten voor radiospectrum die geheel of gedeeltelijk gebruikt worden voor het aanbieden van openbare elektronische communicatienetwerken of voor het publiek

beschikbare elektronische communicatiediensten;	beschikbare elektronische communicatiediensten;
34° “radiocommunicatie”: communicatie door middel van radiogolven, met uitsluiting van de exclusieve transmissie van signalen van audiovisuele en auditieve mediadiensten;	34° “radiocommunicatie”: communicatie door middel van radiogolven, met uitsluiting van de exclusieve transmissie van signalen van audiovisuele en auditieve mediadiensten;
35° (opgeheven)	35° (opgeheven)
36° (opgeheven)	36° (opgeheven)
37° (opgeheven)	37° (opgeheven)
38° “radiostation”: radioapparatuur, eventueel aangevuld met antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van radiocommunicatie of radiodeterminatie;	38° “radiostation”: radioapparatuur, eventueel aangevuld met antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van radiocommunicatie of radiodeterminatie;
38/1° “radionet”: het geheel samengesteld uit verscheidene radiostations die met elkaar in verbinding mogen treden binnen de grenzen van een vergunning voor private radiocommunicatie of een gebruiksrecht voor radiospectrum;	38/1° “radionet”: het geheel samengesteld uit verscheidene radiostations die met elkaar in verbinding mogen treden binnen de grenzen van een vergunning voor private radiocommunicatie of een gebruiksrecht voor radiospectrum;
38/2° “vergunning voor private radiocommunicatie”: vergunning om een radiostation of een radionetwerk te mogen gebruiken voor andere doeleinden dan het aanbieden van openbare elektronischecommunicatienetwerken of voor het publiek beschikbare elektronischecommunicatiediensten;	38/2° “vergunning voor private radiocommunicatie”: vergunning om een radiostation of een radionetwerk te mogen gebruiken voor andere doeleinden dan het aanbieden van openbare elektronischecommunicatienetwerken of voor het publiek beschikbare elektronischecommunicatiediensten;
38/3° “omroepstation”: radioapparatuur, eventueel aangevuld met de bijbehorende antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van het aanbieden van audiovisuele en auditieve mediadiensten;	38/3° “omroepstation”: radioapparatuur, eventueel aangevuld met de bijbehorende antennes alsook alle onderdelen die nodig zijn om het geheel te laten functioneren, dat doelbewust radiogolven uitzendt of ontvangt ten behoeve van het aanbieden van audiovisuele en auditieve mediadiensten;
38/4° “storing”: effect op de ontvangst in een radiocommunicatiesysteem van een niet-gewenste energie, te wijten aan een uitzending, aan een straling of aan een inductie (of aan een combinatie van die uitzendingen, stralingen of inducties), dat zich manifesteert door een verslechtering van de transmissiekwaliteit, een	38/4° “storing”: effect op de ontvangst in een radiocommunicatiesysteem van een niet-gewenste energie, te wijten aan een uitzending, aan een straling of aan een inductie (of aan een combinatie van die uitzendingen, stralingen of inducties), dat zich manifesteert door een verslechtering van de transmissiekwaliteit, een

vervorming of een verlies van informatie die men had kunnen verkrijgen indien die niet-gewenste energie er niet was geweest;	vervorming of een verlies van informatie die men had kunnen verkrijgen indien die niet-gewenste energie er niet was geweest;
39° " schadelijke storing " : storing die het functioneren van een radionavigatiedienst of van andere veiligheidsdiensten in gevaar brengt, of die een overeenkomstig de van toepassing zijnde voorschriften werkende radiocommunicatiedienst, dienst voor de verstrekking van audiovisuele en auditieve mediadiensten of elektronische-communicatiedienst ernstig verslechtert, hindert of herhaaldelijk onderbreekt;	39° " schadelijke storing " : storing die het functioneren van een radionavigatiedienst of van andere veiligheidsdiensten in gevaar brengt, of die een overeenkomstig de van toepassing zijnde voorschriften werkende radiocommunicatiedienst, dienst voor de verstrekking van audiovisuele en auditieve mediadiensten of elektronische-communicatiedienst ernstig verslechtert, hindert of herhaaldelijk onderbreekt;
40° " versleuteling " : alle diensten die de beginselen, middelen en methodes voor de omzetting van gegevens aanwenden met de bedoeling de semantische inhoud ervan te verbergen, de authenticiteit ervan vast te stellen, te verhinderen dat zij onopgemerkt worden gewijzigd, te verhinderen dat zij worden verworpen en te verhinderen dat zij zonder toestemming worden gebruikt;	40° " versleuteling " : alle diensten die de beginselen, middelen en methodes voor de omzetting van gegevens aanwenden met de bedoeling de semantische inhoud ervan te verbergen, de authenticiteit ervan vast te stellen, te verhinderen dat zij onopgemerkt worden gewijzigd, te verhinderen dat zij worden verworpen en te verhinderen dat zij zonder toestemming worden gebruikt;
41° " eindapparatuur " :	41° " eindapparatuur " :
a) de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar elektronische-communicatienetwerk zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen de eindapparaatuur en de interface van het net;	a) de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar elektronische-communicatienetwerk zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen de eindapparaatuur en de interface van het net;
b) satellietgrondstationapparatuur;	b) satellietgrondstationapparatuur;
42° "radioapparatuur" : elektrisch of elektronisch product dat doelbewust radiogolven uitzendt en/of ontvangt ten behoeve van radiocommunicatie, verstrekking van audiovisuele en auditieve mediadiensten of radiodeterminatie, of elektrisch of elektronisch product dat moet worden aangevuld met een accessoire, zoals een antenne, om doelbewust radiogolven uit te zenden of ontvangen ten behoeve van radiocommunicatie, verstrekking	42° "radioapparatuur" : elektrisch of elektronisch product dat doelbewust radiogolven uitzendt en/of ontvangt ten behoeve van radiocommunicatie, verstrekking van audiovisuele en auditieve mediadiensten of radiodeterminatie, of elektrisch of elektronisch product dat moet worden aangevuld met een accessoire, zoals een antenne, om doelbewust radiogolven uit te zenden of ontvangen ten behoeve van radiocommunicatie, verstrekking

van audiovisuele en auditieve mediadiensten en/of radiodeterminatie;	van audiovisuele en auditieve mediadiensten en/of radiodeterminatie;
43° " apparatuur " : alle producten die als radioapparatuur of als eindapparatuur, of als beide fungeren;	43° " apparatuur " : alle producten die als radioapparatuur of als eindapparatuur, of als beide fungeren;
44° " technische specificatie " : de omschrijving van de kenmerken van alle elektronische-communicatiediensten die via het netwerkaansluitpunt of de radiointerface verstrekt worden;	44° " technische specificatie " : de omschrijving van de kenmerken van alle elektronische-communicatiediensten die via het netwerkaansluitpunt of de radiointerface verstrekt worden;
45° " nummeringsruimte " : het geheel van nummers, adressen en namen die aangewend worden om operatoren of gebruikers te identificeren;	45° " nummeringsruimte " : het geheel van nummers, adressen en namen die aangewend worden om operatoren of gebruikers te identificeren;
46 " geografisch nummer " : een nummer van het nationale nummerplan waarvan een deel van de cijferstructuur een geografische betekenis heeft die wordt gebruikt voor het routeren van gesprekken naar de fysieke locatie van het netwerkaansluitpunt;	46 " geografisch nummer " : een nummer van het nationale nummerplan waarvan een deel van de cijferstructuur een geografische betekenis heeft die wordt gebruikt voor het routeren van gesprekken naar de fysieke locatie van het netwerkaansluitpunt;
47° " niet-geografisch nummer " : een nummer van het nationale nummerplan dat geen geografisch nummer is; het betreft hier onder meer nummers voor mobiele oproepen, nummers die gratis zijn voor de oproepers en betaalnummers;	47° " niet-geografisch nummer " : een nummer van het nationale nummerplan dat geen geografisch nummer is; het betreft hier onder meer nummers voor mobiele oproepen, nummers die gratis zijn voor de oproepers en betaalnummers;
48° " nummeroverdraagbaarheid " : de faciliteit die het de abonnees [...] mogelijk maakt hun nummer te behouden, ongeacht de operator die de dienst levert, binnen een welbepaald geografisch gebied in geval van een geografisch nummer en op ongeacht welke locatie in geval van andere dan geografische nummers; de faciliteit omvat niet de mogelijkheid om het nationale telefoonnummer te behouden tussen een operator van voor het publiek beschikbare telefoondiensten aangeboden op een vaste locatie en een operator van oor het publiek beschikbare telefoondiensten aangeboden op een mobiel elektronisch communicatienetwerk;	48° " nummeroverdraagbaarheid " : de faciliteit die het de abonnees [...] mogelijk maakt hun nummer te behouden, ongeacht de operator die de dienst levert, binnen een welbepaald geografisch gebied in geval van een geografisch nummer en op ongeacht welke locatie in geval van andere dan geografische nummers; de faciliteit omvat niet de mogelijkheid om het nationale telefoonnummer te behouden tussen een operator van voor het publiek beschikbare telefoondiensten aangeboden op een vaste locatie en een operator van oor het publiek beschikbare telefoondiensten aangeboden op een mobiel elektronisch communicatienetwerk;
48/1° " Internetdomeinnaamregistreerbureau": een entiteit die een register van domeinnamen bijhoudt en die een systeem uitbaat zodat deze domeinnamen kunnen worden gebruikt om	48/1° " Internetdomeinnaamregistreerbureau": een entiteit die een register van domeinnamen bijhoudt en die een systeem uitbaat zodat deze domeinnamen kunnen worden gebruikt om

toegang te krijgen tot Internet- protocol-adressen of andere informatie via het Internet;	toegang te krijgen tot Internet- protocol-adressen of andere informatie via het Internet;
48/2° " universele dienst " : het minimumpakket van diensten als gedefinieerd in artikel 68 van een bepaalde kwaliteit dat voor alle gebruikers, ongeacht hun geografische locatie, beschikbaar is voor een in het licht van specifieke nationale omstandigheden betaalbare prijs;	48/2° " universele dienst " : het minimumpakket van diensten als gedefinieerd in artikel 68 van een bepaalde kwaliteit dat voor alle gebruikers, ongeacht hun geografische locatie, beschikbaar is voor een in het licht van specifieke nationale omstandigheden betaalbare prijs;
49° " telefoongids " : boek, lijst of bestand dat of die hoofdzakelijk of uitsluitend gegevens bevat over de abonnees van een openbare telefoondienst en die beschikbaar wordt gesteld voor het publiek om uitsluitend of hoofdzakelijk de oproepnummers van de eindgebruikers te kunnen identificeren;	49° " telefoongids " : boek, lijst of bestand dat of die hoofdzakelijk of uitsluitend gegevens bevat over de abonnees van een openbare telefoondienst en die beschikbaar wordt gesteld voor het publiek om uitsluitend of hoofdzakelijk de oproepnummers van de eindgebruikers te kunnen identificeren;
50° (opgeheven)	50° (opgeheven)
51° " antenne " : een onderdeel van een apparaat of radiostation voor het uitstralen en/of opvangen van radiogolven;	51° " antenne " : een onderdeel van een apparaat of radiostation voor het uitstralen en/of opvangen van radiogolven;
52° " basisstation " : een radiostation van een elektronische-communicatienetwerk opgesteld en gebruikt op een bepaalde plaats en bestemd voor radiodekking van een gegeven geografische zone;	52° " basisstation " : een radiostation van een elektronische-communicatienetwerk opgesteld en gebruikt op een bepaalde plaats en bestemd voor radiodekking van een gegeven geografische zone;
53° " steun " : structuur waarop antennes van basisstations kunnen worden geplaatst;	53° " steun " : structuur waarop antennes van basisstations kunnen worden geplaatst;
54° " antennesite " : geheel van constructies dat ten minste één steun, één antenne en lokalen omvat voor de elektrische en elektronische apparatuur, dat de installatie en de exploitatie van een of meer basisstations mogelijk maakt;	54° " antennesite " : geheel van constructies dat ten minste één steun, één antenne en lokalen omvat voor de elektrische en elektronische apparatuur, dat de installatie en de exploitatie van een of meer basisstations mogelijk maakt;
55° " nationale raming " : de mogelijkheid voor een operator om zijn klanten in staat te stellen in hetzelfde land toegang te krijgen tot de basisdiensten die verstrekt worden door een andere operator van een mobiel communicatienetwerk;	55° " nationale raming " : de mogelijkheid voor een operator om zijn klanten in staat te stellen in hetzelfde land toegang te krijgen tot de basisdiensten die verstrekt worden door een andere operator van een mobiel communicatienetwerk;
56° " identificatie van de lijn " : nummer, teken of geheel van tekens dat aan een abonnee, eindgebruiker, gebruiker of eindapparaat is toegewezen, waarmee deze door andere abonnees, eindgebruikers of gebruikers van	56° " identificatie van de lijn " : nummer, teken of geheel van tekens dat aan een abonnee, eindgebruiker, gebruiker of eindapparaat is toegewezen, waarmee deze door andere abonnees, eindgebruikers of gebruikers van

voor het publiek beschikbare elektronische-communicatienetwerken of -diensten kan worden bereikt;	voor het publiek beschikbare elektronische-communicatienetwerken of -diensten kan worden bereikt;
57° " identificatie van de oproeper " : elk gegeven, rechtstreeks of onrechtstreeks beschikbaar, in de netwerken en diensten van een operator, dat het oproepnummer van het eindapparaat, de naam van de eindgebruiker en de plaats waar de eindapparatuur zich bevindt op het ogenblik van de oproep bepaalt;	57° " identificatie van de oproeper " : elk gegeven, rechtstreeks of onrechtstreeks beschikbaar, in de netwerken en diensten van een operator, dat het oproepnummer van het eindapparaat, de naam van de eindgebruiker en de plaats waar de eindapparatuur zich bevindt op het ogenblik van de oproep bepaalt;
58° " nooddienst " : elke overheidsdienst of dienst van openbaar nut zoals geviseerd in artikel 107, § 1, eerste lid, of vastgesteld door de Koning overeenkomstig artikel 107, § 1, tweede lid, 1°;	58° " nooddienst " : elke overheidsdienst of dienst van openbaar nut zoals geviseerd in artikel 107, § 1, eerste lid, of vastgesteld door de Koning overeenkomstig artikel 107, § 1, tweede lid, 1°;
59° " noodnummer " : oproepnummer van een nooddienst, bepaald overeenkomstig de procedure in artikel 107, § 1, tweede lid, 2° van deze wet;	59° " noodnummer " : oproepnummer van een nooddienst, bepaald overeenkomstig de procedure in artikel 107, § 1, tweede lid, 2° van deze wet;
60° “noodcommunicatie”: communicatie door middel van interpersoonlijke communicatiediensten tussen een eindgebruiker en een PSAP met het doel noodhulp te ontvangen van hulpdiensten;	60° “noodcommunicatie”: communicatie door middel van interpersoonlijke communicatiediensten tussen een eindgebruiker en een PSAP met het doel noodhulp te ontvangen van hulpdiensten;
61° “PSAP” (“Public Safety Answering Point”) of “centrale voor het beheer van noodoproepen”: de fysieke locatie waar noodcommunicatie initieel wordt ontvangen onder de verantwoordelijkheid van een openbare instantie of een erkende private organisatie;	61° “PSAP” (“Public Safety Answering Point”) of “centrale voor het beheer van noodoproepen”: de fysieke locatie waar noodcommunicatie initieel wordt ontvangen onder de verantwoordelijkheid van een openbare instantie of een erkende private organisatie;
62° “werkingsgebied van een PSAP”: geografisch gebied waarvoor een PSAP alle noodcommunicatie naar de nooddienst beheert, hierna “werkingsgebied” genoemd;	62° “werkingsgebied van een PSAP”: geografisch gebied waarvoor een PSAP alle noodcommunicatie naar de nooddienst beheert, hierna “werkingsgebied” genoemd;
62/1° “meest geschikte PSAP”: een PSAP die door de bevoegde instanties is opgericht om noodcommunicatie uit een bepaald gebied of van een bepaald type te behandelen;	62/1° “meest geschikte PSAP”: een PSAP die door de bevoegde instanties is opgericht om noodcommunicatie uit een bepaald gebied of van een bepaald type te behandelen;
62/2° “beveiliging van netwerken en diensten”: het vermogen van elektronische-communicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de	62/2° “beveiliging van netwerken en diensten”: het vermogen van elektronische-communicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de

beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van die netwerken en diensten, van de opgeslagen, verzonden of verwerkte gegevens of van de daaraan gerelateerde diensten die via die elektronischecommunicatienetwerken en -diensten worden aangeboden, in gevaar brengen;	beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van die netwerken en diensten, van de opgeslagen, verzonden of verwerkte gegevens of van de daaraan gerelateerde diensten die via die elektronischecommunicatienetwerken en -diensten worden aangeboden, in gevaar brengen;
62/3° “beveiligingsincident”: een gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van elektronische communicatienetwerken of -diensten;	62/3° “beveiligingsincident”: een gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van elektronische communicatienetwerken of -diensten;
63° " erkend revisor " : bedrijfsrevisor ingeschreven op de rol van het Instituut voor Bedrijfsrevisoren;	63° " erkend revisor " : bedrijfsrevisor ingeschreven op de rol van het Instituut voor Bedrijfsrevisoren;
64° " ziekenhuizen " : de instellingen voor gezondheidszorg zoals bepaald in artikel 2 van de wet op de ziekenhuizen, gecoördineerd op 7 augustus 1987;	64° " ziekenhuizen " : de instellingen voor gezondheidszorg zoals bepaald in artikel 2 van de wet op de ziekenhuizen, gecoördineerd op 7 augustus 1987;
65° " scholen " : alle instellingen van het lager, secundair of hoger onderwijs die behoren tot het net van een Gemeenschap, van een provincie, van een gemeente of tot een vrij gesubsidieerd net;	65° " scholen " : alle instellingen van het lager, secundair of hoger onderwijs die behoren tot het net van een Gemeenschap, van een provincie, van een gemeente of tot een vrij gesubsidieerd net;
66° " openbare bibliotheken " : elke bibliotheek erkend door de federale Staat of door een Gemeenschap;	66° " openbare bibliotheken " : elke bibliotheek erkend door de federale Staat of door een Gemeenschap;
67° " openbaar bureau voor elektronische communicatie " : voor het publiek toegankelijke ruimte of inrichting voor de tijdelijke beschikbaarstelling van eindapparatuur waarmee tegen betaling een elektronische-communicatienetwerk of -dienst ter plaatse kan worden gebruikt zonder contractuele betrekking met de leverancier van het netwerk of de dienst;	67° " openbaar bureau voor elektronische communicatie " : voor het publiek toegankelijke ruimte of inrichting voor de tijdelijke beschikbaarstelling van eindapparatuur waarmee tegen betaling een elektronische-communicatienetwerk of -dienst ter plaatse kan worden gebruikt zonder contractuele betrekking met de leverancier van het netwerk of de dienst;
68° " inbreuk in verband met persoonsgegevens " : een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een voor het publiek	68° " inbreuk in verband met persoonsgegevens " : een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een voor het publiek

beschikbare elektronische-communicatiedienst in de Gemeenschap;	beschikbare elektronische-communicatiedienst in de Gemeenschap;
69° " ENISA " : Europees Agentschap voor netwerk- en informatiebeveiliging opgericht door Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging;	69° " ENISA " : Europees Agentschap voor netwerk- en informatiebeveiliging opgericht door Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging;
70° "Berec": Orgaan van Europese regelgevende instanties voor elektronische communicatie, in het Engels "Body of European Regulators for Electronic Communications (Berec)", opgericht door Verordening (EU) 2018/1971 van het Europees Parlement en de Raad van 11 december 2018 tot instelling van het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec) en het Bureau voor ondersteuning van Berec (Berec-Bureau), tot wijziging van Verordening (EU) 2015/2120 en tot intrekking van Verordening (EG) nr. 1211/2009, hierna "Verordening (EU) 2018/1971" genoemd;	70° "Berec": Orgaan van Europese regelgevende instanties voor elektronische communicatie, in het Engels "Body of European Regulators for Electronic Communications (Berec)", opgericht door Verordening (EU) 2018/1971 van het Europees Parlement en de Raad van 11 december 2018 tot instelling van het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec) en het Bureau voor ondersteuning van Berec (Berec-Bureau), tot wijziging van Verordening (EU) 2015/2120 en tot intrekking van Verordening (EG) nr. 1211/2009, hierna "Verordening (EU) 2018/1971" genoemd;
71° "Bureau": Bureau voor ondersteuning van Berec, ingesteld door de Verordening (EU) 2018/1971;	71° "Bureau": Bureau voor ondersteuning van Berec, ingesteld door de Verordening (EU) 2018/1971;
71/1° "RSPG": Beleidsgroep radiospectrum, in het Engels "Radio Spectrum Policy Group", opgericht bij besluit van de Europese Commissie van 11 juni 2019 tot oprichting van de Beleidsgroep radiospectrum en tot intrekking van Besluit 2002/622/EG;	71/1° "RSPG": Beleidsgroep radiospectrum, in het Engels "Radio Spectrum Policy Group", opgericht bij besluit van de Europese Commissie van 11 juni 2019 tot oprichting van de Beleidsgroep radiospectrum en tot intrekking van Besluit 2002/622/EG;
72° " Prioritair gebruiker " : gebruiker van elektronische-communicatiediensten of -netwerken die door de taken die hij uitoefent of zijn activiteiten een door de overheden erkende belangrijke maatschappelijke functie heeft en die door een gebrek aan toegang tot elektronische-communicatiediensten of -netwerken niet meer in staat is zijn taken of activiteiten adequaat uit te voeren wat tot een toestand kan leiden die de openbare veiligheid, of de civiele veiligheid en de civiele bescherming, of de civiele verdediging, of de crisisplanning, of de veiligheid of de bescherming van het economische en	72° " Prioritair gebruiker " : gebruiker van elektronische-communicatiediensten of -netwerken die door de taken die hij uitoefent of zijn activiteiten een door de overheden erkende belangrijke maatschappelijke functie heeft en die door een gebrek aan toegang tot elektronische-communicatiediensten of -netwerken niet meer in staat is zijn taken of activiteiten adequaat uit te voeren wat tot een toestand kan leiden die de openbare veiligheid, of de civiele veiligheid en de civiele bescherming, of de civiele verdediging, of de crisisplanning, of de veiligheid of de bescherming van het economische en

wetenschappelijke potentieel van het land, kan schaden;	wetenschappelijke potentieel van het land, kan schaden;
73° (opgeheven)	73° (opgeheven)
74° (vernietigd door het Grondwettelijk Hof)	**74° "Oproeppoging zonder resultaat": iedere communicatie waarbij een oproep wel werd doorgezonden, maar onbeantwoord is gebleven of door de netwerkbeheerder is beantwoord;**
75° "radiodeterminatie" : het vaststellen van de positie, snelheid en/of andere kenmerken van een object of het verkrijgen van informatie over deze parameters door middel van de voortplantingseigenschappen van radiogolven;	75° "radiodeterminatie" : het vaststellen van de positie, snelheid en/of andere kenmerken van een object of het verkrijgen van informatie over deze parameters door middel van de voortplantingseigenschappen van radiogolven;
76° "op de markt aanbieden" : het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van radioapparatuur met het oog op distributie, consumptie of gebruik op de markt van de Unie;	76° "op de markt aanbieden" : het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van radioapparatuur met het oog op distributie, consumptie of gebruik op de markt van de Unie;
77° "in de handel brengen" : het voor het eerst in de Unie op de markt aanbieden van radioapparatuur;	77° "in de handel brengen" : het voor het eerst in de Unie op de markt aanbieden van radioapparatuur;
78° "ingebruikneming" : het eerste gebruik van radioapparatuur in de Unie door de eindgebruiker ervan;	78° "ingebruikneming" : het eerste gebruik van radioapparatuur in de Unie door de eindgebruiker ervan;
79° "fabrikant" : natuurlijke of rechtspersoon die radioapparatuur vervaardigt of laat ontwerpen of vervaardigen, en deze apparatuur onder zijn naam of merknaam verhandelt;	79° "fabrikant" : natuurlijke of rechtspersoon die radioapparatuur vervaardigt of laat ontwerpen of vervaardigen, en deze apparatuur onder zijn naam of merknaam verhandelt;
80° "invoerder" : in de Europese Unie gevestigde natuurlijke of rechtspersoon die radioapparatuur uit een derde land in de Europese Unie in de handel brengt;	80° "invoerder" : in de Europese Unie gevestigde natuurlijke of rechtspersoon die radioapparatuur uit een derde land in de Europese Unie in de handel brengt;
81° "distributeur" : natuurlijke of rechtspersoon in de toeleveringsketen, verschillend van de fabrikant of de invoerder, die radioapparatuur op de markt aanbiedt;	81° "distributeur" : natuurlijke of rechtspersoon in de toeleveringsketen, verschillend van de fabrikant of de invoerder, die radioapparatuur op de markt aanbiedt;
82° "terugroepen" : maatregel waarmee wordt beoogd radioapparatuur te doen terugkeren die al aan de eindgebruiker ter beschikking is gesteld;	82° "terugroepen" : maatregel waarmee wordt beoogd radioapparatuur te doen terugkeren die al aan de eindgebruiker ter beschikking is gesteld;

83° "uit de handel nemen" : maatregel waarmee wordt beoogd te voorkomen dat radioapparatuur die zich in de toeleveringsketen bevindt, op de markt wordt aangeboden;	83° "uit de handel nemen" : maatregel waarmee wordt beoogd te voorkomen dat radioapparatuur die zich in de toeleveringsketen bevindt, op de markt wordt aangeboden;
84° "radio-interface" : specificatie van het gereguleerd gebruik van het radiospectrum;	84° "radio-interface" : specificatie van het gereguleerd gebruik van het radiospectrum;
85° "dienstenaanbieder" : persoon wiens dienst of inhoud geleverd via een elektronische-communicatienetwerk door een operator aan de eindgebruiker in rekening wordt gebracht;	85° "dienstenaanbieder" : persoon wiens dienst of inhoud geleverd via een elektronische-communicatienetwerk door een operator aan de eindgebruiker in rekening wordt gebracht;
86° "faciliterende operator" : operator die nummers of andere middelen ter beschikking stelt van een dienstenaanbieder, zodat deze een vergoeding voor zijn dienst of inhoud kan laten invorderen via facturatie door een operator of aanrekening op een voorafbetaalde kaart van een operator.	86° "faciliterende operator" : operator die nummers of andere middelen ter beschikking stelt van een dienstenaanbieder, zodat deze een vergoeding voor zijn dienst of inhoud kan laten invorderen via facturatie door een operator of aanrekening op een voorafbetaalde kaart van een operator.
87° “passieve infrastructuur”: elk element van een elektronischecommunicatienetwerk dat bedoeld is om er andere elementen van een ander elektronische-communicatienetwerk in onder te brengen zonder dat het zelf een actief element van dat laatste netwerk wordt, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens of palen;	87° “passieve infrastructuur”: elk element van een elektronischecommunicatienetwerk dat bedoeld is om er andere elementen van een ander elektronische-communicatienetwerk in onder te brengen zonder dat het zelf een actief element van dat laatste netwerk wordt, zoals buizen, masten, kabelgoten, inspectieputten, mangaten, straatkasten, gebouwen of ingangen in gebouwen, antenne-installaties, torens of palen;
88° “centraal informatiepunt”: het informatiesysteem ingevoerd binnen het platform van de vzw “KLIM-CICC (Federaal Kabels en Leidingen Informatie Meldpunt – Point de Contact fédéral Information Câbles et Conduites).	88° “centraal informatiepunt”: het informatiesysteem ingevoerd binnen het platform van de vzw “KLIM-CICC (Federaal Kabels en Leidingen Informatie Meldpunt – Point de Contact fédéral Information Câbles et Conduites).
89° (Binnenkort)	
90° (Binnenkort)	
	91° "elektronische-communicatiegegevens": de inhoud en de metagegevens van elektronische communicatie;”
	92° "inhoud van elektronische communicatie": de inhoud die wordt uitgewisseld door middel

	van elektronische-communicatiediensten, met name tekst, spraak, video, beelden en geluid;
	93° "metagegevens van elektronische communicatie": de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie; met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie.
TITRE IV. De bescherming van de belangen van de maatschappij en van de gebruikers	TITRE IV. De bescherming van de belangen van de maatschappij en van de gebruikers
HOOFDSTUK II/1. - Veiligheid van de elektronische communicatie	HOOFDSTUK II/1. - Veiligheid van de elektronische communicatie
Art. 107/5	**Art. 107/5**
Het gebruik van versleuteling is vrij.	**§ 1. Ter bevordering van de digitale veiligheid is het gebruik van versleuteling vrij binnen de in de paragrafen 2 tot en met 4 gestelde grenzen.**
De terbeschikkingstelling aan het publiek van versleutelingsdiensten aangewezen door de Koning, na advies van het Instituut, is onderworpen aan een voorafgaande kennisgeving aan het Instituut.	**§ 2. Het gebruik van versleuteling mag noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of het verstrekken van de identificatiegegevens van de oproeper, niet verhinderen.**
De Koning legt na advies van het Instituut de inhoud en de vorm van die kennisgeving vast.	**§ 3. Het gebruik van versleuteling door een operator, met als doel de veiligheid van de communicatie te waarborgen, mag geen beletsel vormen voor de uitvoering van een gericht verzoek van een bevoegde autoriteit, onder de bij wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie.**
	§ 4. Het gebruik van versleuteling door een buitenlandse operator, wiens eindgebruiker of

	abonnee zich op het Belgisch grondgebied bevindt, mag de uitvoering van een verzoek van een bevoegde overheid, zoals bedoeld in de paragrafen 2 tot 3, niet verhinderen.
	Elk contractueel beding dat door de operatoren wordt opgesteld en de uitvoering van dit lid belemmert, is verboden en van rechtswege nietig.
Onderafdeling 7. - Diverse bepalingen.	Onderafdeling 7. - Diverse bepalingen.
	Art. 121/8
	§ 1. Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden.
	De Koning kan de door de operatoren krachtens het eerste lid te treffen maatregelen preciseren.
	Het Instituut is bevoegd om bindende instructies te geven, met inbegrip van instructies betreffende de uitvoeringstermijnen, met het oog op de toepassing van deze paragraaf.
	§ 2. Wanneer dat gerechtvaardigd is ten aanzien van de ernst van de omstandigheden, die per geval onderzocht moeten worden, kunnen de in paragraaf 1, eerste lid, bedoelde passende maatregelen met name het volgende omvatten:
	- **Maatregelen op netwerkniveau, zoals de blokkering van nummers, diensten, URL's, domeinnamen, IP-adressen of elk ander element ter identificatie van de elektronische communicatie;**

	- **Maatregelen op het niveau van de eindgebruiker, zoals de volledige of gedeeltelijke deactivering van bepaalde diensten of apparatuur.**
HOOFDSTUK III. - Bescherming van de eindgebruikers	HOOFDSTUK III. - Bescherming van de eindgebruikers
Afdeling 2. Geheimhouding van de communicatie, verwerking van de gegevens en bescherming van de persoonlijke levenssfeer	Afdeling 2. Geheimhouding van de communicatie, verwerking van de gegevens en bescherming van de persoonlijke levenssfeer
Art. 122	**Art. 122**
§ 1. De operatoren verwijderen de verkeersgegevens met betrekking tot abonnees of eindgebruikers uit hun verkeersgegevens of maken deze gegevens anoniem, zodra zij niet langer nodig zijn voor de transmissie van de communicatie.	§ 1. De operatoren verwijderen de verkeersgegevens met betrekking tot abonnees of eindgebruikers uit hun verkeersgegevens of maken deze gegevens anoniem, zodra zij niet langer nodig zijn voor de transmissie van de communicatie.
Het eerste lid is van toepassing onverminderd de naleving van de door of krachtens de wet vastgestelde verplichtingen inzake samenwerking met :	
1° de autoriteiten die bevoegd zijn voor het onderzoek en de vervolging van strafbare feiten;	
2° de ombudsdienst voor telecommunicatie voor het onderzoek naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst.	
3° de inlichtingen- en veiligheidsdiensten in het kader van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	
§ 2. In afwijking van § 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, verwerken en slaan de operatoren de volgende gegevens op :	**§ 2. In afwijking van paragraaf 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken.**
1° de identificatie van de oproeplijn;	
2° het adres van de abonnee en van de plaats van de aansluiting, alsook het soort eindapparatuur;	

3° het totale aantal voor de berekeningsperiode aan te rekenen eenheden;	
4° de identificatie van de opgeroepen lijn;	
5° het type, het tijdstip van aanvang en de duur van de oproep of de verzonden hoeveelheid gegevens;	
6° de datum van de verbinding of van de dienst;	
7° andere gegevens betreffende betalingen, zoals vooruitbetaling, betaling in termijnen, afsluitingen en aanmaningen.	
Onverminderd de toepassing van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens stelt de operator de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan de verwerking in kennis van :	Onverminderd de toepassing **van de AVG en van de wet van 30 juli 2018** stelt de operator de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan de verwerking in kennis van:
1° de soorten verkeersgegevens die worden verwerkt;	1° de soorten verkeersgegevens die worden verwerkt;
2° de precieze doeleinden van de verwerking;	2° de precieze doeleinden van de verwerking;
3° de duur van de verwerking.	3° de duur van de verwerking.
De verwerking van de gegevens opgesomd in het eerste lid, is slechts toegestaan tot het einde van de periode van de betwisting van de factuur of tot het einde van de periode waarin de betaling gerechtelijk kan worden afgedwongen.	De verwerking van de gegevens **bedoeld** in het eerste lid, is slechts toegestaan tot het einde van de periode van de betwisting van de factuur of tot het einde van de periode waarin de betaling gerechtelijk kan worden afgedwongen.
§ 3. In afwijking van § 1 en met als enig doel de marketing te verzorgen van de eigen elektronische-communicatiediensten het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, op te stellen, of diensten met verkeersgegevens of locatiegegevens te leveren, mogen de operatoren de in § 1 bedoelde gegevens slechts verwerken onder de volgende voorwaarden :	§ 3. In afwijking van § 1 en met als enig doel de marketing te verzorgen van de eigen elektronische-communicatiediensten het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, op te stellen, of diensten met verkeersgegevens of locatiegegevens te leveren, mogen de operatoren de in § 1 bedoelde gegevens slechts verwerken onder de volgende voorwaarden :
1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de	1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de

gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking, in kennis van :	gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking, in kennis van :
a) de soorten verkeersgegevens die worden verwerkt;	a) de soorten verkeersgegevens die worden verwerkt;
b) de precieze doeleinden van de verwerking;	b) de precieze doeleinden van de verwerking;
c) de duur van verwerking.	c) de duur van verwerking.
2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.	2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.
Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat verkeersgegevens die op hem betrekking hebben worden verwerkt.	Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan **de toestemming in de zin van artikel 4 van de AVG.**
3° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om op eenvoudige wijze de gegeven toestemming in te trekken.	3° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om **makkelijk en te allen tijde** de gegeven toestemming in te trekken.
4° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens voor het opstellen van het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, of voor de marketingactie in kwestie.	4° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens voor het opstellen van het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, of voor de marketingactie in kwestie.
Deze voorwaarden zijn van toepassing onverminderd de bijkomende voorwaarden die voortvloeien uit de toepassing van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.	Deze voorwaarden zijn van toepassing onverminderd de bijkomende voorwaarden die voortvloeien uit de toepassing **van de AVG en van de wet van 30 juli 2018**.
§ 4. In afwijking van § 1 kunnen de gegevens worden verwerkt om eventuele fraude op te sporen.	**§ 4. In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en**

	de herkomst ervan te kunnen identificeren, dient de operator:
De gegevens worden ingeval van strafbaar feit aan de bevoegde autoriteiten meegedeeld.	
	1° de gegevens opgenomen in de "Call detail record" (CDR) of in een functioneel gelijkwaardig register te bewaren, alsook de locatiegegevens van de dader van de vermeende fraude of het vermeende kwaadwillige gebruik van het netwerk wanneer deze beschikbaar zijn, gedurende 4 maanden vanaf de datum van de communicatie;
	2° gedurende 12 maanden vanaf de datum van de communicatie de verkeersgegevens betreffende de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten te bewaren;
	3° de in 1° bedoelde gegevens die betrekking hebben op een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk te bewaren gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van 4 maanden zoals bedoeld in 1°;
	4° de verkeersgegevens bedoeld in 2° en met betrekking tot een specifiek kwaadwillig gebruik van het netwerk te bewaren gedurende de periode die nodig is voor de verwerking ervan, in voorkomend geval langer dan de termijn van 12 maanden zoals bedoeld in 2°;
	5° de noodzakelijke verkeersgegevens daartoe te verwerken, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.
	In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en

	verwerken, die voor deze doeleinden nodig worden geacht.
	De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de doeleinden waarin deze paragraaf voorziet, preciseren en uitbreiden.
	In geval van vermeende fraude of van vermeend kwaadwillig gebruik, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermeende fraude of het vermeende kwaadwillig gebruik doorsturen.";
	§ 4/1. In afwijking van paragraaf 1 mogen de operatoren die verkeersgegevens bewaren en verwerken die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.
	Zij mogen deze bewaren voor een duur van twaalf maanden vanaf de datum van de communicatie.
	Ze mogen de in het eerste lid bedoelde gegevens met betrekking tot een specifieke schending van de veiligheid van het netwerk bewaren gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van 12 maanden zoals bedoeld in het tweede lid.
	In geval van schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten doorsturen.

	§ 4/2. In afwijking van paragraaf 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm, voor de daartoe benodigde duur.
§ 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van klanten, de opsporing van fraude, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten met verkeersgegevens of locatiegegevens.	**§ 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten die gebruik maken van verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel.**
De verwerking is beperkt tot hetgeen strikt noodzakelijk is om die activiteiten te verrichten.	
§ 6. Het Instituut, de Belgische Mededingingsautoriteit, de rechtscolleges van de rechterlijke orde en de Raad van State kunnen in het kader van hun bevoegdheden in kennis worden gesteld van de relevante verkeers- en rekeninggegevens met het oog op het beslechten van geschillen, waaronder geschillen met betrekking tot interconnectie en facturering.	§ 6. **Het Instituut, de Ombudsdienst voor telecommunicatie,** de Belgische Mededingingsautoriteit, de rechtscolleges van de rechterlijke orde en de Raad van State kunnen in het kader van hun bevoegdheden in kennis worden gesteld van de relevante verkeers- en rekeninggegevens met het oog op het beslechten van geschillen, waaronder geschillen met betrekking tot interconnectie en facturering.
Art. 123	**Art. 123**
§ 1. Onverminderd de toepassing van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens mogen de operatoren van mobiele netwerken locatiegegevens die betrekking hebben op een abonnee of een eindgebruiker slechts verwerken wanneer zij anoniem gemaakt zijn of wanneer de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens.	**§ 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen:**

	1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard gedurende maximaal 12 maanden vanaf de datum van de communicatie, tenzij in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;
	2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, waarbij de gegevens worden bewaard gedurende maximaal 4 maanden vanaf de datum van de communicatie, tenzij in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;
	3° wanneer de gegevens anoniem gemaakt zijn;
	4° wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens;
	5° wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm.
§ 2. De verwerking in het kader van de levering van een dienst gebaseerd op verkeersgegevens of locatiegegevens is onderworpen aan de volgende voorwaarden :	§ 2. De verwerking in het kader van de levering van een dienst gebaseerd op verkeersgegevens of locatiegegevens is onderworpen aan de volgende voorwaarden :
1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking in kennis van :	1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking in kennis van :
a) de soorten locatiegegevens die worden verwerkt;	a) de soorten locatiegegevens die worden verwerkt;
b) de precieze doeleinden van de verwerking;	b) de precieze doeleinden van de verwerking;
c) de duur van de verwerking;	c) de duur van de verwerking;
d) de eventuele derden waaraan deze gegevens zullen worden doorgegeven;	d) de eventuele derden waaraan deze gegevens zullen worden doorgegeven;

e) de mogelijkheid om te allen tijde de gegeven toestemming voor de verwerking definitief of tijdelijk in te trekken.	e) de mogelijkheid om te allen tijde de gegeven toestemming voor de verwerking definitief of tijdelijk in te trekken.
2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.	2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.
Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat locatiegegevens die op hem betrekking hebben worden verwerkt.	Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan **de toestemming in de zin van artikel 4 van de AVG.**
3° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens.	3° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens.
4° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om te allen tijde op eenvoudige wijze de gegeven toestemming, definitief of tijdelijk, in te trekken.	4° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om te allen tijde op eenvoudige wijze de gegeven toestemming, definitief of tijdelijk, in te trekken.
§ 4. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst met verkeersgegevens of locatiegegevens levert.	**§ 4. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst die gebruik maakt van verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator waarvan sprake in artikel 127/3.**
De verwerking is beperkt tot hetgeen strikt noodzakelijk is om de betrokken dienst met verkeersgegevens of locatiegegevens aan te kunnen bieden.	De verwerking is beperkt tot hetgeen strikt noodzakelijk is om de betrokken dienst met verkeersgegevens of locatiegegevens aan te kunnen bieden.
§ 5. In geval van een noodcommunicatie naar de beheercentrales van de nooddiensten die ter plaatse hulp bieden, heffen de operatoren in zoverre dit technisch mogelijk is, met als doel de behandeling van de noodcommunicatie door de betrokken beheercentrales mogelijk te maken, de tijdelijke weigering of het ontbreken van toestemming van de abonnee of de eindgebruiker betreffende de verwerking van	§ 5. In geval van een noodcommunicatie naar de beheercentrales van de nooddiensten die ter plaatse hulp bieden, heffen de operatoren in zoverre dit technisch mogelijk is, met als doel de behandeling van de noodcommunicatie door de betrokken beheercentrales mogelijk te maken, de tijdelijke weigering of het ontbreken van toestemming van de abonnee of de eindgebruiker betreffende de verwerking van

lokalisatiegegevens per afzonderlijke, oproepende lijn, op.	lokalisatiegegevens per afzonderlijke, oproepende lijn, op.
Die opheffing is gratis	Die opheffing is gratis
Art. 125.§ 1. De bepalingen van artikel 124 van deze wet en de artikel en 259bis en 314bis van het Strafwetboek zijn niet van toepassing :	Art. 125.§ 1. De bepalingen van artikel 124 van deze wet en de artikel en 259bis en 314bis van het Strafwetboek zijn niet van toepassing :
1° wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt;	1° wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt;
2° wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische-communicatiedienst te garanderen;	2° wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische-communicatiedienst te garanderen;
3° wanneer de handelingen worden gesteld om de interventie van hulp- en nooddiensten mogelijk te maken die antwoorden op aan hen gerichte verzoeken om hulp;	3° wanneer de handelingen worden gesteld om de interventie van hulp- en nooddiensten mogelijk te maken die antwoorden op aan hen gerichte verzoeken om hulp;
4° wanneer de handelingen door het Instituut worden gesteld op bevel van de onderzoeksrechter, van de procureur des Konings, op verzoek van het diensthoofd bedoeld in artikel 3, 8°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, van de officier van gerechtelijke politie van de cel Vermiste Personen van de federale politie in het kader van zijn opdrachten en/of in het kader van zijn algemene opdracht inzake toezicht en controle;	4° wanneer de handelingen door het Instituut worden gesteld op bevel van de onderzoeksrechter, van de procureur des Konings, op verzoek van het diensthoofd bedoeld in artikel 3, 8°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, van de officier van gerechtelijke politie van de cel Vermiste Personen van de federale politie in het kader van zijn opdrachten en/of in het kader van zijn algemene opdracht inzake toezicht en controle;
5° wanneer de handelingen door de ombudsdienst voor telecommunicatie of op zijn verzoek worden gesteld in het kader van zijn wettelijke onderzoeksopdrachten en niet het afluisteren van communicaties betreffen;	5° wanneer de handelingen door de ombudsdienst voor telecommunicatie of op zijn verzoek worden gesteld in het kader van zijn wettelijke onderzoeksopdrachten en niet het afluisteren van communicaties betreffen;
5° /1: wanneer de handelingen worden uitgevoerd door de ambtenaren die zijn gemachtigd door de minister die de economie onder zijn bevoegdheden heeft, in het kader van hun wettelijke bevoegdheden tot opsporing en niet het afluisteren van communicaties betreffen;	5° /1: wanneer de handelingen worden uitgevoerd door de ambtenaren die zijn gemachtigd door de minister die de economie onder zijn bevoegdheden heeft, in het kader van hun wettelijke bevoegdheden tot opsporing en niet het afluisteren van communicaties betreffen;
5°/2 (opgeheven)	5°/2 (opgeheven)

6° wanneer de handelingen worden gesteld met als enig doel de eindgebruiker diensten aan te bieden die erin bestaan het ontvangen van ongewenste elektronische communicatie te verhinderen, mits hiertoe de nodige toestemming werd verkregen van de eindgebruiker.	6° wanneer de handelingen worden gesteld met als enig doel de eindgebruiker diensten aan te bieden die erin bestaan het ontvangen van ongewenste elektronische communicatie te verhinderen, mits hiertoe de nodige toestemming werd verkregen van de eindgebruiker.
7° wanneer de handelingen worden gesteld door operatoren met als enig doel het bestrijden van fraude gepleegd door middel van berichten die gebruik maken van telefoonnummers zoals sms en mms en onder de volgende voorwaarden:	7° wanneer de handelingen worden gesteld door operatoren met als enig doel het bestrijden van fraude gepleegd door middel van berichten die gebruik maken van telefoonnummers zoals sms en mms en onder de volgende voorwaarden:
a) de handelingen blijven beperkt tot het machinaal onderzoeken van de berichten om fraude vast te stellen; een menselijke tussenkomst is uitsluitend toegestaan om de goede werking van de computeralgoritmes te controleren;	a) de handelingen blijven beperkt tot het machinaal onderzoeken van de berichten om fraude vast te stellen; een menselijke tussenkomst is uitsluitend toegestaan om de goede werking van de computeralgoritmes te controleren;
b) de operatoren zijn transparant tegenover de eindgebruikers zodat voor hen duidelijk is dat berichten machinaal kunnen worden onderzocht in het kader van fraudebestrijding;	b) de operatoren zijn transparant tegenover de eindgebruikers zodat voor hen duidelijk is dat berichten machinaal kunnen worden onderzocht in het kader van fraudebestrijding;
c) de betrokken gegevens mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de fraudebestrijding;	c) de betrokken gegevens mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de fraudebestrijding;
d) de verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de fraudebestrijding of tot het einde van de periode waarin een gerechtelijke betwisting mogelijk is.	d) de verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de fraudebestrijding of tot het einde van de periode waarin een gerechtelijke betwisting mogelijk is.
Indien het in het eerste lid, 7°, *a)*, bedoelde onderzoek fraude aantoont, nemen operatoren concrete maatregelen om de fraude te bestrijden, zoals het blokkeren van de berichten of in de berichten het vervangen van URL's die doorverwijzen naar een frauduleuze website door een waarschuwingsboodschap of een URL met waarschuwingsboodschap.	Indien het in het eerste lid, 7°, *a)*, bedoelde onderzoek fraude aantoont, nemen operatoren concrete maatregelen om de fraude te bestrijden, zoals het blokkeren van de berichten of in de berichten het vervangen van URL's die doorverwijzen naar een frauduleuze website door een waarschuwingsboodschap of een URL met waarschuwingsboodschap.
Voor 1 februari bezorgen de operatoren het Instituut een jaarlijks verslag waarin minstens aan bod komen de maatregelen die zij het afgelopen jaar genomen hebben om fraude te	Voor 1 februari bezorgen de operatoren het Instituut een jaarlijks verslag waarin minstens aan bod komen de maatregelen die zij het afgelopen jaar genomen hebben om fraude te

bestrijden, de effectiviteit ervan alsook de evoluties inzake fraude.	bestrijden, de effectiviteit ervan alsook de evoluties inzake fraude.
§ 2. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels en de middelen die moeten worden ingezet om het identificeren, het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van elektronische communicatie mogelijk te maken. *De opheffing van deze paragraaf door de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische, werd nietig verklaard door het Grondwettelijk Hof.*	
Art. 126	**Art. 126**
Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de Minister van Justitie en van de minister en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst.	**§ 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten bieden, alsook de operatoren die de elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de door de Koning opgesomde gegevens, waarbij het besluit wordt genomen na advies van de Gegevensbeschermingsautoriteit en van het Instituut.**
De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut.	**Dat besluit mag niets anders bevatten dan de abonnementsgegevens van de abonnee inzake de dienst alsook de gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren. Het besluit heeft geen betrekking op de inhoud van elektronische-communicatie, noch op de metagegevens van de elektronische communicatie die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de**

	communicatie, of over de locatie van de eindapparatuur.
De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België.	**Onder abonnementsgegevens wordt verstaan de producten waarop de abonnee heeft ingetekend, het begin en het einde van de dienst alsook de identificatiecodes en verschillende nummers die eraan zijn toegewezen bij de intekening op de dienst.**
	De operatoren bewaren de in het eerste lid bedoelde gegevens maar voor zover ze deze in het kader van de verstrekking van de elektronische-communicatienetwerken of -diensten in kwestie verwerken of ze genereren.
	§ 2. De operatoren bewaren de in paragraaf 1, eerste lid, beoogde gegevens vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is.
	In afwijking van het eerste lid bewaren de operatoren de andere IP-adressen aan de bron van de verbinding dan diegene die is gebruikt om in te tekenen op de dienst, alsook de overige technische identificatiegegevens van de eindgebruikers, van de eindtoestellen of van de gebruikte elektronische-communicatiedienst, waarvan de lijst wordt vastgesteld door de Koning, tot twaalf maanden na het einde van de sessie.
	§ 3. De Koning bepaalt, na advies van de Gegevensbeschermingsautoriteit en van het Instituut, de vereisten waaraan de in paragraaf 1, eerste lid, bedoelde gegevens moeten beantwoorden.
Opmerking: de wijzigingen die de wet van 1 september 2016 heeft aangebracht in artikel 127, werden vernietigd door het Grondwettelijk Hof in zijn arrest nr. 158/2021 van 18 november 2021. In dat arrest handhaaft het Hof evenwel de gevolgen van de vernietigde bepalingen tot de inwerkingtreding van een wettelijke regeling die deze identificatiegegevens en identificatiedocumenten opsomt, en uiterlijk tot en met 31 december 2022.	

Art. 126/1	Art. 126/1
In zijn arrest nr. 57/2021 van 22 april 2021 (BS 28/06/2021, blz. 65587) heeft het Grondwettelijk Hof dit artikel vernietigd.	**§ 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden, de in paragraaf 2 bedoelde gegevens voor de geografische zones bedoeld in paragraaf 3, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in huidig artikel.**
	Elke operator bewaart de gegevens die door hem gegenereerd of verwerkt zijn in het kader van de verstrekking van de betrokken elektronische-communicatiediensten en -netwerken.
	Deze gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.
	§ 2. De gegevens bedoeld in paragraaf 1 zijn de gegevens bepaald door de Koning, bij een in Ministerraad overlegd besluit, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en van de minister, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, en die behoren tot de volgende categorie:
	De metagegevens van elektronische communicatie, met inbegrip van de herkomst en de bestemming van de communicatie, de plaats van de eindapparatuur tijdens de communicatie, en de metagegevens van oproeppogingen zonder resultaat, voor zover die laatste gegevens in het kader van de aanbieding van de bedoelde elektronische-communicatiediensten:
	i° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren; of

	ii° wat de internetgegevens betreft, door deze operatoren worden gelogd.
	De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten bepalen waaraan deze gegevens moeten beantwoorden.
	§ 3. De geografische zones waarbinnen de gegevens bedoeld in paragraaf 2 bewaard worden, zijn de volgende:
	1° de geografische zones bestaande uit:
	- **de gerechtelijke arrondissementen waar minstens 3 strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4 van het Wetboek van Strafvordering per 1000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;**
	- **de politiezones waar minstens 3 strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan 3 strafbare feiten zoals bedoeld in artikel 90ter, §§2 tot 4, van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de 3 voorbije kalenderjaren.**
	In het geval bedoeld in het eerste streepje bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2:
	a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90ter, §§2 tot 4, van het

	Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;
	b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;
	c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de 3 voorbije kalenderjaren.
	In het geval bedoeld in het tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in paragraaf 2:
	a) 6 maanden, indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;
	b) 9 maanden, indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren;
	c) 12 maanden, indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90ter, §§2 tot 4, van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld zijn in de drie voorbije kalenderjaren.
	Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet 5 bereikt.
	De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90ter, §§ 2 tot 4, van het Wetboek van Strafvordering per jaar per 1000 inwoners vastgesteld in de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals

	bedoeld in artikel 44/7 van de wet op het politieambt.
	De grenzen van de gerechtelijke arrondissementen bedoeld onder 1° zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.
	De grenzen van de politiezones bedoeld onder 1° zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.
	De directie, zoals bedoeld in artikel 44/11 van de wet op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.
	De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.
	Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.
	Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

	2° Alle geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2° van de wet van 10 juli 2006 betreffende de dreigingsanalyse, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de dreigingsanalyse, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.
	Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze de nodige maatregelen kan nemen om de operatoren in te lichten en tot een bewaring van de gegevens bedoeld in § 2 over te gaan voor het gehele grondgebied.
	De bewaarplicht bedoeld in het vorige lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het vorige lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.
	3° De gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:
	a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2., 3°, 4° en 5° van het Scheepvaartwetboek;

	b) de spoorwegstations in de zin van artikel 2, 5° van de Wet van 27 april 2018 houdende de spoorwegpolitie;
	c) de metro- en de pre-metrostations;
	d) de luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad, alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden;
	e) de gebouwen bestemd voor de administratie van douane en accijnzen;
	f) de gevangenissen in de zin van artikel 2, 15°, van de Basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gesteld, bedoeld in artikel 606 van het Wetboek van Strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;
	g) de wapenkamers en schietstanden zoals bedoeld in artikel 2, punten 1 en 19 van de Wet van 8 juni 2006 houdende de economische en individuele activiteiten met wapens;
	h) de faciliteiten bedoeld in artikel 3.1.a) van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;
	i) de SEVESO-inrichtingen zoals bedoeld in het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

	j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren en de uitvoeringsbesluiten; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;
	k) de zetel van de nv Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en versleutelde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;
	l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid;
	m) in voorkomend geval, en onverminderd § 6, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.
	4° De zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:
	a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten en de ministeriële kabinetten;

	b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;
	c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;
	d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:
	i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;
	ii) de gemeentehuizen en de stadhuizen;
	iii) het koninklijk paleis;
	iv) de koninklijke domeinen;
	v) de gebouwen toegewezen aan de instellingen bedoeld in Titel III, hoofdstukken 5 tot 7 van de Grondwet;
	vi) de gemeenten waar zich militaire domeinen bevinden;
	vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;
	e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;
	f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale

	aangelegenheden, de volksgezondheid en de sociale zekerheid:
	i) de ziekenhuizen zoals bedoeld in artikel 2 van de Gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;
	ii) de Nationale Bank van België;
	g) in voorkomend geval, en onverminderd § 6, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.
	5° De zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:
	a) de ambassades en diplomatieke vertegenwoordigingen;
	b) de gebouwen bestemd voor de Europese Unie;
	c) de gebouwen en de infrastructuren bestemd voor de NAVO;
	d) de instellingen van de Europese Economische Ruimte;
	e) de instellingen van de Verenigde Naties;
	f) in voorkomend geval, en onverminderd § 6, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.
	Voor elke categorie van zone bedoeld in het eerste lid, 3° tot en met 5° bepaalt de Koning de omvang van de perimeter van de zone.
	Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in het eerste lid, punten 3° tot en met 5°, deelt jaarlijks op de

	door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.
	Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld in paragraaf 1 in deze zone zo spoedig mogelijk kan worden beëindigd.
	Met uitzondering van de in het eerste lid, punt 4°, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in het eerste lid, punten 3° tot en met 5°, waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.
	Het controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het gemotiveerde bevel geven dat bepaald geografische zones bedoeld in het eerste lid, punten 3° tot en met 5°, van de lijst geschrapt worden.
	Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vorige lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.
	Het ministerieel besluit bedoeld in het vorige lid wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.
	Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

	Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van huidig artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.
	§ 4. De operatoren bewaren de verkeersgegevens voor iedere communicatie of alle oproepen zonder resultaat die vanuit of naar een geografisch gebied als bedoeld in paragraaf 3 worden gevoerd.
	Indien de operator, als gevolg van de door hem gebruikte technologie, niet in staat is de eindapparatuur die betrokken is bij de communicatie, met inbegrip van de oproeppoging zonder resultaat, nauwkeuriger te lokaliseren dan de lokalisatie ervan op het nationale grondgebied, bewaart de operator de in paragraaf 2 bedoelde gegevens gedurende de kortste overeenkomstig huidig artikel bepaalde termijn, op voorwaarde dat overeenkomstig dit artikel het gehele nationale grondgebied gedekt is door een bewaarplicht. Indien niet aan deze voorwaarde is voldaan, bewaart de betrokken operator geen gegevens in uitvoering van huidig artikel.
	Wanneer de eindgebruiker zich tijdens een elektronische communicatie verplaatst, bewaart de operator de verkeersgegevens voor zover de eindgebruiker zich op een bepaald moment van de communicatie bevindt in een gebied bedoeld in paragraaf 3.
	De operatoren bewaren de gegevens met betrekking tot de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, die opgesomd zijn in het koninklijk besluit bedoeld in paragraaf 2, tweede lid, wanneer die apparatuur zich bevindt in een in paragraaf 3 bedoeld gebied.

	Om te bepalen of eindapparatuur zich in een geografisch gebied als bedoeld in paragraaf 3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens die beschikbaar zijn. Zij maken hiervoor, indien beschikbaar, gebruik van de satellietlocatie van eindapparatuur.
	Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot een in paragraaf 3 bedoelde zone, bewaart hij de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.
	Wanneer een aggregatiepunt van de operator, zoals een antenne, verschillende in paragraaf 3 bedoelde geografische gebieden dekt die onderworpen zijn aan een verschillende bewaringstermijn, bewaart de operator de gegevens voor dat aggregatiepunt gedurende de kortste bewaringstermijn.
	Wanneer op grond van dit artikel verschillende bewaringstermijnen van toepassing zijn op dezelfde gegevens, bewaren de operatoren de gegevens gedurende de kortste termijn.
	§ 5. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister, na raadpleging van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende bepalen:
	- de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in paragraaf 3 bedoelde zones;
	- de lijst van de verschillende autoriteiten die bevoegd zijn voor de in paragraaf 3, eerste lid, punten 2° tot en met 5° bedoelde aangelegenheden;

	- de modaliteiten voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de modaliteiten voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen;
	- in voorkomend geval, de bijkomende geografische zones bedoeld in paragraaf 3, eerste lid, punten 3°, m), 4°, g) en 5°,f).
	Elke drie jaar dient het koninklijk besluit bedoeld in het eerste lid, vierde streepje te worden hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 voor wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.
	§ 6. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité Inlichtingen en Veiligheid, en van het Instituut en de autoriteiten bevoegd voor de bescherming van de gegevens , jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 5 bedoelde koninklijk besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.
	In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 5 bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in paragraaf 3, eerste lid, punten 3° tot 5° en of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.
	Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het

	voorbereiden of plegen van daden van zware criminaliteit.
	Het evaluatieverslag bevat ook het percentage van het nationale grondgebied waarvoor de verplichting tot gegevensbewaring op basis van huidig artikel van toepassing is.
	Dit evaluatierapport wordt gestuurd naar het controleorgaan op de politionele informatie en naar het Vast Comité I.
Art. 127.	**Art. 127.**
§ 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren, aan de aanbieders bedoeld in artikel 126, § 1, eerste lid, de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken of aan de eindgebruikers worden opgelegd om :	§1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren, de verkoopkanalen van elektronische-communicatiediensten, de ondernemingen die een identificatiedienst verstrekken of aan de eindgebruikers worden opgelegd om :
1° in het kader van een noodoproep de oproeplijn te kunnen identificeren;	1° in het kader van een noodoproep de oproeplijn te kunnen identificeren;
2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
Wat de identificatie van de eindgebruiker betreft, is de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.	Wat de identificatie van de eindgebruiker betreft, is de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.
Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.	Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

Wanneer de eindgebruiker een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator, de aanbieder bedoeld in artikel 126, § 1, eerste lid, het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.	Wanneer de eindgebruiker een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator, de aanbieder bedoeld in artikel 126, § 1, eerste lid, het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.
Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator, naar de aanbieder bedoeld in artikel 126, § 1, eerste lid, of naar de onderneming die een identificatiedienst verstrekt.	Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator, naar de aanbieder bedoeld in artikel 126, § 1, eerste lid, of naar de onderneming die een identificatiedienst verstrekt.
Indien een rechtstreekse invoer in de computersystemen van de operator, van de aanbieder bedoeld in artikel 126, § 1, eerste lid, of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.	Indien een rechtstreekse invoer in de computersystemen van de operator, van de aanbieder bedoeld in artikel 126, § 1, eerste lid, of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.
De operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.	De operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.
De verzamelde identificatiegegevens en -documenten worden bewaard overeenkomstig artikel 126, § 3, eerste lid.	De verzamelde identificatiegegevens en -documenten worden bewaard overeenkomstig artikel 126, § 3, eerste lid.
De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren en de aanbieders bedoeld in artikel 126, § 1, eerste lid, aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.	De Koning bepaalt, na advies van het Instituut, de tarieven voor de vergoeding van de medewerking van de operatoren, aan de in het eerste lid, 2°, bedoelde verrichtingen alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen.
§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen,	§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen,

zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.	zijn verboden, **met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen, welke onder specifieke regels vallen die vastgesteld worden in artikel 107/5.**
§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele voor het publiek beschikbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.	§ 3. Totdat de maatregelen, bedoeld in § 1, in werking treden, is het verbod bedoeld in § 2 niet van toepassing op de mobiele voor het publiek beschikbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.
De in dit koninklijk besluit gedefinieerde, niet-geïdentificeerde eindgebruikers van voorafbetaalde kaarten die zijn gekocht voor de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, identificeren zich binnen de termijn die wordt vastgesteld door de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, waarbij deze termijn niet langer mag zijn dan zes maanden na de bekendmaking van het koninklijk besluit bedoeld in paragraaf 1. Het in paragraaf 2 bedoelde verbod geldt pas na het einde van de termijn die aan de eindgebruiker wordt toegestaan om zich te identificeren.	De in dit koninklijk besluit gedefinieerde, niet-geïdentificeerde eindgebruikers van voorafbetaalde kaarten die zijn gekocht voor de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, identificeren zich binnen de termijn die wordt vastgesteld door de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, waarbij deze termijn niet langer mag zijn dan zes maanden na de bekendmaking van het koninklijk besluit bedoeld in paragraaf 1. Het in paragraaf 2 bedoelde verbod geldt pas na het einde van de termijn die aan de eindgebruiker wordt toegestaan om zich te identificeren.
§ 4. Indien een operator [...]of een aanbieder bedoeld in artikel 126, § 1, eerste lid, niet voldoet aan de hem door dit artikel of door de Koning opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.	§ 4. Indien een operator [...]of een aanbieder bedoeld in artikel 126, § 1, eerste lid, niet voldoet aan de hem door dit artikel of door de Koning opgelegde technische en administratieve maatregelen, is het hem verboden de dienst, waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.
§ 5. De operatoren en de aanbieders bedoeld in artikel 126, § 1, eerste lid, sluiten de eindgebruikers die [...] niet voldoen aan de hen door dit artikel of door de Koning opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting.	§ 5. De operatoren en de aanbieders bedoeld in artikel 126, § 1, eerste lid, sluiten de eindgebruikers die [...] niet voldoen aan de hen door dit artikel of door de Koning opgelegde technische en administratieve maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die eindgebruikers worden op geen enkele wijze vergoed voor de afsluiting.
[...]	[...]
§ 6. [...] (intrekking vernietigd door het Grondwettelijk Hof)	§ 6. Elke operator zet een interne procedure op voor de afhandeling van verzoeken om toegang

	tot persoonsgegevens van gebruikers op grond van paragraaf 1. Hij verstrekt op verzoek aan het Instituut gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en zijn antwoord.
	Art. 127/1
	§ 1. Voor de toepassing van dit artikel omvat zware criminaliteit met name de feiten waarvoor er ernstige aanwijzingen bestaan:
	1° dat ze de minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88bis, eerste lid, van het Wetboek van Strafvordering tot gevolg kunnen hebben;
	2° dat ze kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht;
	3° dat ze een inbreuk zouden kunnen vormen op de artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening betreffende machtsmisbruik) of op de bepalingen die worden genomen op basis of ter uitvoering van deze artikelen.
	§ 2. Enkel de volgende autoriteiten mogen van een operator gegevens krijgen die worden bewaard krachtens de artikelen 122 en 123, voor de doeleinden hieronder voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm:
	1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;
	2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;
	3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

	4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;
	5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;
	6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;
	7° de administratieve autoriteiten belast met het behoud van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid;
	8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;
	9° het Instituut in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;
	10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden.
	§ 3. De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.
	Enkel de autoriteiten bedoeld in paragraaf 2, mogen van een operator gegevens ontvangen die worden bewaard krachtens de artikelen 126 en 127 voor de doeleinden waarin dezelfde

	paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.
	In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.
	In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen voor de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.
	§ 4. De gegevens die worden bewaard krachtens artikel 126/1 worden bewaard voor de autoriteiten en doeleinden bedoeld in paragraaf 2, 1°, 2°, 3° en 6°.
	Enkel de in paragraaf 2, 1°, 2°, 3°, 6° en 9°, bedoelde autoriteiten mogen van een operator voor de doeleinden beoogd in dezelfde paragraaf, de krachtens artikel 126/1 bewaarde gegevens krijgen, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.
	§ 5. De formele wettelijke norm van Belgisch recht bedoeld in de paragrafen 2 tot 4 preciseert:
	- **de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen;**
	- **de categorieën van gegevens die mogen gevraagd worden;**
	- **de beoogde doeleinden;**

	- **de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit.**
	De minister laat in het Belgisch Staatsblad een omzendbrief publiceren die een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127.
	Op het verzoek van de minister of van het Instituut verstrekken de Belgische autoriteiten bedoeld in de paragrafen 2 tot 4 de informatie die nodig is om deze omzendbrief op te stellen.
	§ 6. De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 of 127, omvatten de volgende minimale vermeldingen:
	1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;
	2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;
	3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;
	4° de gewenste antwoordtermijn.
	§ 7. Het Instituut stuurt jaarlijks aan de minister en de minister van Justitie statistieken over de verstrekking aan de autoriteiten van gegevens bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127. Deze ministers sturen die

	jaarlijks door naar de Kamer van volksvertegenwoordigers.
	Die statistieken omvatten met name:
	1° de gevallen waarin bewaarde gegevens zijn verstrekt aan de bevoegde autoriteiten overeenkomstig de toepasselijke wettelijke bepalingen;
	2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;
	3° de gevallen waarin verzoeken om bewaarde gegevens niet konden worden ingewilligd.
	Die statistieken mogen geen persoonsgegevens noch vertrouwelijke informatie omvatten.
	De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering moet uitbrengen aan het Parlement.
	Het Instituut vraagt aan de operatoren en aan de door de Koning aangewezen dienst de informatie aan de hand waarvan het de in het eerste lid bedoelde verplichting kan vervullen.
	Art. 127/2
	§ 1. De operatoren garanderen de kwaliteit van de bewaarde metagegevens van elektronische communicatie en, in het geval van de gegevens bewaard voor de autoriteiten, zorgen ze ervoor dat ze dezelfde kwaliteit hebben als de gegevens die worden verwerkt in het kader van de verstrekking van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst.
	De operatoren stellen alles in het werk om de technische verbanden te leggen tussen de gegevens bewaard voor de autoriteiten die nodig zijn om op hun vragen te antwoorden.

	§ 2. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie, bewaard voor de autoriteiten, dienen de operatoren:
	1° te garanderen dat de bewaarde gegevens onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk of verwerkt door de dienst;
	2° te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;
	3° mogen de bewaarde gegevens niet gebruiken voor andere doeleinden dan de verstrekking van deze gegevens aan de autoriteiten, tenzij wanneer ze de toestemming krijgen van de betrokken abonnees, conform artikel 4 van de AVG en onverminderd andere wettelijke bepalingen.
	§ 3. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie dienen de operatoren:
	1° de gegevens op het grondgebied van de Europese Unie te bewaren en in België de door een Belgische autoriteit gevraagde gegevens te verstrekken;
	2° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt van elke drager worden verwijderd of dat deze gegevens worden geanonimiseerd;
	3° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij onbedoeld hetzij onrechtmatig, tegen een onbedoeld verlies of onbedoelde wijziging of tegen niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, conform artikel 105/1;

	4° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 127/3, § 1, op manuele of op geautomatiseerde wijze;
	5° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord.
	§ 4. De in de paragraaf 3, eerste lid, 5°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek.
	De operator neemt de nodige maatregelen opdat elke raadpleging van de gegevens die hij bewaart voor de autoriteiten, automatisch in het logboek een registratie van de volgende gegevens genereert: de identiteit van de persoon die de gegevens heeft geraadpleegd, het moment van de raadpleging en de geraadpleegde gegevens.
	Dit logboek bevat eveneens de volgende informatie en documenten, die eventueel manueel daarin worden ingevoerd:
	1° de identiteit van de vragende autoriteit, het voorwerp, de datum en het tijdstip van het verzoek, een kopie van het verzoek of een link naar dit laatste;
	2° wat betreft het antwoord van de operator op het verzoek van de autoriteit: de identiteit van zijn geadresseerde, de datum en het tijdstip van de verzending ervan alsook het communicatiemiddel dat werd gebruikt voor de verzending.
	Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan.
	De gegevens van dit logboek worden bewaard gedurende een periode van tien jaar. Nadat deze bewaringstermijn is verstreken, worden de logboekgegevens vernietigd.

	De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen. Elke wijziging van de in het logboek opgenomen gegevens is verboden. Elke raadpleging van het logboek wordt geregistreerd.
	De Koning kan, na advies van de Gegevensbeschermingsautoriteit en van het Instituut, de eisen bepalen die de operatoren in acht moeten nemen wat betreft het logboek.
	In het kader van de controle van de operator mogen het Instituut en de Gegevensbeschermingsautoriteit dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.
	§ 5. Indien het Instituut over aanwijzingen beschikt die zouden kunnen duiden op een inbreuk van een operator op paragraaf 2, 3 of 4, dan kan het de operator verplichten om zich te onderwerpen aan een veiligheidscontrole door een gekwalificeerde onafhankelijke instantie die de operator ter goedkeuring voorlegt aan het Instituut.
	Die instantie neemt geen kennis van de verzoeken van de autoriteiten jegens de operatoren, inclusief het logboek bedoeld in paragraaf 4.
	Het rapport en de resultaten van deze veiligheidscontrole worden bezorgd aan het Instituut. De kosten van de controle worden door de operator gedragen.
	Art. 127/3
	§ 1. Bij elke operator wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.
	Enkel de leden van de Coördinatiecel mogen antwoorden op de verzoeken van de autoriteiten met betrekking tot de gegevens bedoeld in het eerste lid. Ze mogen echter, onder hun toezicht en binnen de grenzen van

	het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator.
	Deze autoriteiten richten hun verzoeken tot deze cel.
	In voorkomend geval kunnen verscheidene operatoren een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval neemt elke operator de nodige maatregelen opdat deze gemeenschappelijke Coördinatiecel in staat is om te antwoorden op de verzoeken die eraan worden gericht.
	De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens, en van het Instituut, de vereisten waaraan de Coördinatiecel moet beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid.
	§ 2. De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim. Deze leden delen aan de aangestelden enkel de gegevens mee die strikt noodzakelijk zijn om die bijstand te krijgen.
	Elke operator waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel.
	De leden van de Coördinatiecel beschikken over een positief en niet-achterhaald veiligheidsadvies bedoeld in artikel 22quinquies/1 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.
	Een veiligheidsadvies heeft een maximale geldigheidsduur van 5 jaar.
	De administratieve instantie die bevoegd is voor de behandeling van de adviezen is de minister van Justitie.
	De Koning bepaaltalternatieve veiligheidsmaatregelen die passend zijn voor de personen voor wie een veiligheidsadvies

	niet kan worden verstrekt wegens gebrek aan voldoende informatie.
	In afwijking van het derde lid kan een in het zesde lid bedoelde persoon deel uitmaken van de Coördinatiecel, wanneer deze alternatieve veiligheidsmaatregelen in acht worden genomen en zonder over een veiligheidsadvies te beschikken.
	De Koning bepaalt na advies van de autoriteiten bevoegd voor de bescherming van de gegevens, en van het Instituut het volgende:
	1° voor de andere operatoren dan diegene die reeds over een veiligheidsofficier beschikken wegens andere activiteiten dan de Coördinatiecel, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een dergelijke officier aan te stellen in functie van het aantal verzoeken ontvangen vanwege de gerechtelijke autoriteiten, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;
	2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inzonderheid wat het gebruik van de talen betreft;
	3° de regels voor de toegang van de gemachtigde Belgische autoriteiten tot de contactgegevens van de Coördinatiecel en zijn leden.
	§ 3. Elke operator stelt een interne procedure voor het beantwoorden van de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens van eindgebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en zijn antwoord.
	Elke operator wordt beschouwd als verwerkingsverantwoordelijke in de zin van de AVG, voor de gegevens verwerkt op basis van artikelen 122, 123, 126, 126/1 en 127.
	§ 4. De Koning bepaalt na advies van de autoriteiten bevoegd voor de bescherming van

	de gegevens, en van het Instituut de regels voorde samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen. Zo worden onder andere, in voorkomend geval en per betrokken overheid, de volgende zaken geregeld:
	a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;
	b) het dringendheidsniveau voor de behandeling van de verzoeken;
	c) de antwoordtermijn;
	d) de vereiste beschikbaarheid van de dienst;
	e) de modaliteiten voor het testen van de samenwerking;
	f) de tarieven voor de vergoeding van die samenwerking.
	Indien nodig en voor de toepassing van dit artikel, kan de Koning verschillende regels bepalen al naargelang de verschillende categorieën van operatoren, met name volgens het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en of zij al dan niet een elektronische-communicatienetwerk aanbieden in België.
TITEL V. - Procedurele bepalingen en strafbepalingen.	TITEL V. - Procedurele bepalingen en strafbepalingen.
HOOFDSTUK IV. - Strafbepalingen.	HOOFDSTUK IV. - Strafbepalingen.
Art. 145	**Art. 145**
§ 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 124, en de aanbieders bedoeld in artikel 126, § 1, eerste lid, 127, 133 en de ter uitvoering van de artikelen 32, 39, § 3, 47, 106/2, 126, 126/1 en 127 genomen besluiten overtreedt.	**§ 1. Met een geldboete van 50 tot 100 000 EUR wordt gestraft de persoon die de artikelen 15, 32, 33, 35, 41, 42, 45, 46, 106/2, 107/5, 124, 126 tot en met 127/3, 133 en de ter uitvoering van de artikelen 9, § 7, 32, 39, § 3, 47, 106/2, 126, 126/1, 127, 127/2 en 127/3 genomen besluiten overtreedt.**
§ 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt	§ 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt

gestraft de persoon die artikel 13/1, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt.	gestraft de persoon die artikel 13/1, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt.
§ 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft:	§ 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft:
1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische-communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;	1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische-communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;
2° (opgeheven)	2° (opgeheven)
3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan.	3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan.
§ 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan.	§ 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan.
§ 3ter. (vernietigd door het Grondwettelijk Hof)	**§ 3ter. Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft :**
	1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de door de operator voor de autoriteiten bewaarde gegevens op enige manier overneemt, bij zich houdt of er enig gebruik van maakt;

	2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.
§ 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.	§ 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.
HOOFDSTUK 3 - Wijzigingen aan de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren	
Art. 8	**Art. 8**
De sectorale overheid betekent aan de exploitant de met redenen omklede beslissing tot aanduiding van zijn infrastructuur als kritieke infrastructuur en bezorgt een kopie van deze beslissing met vermelding van de datum van betekening aan de ADCC.	De sectorale overheid betekent aan de exploitant de met redenen omklede beslissing tot aanduiding van zijn infrastructuur als kritieke infrastructuur en bezorgt een kopie van deze beslissing met vermelding van de datum van betekening aan de ADCC.
De ADCC deelt eveneens de informatiegegevens die nuttig zijn voor de uitvoering van de in artikel 10 bedoelde dreigingsanalyse, met inbegrip van de datum van de betekening, mee aan het OCAD.	De ADCC deelt eveneens de informatiegegevens die nuttig zijn voor de uitvoering van de in artikel 10 bedoelde dreigingsanalyse, met inbegrip van de datum van de betekening, mee aan het OCAD.
De ADCC brengt de burgemeester van de gemeente op het grondgebied waarvan de kritieke infrastructuur zich bevindt, op de hoogte van deze aanduiding.	De ADCC brengt de burgemeester van de gemeente op het grondgebied waarvan de kritieke infrastructuur zich bevindt, op de hoogte van deze aanduiding.
In de in artikel 13, § 7, bedoelde gevallen brengt de ADCC de gouverneur van de provincie op het grondgebied waarvan de kritieke infrastructuur zich bevindt op de hoogte van deze aanduiding of, wanneer de kritieke infrastructuur zich op het grondgebied van de Brusselse agglomeratie bevindt, de bevoegde overheid krachtens artikel 48 van de bijzondere wet van 12 januari 1989 met betrekking tot de Brusselse instellingen.	In de in artikel 13, § 7, bedoelde gevallen brengt de ADCC de gouverneur van de provincie op het grondgebied waarvan de kritieke infrastructuur zich bevindt op de hoogte van deze aanduiding of, wanneer de kritieke infrastructuur zich op het grondgebied van de Brusselse agglomeratie bevindt, de bevoegde overheid krachtens artikel 48 van de bijzondere wet van 12 januari 1989 met betrekking tot de Brusselse instellingen.
	De ADCC bezorgt na de aanduiding van een kritieke infrastructuur en minstens jaarlijks de gemeente waarin de kritieke infrastructuur zich bevindt of in voorkomend geval een lijst van gemeenten waarin de kritieke infrastructuren zich bevinden aan de door de Koning aangewezen dienst voor de toepassing van

	artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie.
HOOFDSTUK 4 – Wijzigingen aan de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector	
HOOFDSTUK I. - Algemeen.	HOOFDSTUK I. - Algemeen.
Art. 2	**Art. 2**
In deze wet wordt verstaan onder :	In deze wet wordt verstaan onder :
1° wet van 21 maart 1991 : wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;	1° wet van 21 maart 1991 : wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
2° (opgeheven)	2° (opgeheven)
3° Instituut : het Belgisch Instituut voor postdiensten en telecommunicatie, afgekort BIPT;	3° Instituut : het Belgisch Instituut voor postdiensten en telecommunicatie, afgekort BIPT;
4° Minister : de minister of staatssecretaris die bevoegd is voor de aangelegenheden die de postdiensten of telecommunicatie betreffen.	4° Minister : de minister of staatssecretaris die bevoegd is voor de aangelegenheden die de postdiensten of telecommunicatie betreffen.
De termen gebruikt in deze wet hebben dezelfde betekenis als deze verleend in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, in de wet van 13 juni 2005 betreffende de elektronische communicatie, in de wet van 26 januari 2018 betreffende de postdiensten, alsook in de bijbehorende uitvoeringsbesluiten.	De termen gebruikt in deze wet hebben dezelfde betekenis als deze verleend in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, in de wet van 13 juni 2005 betreffende de elektronische communicatie, in de wet van 26 januari 2018 betreffende de postdiensten, alsook in de bijbehorende uitvoeringsbesluiten.
	5° "Gegevens betreffende de eindgebruiker of de abonnee":
	- de intekeningsgegevens van de abonnee op de dienst;
	- de intekeningsgegevens van de abonnee op de dienst;
	- de gegevens ter vaststelling van de burgerlijke identiteit van de abonnee of van de eindgebruiker, met inbegrip van de betalingsgegevens;
	- de technische identificatiegegevens van de eindgebruiker, van de

	eindapparatuur of van de elektronische-communicatiedienst, zonder dat deze gegevens informatie kunnen verstrekken over de bestemmeling van de communicatie, met inbegrip van de IP-adressen van de bestemmeling van de communicatie of over de precieze locatie van de eindapparatuur;
HOOFDSTUK III. - Het Instituut.	HOOFDSTUK III. - Het Instituut.
Afdeling 2. - Bevoegdheden en opdrachten	Afdeling 2. - Bevoegdheden en opdrachten
Art. 14	**Art. 14**
§ 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur , met betrekking tot de sector digitale infrastructuren in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:	§ 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur , met betrekking tot de sector digitale infrastructuren in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:
1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers;	1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers;
2° het nemen van administratieve beslissingen;	2° het nemen van administratieve beslissingen;
3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:	3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:
a) de wet van 13 juni 2005 betreffende de elektronische communicatie;	a) de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;	b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
c) de wet van 26 januari 2018 betreffende de postdiensten;	c) de wet van 26 januari 2018 betreffende de postdiensten;
d) de artikelen 14, § 2, 2°, en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	**d) de artikelen 14, § 2, 2° en 2°/1, 21, §§ 5 tot en met 7, 25, §§ 8 tot en met 10 en 28/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;**
e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;	f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;
g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;	g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;
h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sector digitale infrastructuren;	h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sector digitale infrastructuren;
i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.	i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.
j) elke bindende rechtshandeling in het Europese Unierecht, die opdrachten toewijst aan de nationale regelgevende instantie in de sector van de post of elektronische communicatie.	j) elke bindende rechtshandeling in het Europese Unierecht, die opdrachten toewijst aan de nationale regelgevende instantie in de sector van de post of elektronische communicatie.

Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.	Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.
4° in geval van een geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, (of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten) het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut;	4° in geval van een geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, (of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten) het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut;
4° /1 in geval van geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	4° /1 in geval van geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie.	5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie.
6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van	6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van

openbare dienst toegekend in het kader van artikel 141, § 1bis, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract.	openbare dienst toegekend in het kader van artikel 141, § 1bis, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract.
§ 2. In het kader van zijn bevoegdheden :	§ 2. In het kader van zijn bevoegdheden :
1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren ; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;	1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren ; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;
2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;	2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;
	2°/1 kan het Instituut van een operator gegevens betreffende de eindgebruiker of de abonnee, of andere metagegevens van elektronische communicatie opvragen, die noodzakelijk zijn voor de vervulling van een van zijn opdrachten inzake toepassing en controle van de in artikel 14, paragraaf 1, 3°, a) en g) tot i), vastgestelde bepalingen, onder de voorwaarden van de artikelen 25, §§ 8 tot 9, en 28/1, §§ 1 en 2;

	2°/2 kan het Instituut van een operator eisen dat deze het Instituut een databank laat raadplegen die gegevens bevat die moeten worden bewaard door of krachtens de artikelen 122, 123, 126, 126/1 en 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie, om te controleren of een operator deze artikelen of de uitvoeringsbesluiten ervan naleeft, onder de voorwaarden van de artikelen 25, § 10 en 28/1, § 3;
3° werkt het Instituut samen met en verstrekt het informatie aan :	3° werkt het Instituut samen met en verstrekt het informatie aan :
a) de Europese Commissie, ENISA, het Bureau en aan Berec;	a) de Europese Commissie, ENISA, het Bureau en aan Berec;
b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;	b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;
c) de regulerende instanties in de overige economische sectoren;	c) de regulerende instanties in de overige economische sectoren;
d) de federale overheidsdiensten die belast zijn met consumentenbescherming;	d) de federale overheidsdiensten die belast zijn met consumentenbescherming;
e) de Belgische instanties die belast zijn met mededinging.	e) de Belgische instanties die belast zijn met mededinging.
De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;	De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;
f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;	f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;
g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land;	g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land;

h) de Gegevensbeschermingsautoriteit;	h) de Gegevensbeschermingsautoriteit;
i) de federale overheidsdienst die belast is met statistiek en economische informatie;	i) de federale overheidsdienst die belast is met statistiek en economische informatie;
4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor telecommunicatie, opgericht bij het koninklijk besluit van 10 december 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993;	4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor telecommunicatie, opgericht bij het koninklijk besluit van 10 december 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993;
5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden.	5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden.
6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in artikel 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 35 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald :	6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in artikel 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 35 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald :
- waken over de kwaliteit en het voortbestaan van de universele dienst;	- waken over de kwaliteit en het voortbestaan van de universele dienst;
- waken over de belangen van de gebruikers van postdiensten;	- waken over de belangen van de gebruikers van postdiensten;
- bijdragen tot de ontwikkeling van een interne markt voor postdiensten;	- bijdragen tot de ontwikkeling van een interne markt voor postdiensten;

- het bevorderen van de concurrentie in de postsector.	- het bevorderen van de concurrentie in de postsector.
7° kan, in de hoedanigheid van inspectiedienst, de mededeling van het beveiligingsplan van de exploitant eisen op elk moment, in afwijking van artikel 25, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren	7° kan, in de hoedanigheid van inspectiedienst, de mededeling van het beveiligingsplan van de exploitant eisen op elk moment, in afwijking van artikel 25, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren
§ 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten.	§ 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten.
Afdeling 4. - De leden van het personeel van het Instituut.	Afdeling 4. - De leden van het personeel van het Instituut.
Onderafdeling 1. - Officieren van gerechtelijke politie.	Onderafdeling 1. - Officieren van gerechtelijke politie.
Art. 25	**Art. 25**
§ 1. In het kader van de controle op het gebruik van het spectrum, de bestrijding van storingen, alsook de controle op de naleving van de wetgeving inzake elektromagnetische compatibiliteit en de conformiteit van apparatuur, kunnen de personeelsleden vermeld in artikel 24 in hun hoedanigheid van officier van gerechtelijke politie :	§ 1. In het kader van de controle op het gebruik van het spectrum, de bestrijding van storingen, alsook de controle op de naleving van de wetgeving inzake elektromagnetische compatibiliteit en de conformiteit van apparatuur, kunnen de personeelsleden vermeld in artikel 24 in hun hoedanigheid van officier van gerechtelijke politie :
1° op elk ogenblik, wanneer zulks voor de uitoefening van hun opdracht noodzakelijk is, ieder vervoermiddel, gebouw en aanhorigheid betreden, behalve als het gaat om een woning in de zin van artikel 15 van de Grondwet;	1° op elk ogenblik, wanneer zulks voor de uitoefening van hun opdracht noodzakelijk is, ieder vervoermiddel, gebouw en aanhorigheid betreden, behalve als het gaat om een woning in de zin van artikel 15 van de Grondwet;
1°/1 met machtiging van de onderzoeksrechter een woning betreden in de zin van artikel 15 van de Grondwet, met inachtneming van de wet van 7 juni 1969 tot vaststelling van de tijd gedurende welke geen opsporing ten huize of huiszoeking mag worden verricht;	1°/1 met machtiging van de onderzoeksrechter een woning betreden in de zin van artikel 15 van de Grondwet, met inachtneming van de wet van 7 juni 1969 tot vaststelling van de tijd gedurende welke geen opsporing ten huize of huiszoeking mag worden verricht;

2° alle dienstige vaststellingen doen, zich documenten, stukken, boeken en voorwerpen die bij de opsporing en vaststelling nodig zijn, laten overleggen en die in beslag nemen;	2° alle dienstige vaststellingen doen, zich documenten, stukken, boeken en voorwerpen die bij de opsporing en vaststelling nodig zijn, laten overleggen en die in beslag nemen;
3° alle documenten, stukken, boeken en voorwerpen in beslag nemen, voorzover dit nodig is om aan de inbreuk een einde te maken;	3° alle documenten, stukken, boeken en voorwerpen in beslag nemen, voorzover dit nodig is om aan de inbreuk een einde te maken;
4° alle inlichtingen verzamelen en alle geschreven of mondelinge verklaringen of getuigenissen afnemen;	4° alle inlichtingen verzamelen en alle geschreven of mondelinge verklaringen of getuigenissen afnemen;
5° bijstand te verlenen in het kader van de uitvoering van de besluiten van het Instituut.	5° bijstand te verlenen in het kader van de uitvoering van de besluiten van het Instituut.
Wanneer die daden de kenmerken van een huiszoeking dragen, mogen ze alleen met inachtneming van de artikelen 87 tot 90 van het Wetboek van strafvordering worden gesteld.	Wanneer die daden de kenmerken van een huiszoeking dragen, mogen ze alleen met inachtneming van de artikelen 87 tot 90 van het Wetboek van strafvordering worden gesteld.
§ 2. In het kader van de controle op de naleving van de wetgeving inzake elektromagnetische compatibiliteit en de conformiteit van apparatuur kunnen de personeelsleden van het Instituut vermeld in artikel 24, overgaan tot het nemen van monsters en die laten onderzoeken. De Koning, op advies van het Instituut, bepaalt de nadere regels.	§ 2. In het kader van de controle op de naleving van de wetgeving inzake elektromagnetische compatibiliteit en de conformiteit van apparatuur kunnen de personeelsleden van het Instituut vermeld in artikel 24, overgaan tot het nemen van monsters en die laten onderzoeken. De Koning, op advies van het Instituut, bepaalt de nadere regels.
§ 3. Behoudens de gevallen vermeld in § 1 kunnen de personeelsleden vermeld in artikel 24 in hun hoedanigheid van officier van gerechtelijke politie alle vaststellingen doen, informatie inzamelen verklaringen opnemen, zich documenten, stukken, boeken, en voorwerpen doen vertonen en die in beslag nemen welke nodig zijn bij de opsporing of vaststelling of nodig zijn om aan de inbreuk een einde te maken. Zij kunnen huiszoekingen of alle andere dienstige daden verrichten tot vaststelling van een inbreuk op de wetgeving waarop zij controle uitoefenen.	§ 3. Behoudens de gevallen vermeld in § 1 kunnen de personeelsleden vermeld in artikel 24 in hun hoedanigheid van officier van gerechtelijke politie alle vaststellingen doen, informatie inzamelen verklaringen opnemen, zich documenten, stukken, boeken, en voorwerpen doen vertonen en die in beslag nemen welke nodig zijn bij de opsporing of vaststelling of nodig zijn om aan de inbreuk een einde te maken. Zij kunnen huiszoekingen of alle andere dienstige daden verrichten tot vaststelling van een inbreuk op de wetgeving waarop zij controle uitoefenen.
Elke huiszoeking gebeurt met inachtneming van de bepalingen van het Wetboek van strafvordering.	Elke huiszoeking gebeurt met inachtneming van de bepalingen van het Wetboek van strafvordering.
De instemming van de onderzoeksrechter is vereist voor een huiszoeking in :	De instemming van de onderzoeksrechter is vereist voor een huiszoeking in :

1° de woning van de ondernemingshoofden, bestuurders, zaakvoerders, directeurs en andere personeelsleden van de betrokken onderneming alsook in de woning en de lokalen die gebruikt worden voor professionele doeleinden van natuurlijke en rechtspersonen, intern of extern, belast met het commercieel, rekenplichtig, administratief, fiscaal en financieel beheer van die onderneming;	1° de woning van de ondernemingshoofden, bestuurders, zaakvoerders, directeurs en andere personeelsleden van de betrokken onderneming alsook in de woning en de lokalen die gebruikt worden voor professionele doeleinden van natuurlijke en rechtspersonen, intern of extern, belast met het commercieel, rekenplichtig, administratief, fiscaal en financieel beheer van die onderneming;
2° de maatschappelijke of de exploitatiezetel van de betrokken onderneming.	2° de maatschappelijke of de exploitatiezetel van de betrokken onderneming.
§ 4. De processen-verbaal van de officieren van gerechtelijke politie zijn rechtsgeldig tot bewijs van het tegendeel.	§ 4. De processen-verbaal van de officieren van gerechtelijke politie zijn rechtsgeldig tot bewijs van het tegendeel.
§ 5. In de uitoefening van hun opsporingsopdrachten of bij de vaststelling van inbreuken, staan de officieren van gerechtelijke politie onder het toezicht van de procureur-generaal.	§ 5. In de uitoefening van hun opsporingsopdrachten of bij de vaststelling van inbreuken, staan de officieren van gerechtelijke politie onder het toezicht van de procureur-generaal.
§ 6. De officieren van gerechtelijke politie kunnen voor de uitvoering van hun opdrachten een beroep doen op de openbare macht en beschikken over alle middelen die aan de agenten van de openbare macht worden toegekend.	§ 6. De officieren van gerechtelijke politie kunnen voor de uitvoering van hun opdrachten een beroep doen op de openbare macht en beschikken over alle middelen die aan de agenten van de openbare macht worden toegekend.
§ 7. Onverminderd de bijzondere wetten die de geheimhouding van de verklaringen garanderen, zijn de openbare besturen gehouden hun bijstand te verlenen aan de officieren van gerechtelijke politie in de uitoefening van hun opdrachten.	§ 7. Onverminderd de bijzondere wetten die de geheimhouding van de verklaringen garanderen, zijn de openbare besturen gehouden hun bijstand te verlenen aan de officieren van gerechtelijke politie in de uitoefening van hun opdrachten.
	§ 8. Ten behoeve van de vervulling van hun opdrachten kunnen de officieren van gerechtelijke politie van het Instituut van een operator eisen dat hij hen door de operator bewaarde gegevens betreffende de eindgebruiker of de abonnee verstrekt, die nodig zijn om een inbreuk op een in artikel 24 bedoelde wet te kunnen opsporen, vaststellen of vervolgen, wanneer die is gepleegd door middel van apparatuur, netwerken of diensten voor elektronische communicatie of radiocommunicatie in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie.

	De officier van gerechtelijke politie legt zijn met redenen omkleed verzoek vooraf voor goedkeuring voor aan zijn hiërarchische meerdere.
	§ 9. Ten behoeve van de vervulling van hun opdrachten kunnen de officieren van gerechtelijke politie van het Instituut van een operator eisen dat hij hen andere metagegevens van elektronische communicatie verstrekt dan de gegevens betreffende de eindgebruiker of de abonnee, die nodig zijn om een inbreuk op een in artikel 24 bedoelde wet te kunnen opsporen, vaststellen of vervolgen, wanneer die is gepleegd door middel van apparatuur, netwerken of diensten voor elektronische communicatie of radiocommunicatie in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie.
	De officier van gerechtelijke politie legt zijn met redenen omkleed verzoek ter voorafgaande goedkeuring voor aan de onderzoeksrechter, tenzij in een naar behoren gerechtvaardigd noodgeval.
	In een naar behoren gerechtvaardigd noodgeval zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het Instituut het naar de operator verzonden verzoek na deze verzending onverwijld mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.
	§ 10. In afwijking van de paragrafen 8 en 9, staat een operator op verzoek van een officier van gerechtelijke politie van het Instituut en na toestemming van de Raad van het Instituut, het aan deze officier toe om zijn databanken te raadplegen die uitvoering verlenen aan de artikelen 126, 126/1 en 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie uitvoeren, om de naleving van die artikelen en van de uitvoeringsbesluiten ervan te controleren.
	Deze officiers mogen enkel een kopie nemen van de gegevens en documenten die worden

	geraadpleegd in het kader van het eerste lid om inbreuken gepleegd door de operator vast te stellen.
	§ 11. De officiers van gerechtelijke politie van het Instituut nemen de verzoeken bedoeld in de paragrafen 8, 9 en 10 op in een inventaris.
	Art. 28/1
	§ 1. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mogen de personeelsleden van het Instituut die niet in een strafrechtelijk kader optreden, van een operator eisen dat hij hen door de operator bewaarde gegevens betreffende de eindgebruiker of de abonnee verstrekt.
	Het personeelslid legt zijn met redenen omkleed verzoek ter voorafgaandegoedkeuring voor aan zijn hiërarchische meerdere.
	§ 2. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mogen de personeelsleden van het Instituut die niet in een strafrechtelijk kader optreden, van een operator eisen dat hij hen andere door de operator bewaarde metagegevens van elektronische communicatie verstrekt dan de gegevens betreffende de eindgebruiker of de abonnee.
	Hij legt zijn met redenen omkleed verzoek vooraf voor goedkeuring voor aan de Gegevensbeschermingsautoriteit, behalve in een naar behoren gerechtvaardigd noodgeval. In een naar behoren gerechtvaardigd noodgeval deelt hij het naar de operator verzonden verzoek na deze verzending onverwijld mee aan de Gegevensbeschermingsautoriteit. De Gegevensbeschermingsautoriteit voert daarna een controle uit.
	§ 3. Het tweede lid van paragraaf 2 is niet van toepassing wanneer het Instituut de naleving

	door de operator van de artikelen 122 en 123 van de wet van 13 juni 2005 betreffende de elektronische communicatie controleert, in voorkomend geval door de databanken die uitvoering verlenen aan deze artikelen te raadplegen.
	§ 4. De verzoeken die worden geformuleerd overeenkomstig de paragrafen 1, 2 en 3 worden opgenomen in een inventaris die bij het Instituut wordt bijgehouden.
HOOFDSTUK 5 – Wijzigingen aan het wetboek van strafvordering	
Art. 88bis	**Art. 88bis**
§ 1. Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij:	§ 1. Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij:
1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;	1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;
2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren.	2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren.
Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:	Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:
- de operator van een elektronisch communicatienetwerk; en	- de operator van een elektronisch communicatienetwerk; en
- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder	- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder

wordt ook de verstrekker van een elektronische communicatiedienst begrepen.	wordt ook de verstrekker van een elektronische communicatiedienst begrepen.
In de gevallen bedoeld in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de elektronische communicatie vastgesteld en opgenomen in een proces-verbaal.	In de gevallen bedoeld in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de elektronische communicatie vastgesteld en opgenomen in een proces-verbaal.
De onderzoeksrechter doet in een met redenen omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.	De onderzoeksrechter doet in een met redenen omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.
Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 2.	Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 2.
In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90ter, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter.	In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90ter, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter.
Indien het echter het in artikel 137, 347bis, 434 of 470 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.	Indien het echter het in artikel 137, 347bis, 434 of 470 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.
Indien het het in artikel 137 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings bovendien de maatregel bevelen binnen de tweeënzeventig	Indien het het in artikel 137 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings bovendien de maatregel bevelen binnen de tweeënzeventig

uur na de ontdekking van dit strafbare feit, zonder dat een bevestiging door de onderzoeksrechter nodig is.	uur na de ontdekking van dit strafbare feit, zonder dat een bevestiging door de onderzoeksrechter nodig is.
De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie.	De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3bis van de wet van 13 juni 2005 betreffende de elektronische communicatie.
In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vierde en vijfde lid.	In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vierde en vijfde lid.
§ 2.(vernietigd door GH)	**§ 2. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:**
	- voor een strafbaar feit bedoeld in boek II, titel Iter, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift;
	- voor een ander strafbaar feit bedoeld in artikel 90ter, §§ 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324bis van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;
	- voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.

§ 3. (gedeeltelijk vernietigd door GH)	§ 3. **De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.**
Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	**De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Dezelfde personen zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.**
§ 4. De actoren bedoeld in § 1, tweede lid, delen de gegevens waarom verzocht werd mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de nadere regels vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.	§ 4. De actoren bedoeld in § 1, tweede lid, delen de gegevens waarom verzocht werd mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de nadere regels vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.
Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.
Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in dit artikel weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, medewerking waarvan de nadere regels vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.	Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in dit artikel weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, medewerking waarvan de nadere regels vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.

HOOFDSTUK 6 - Wijzigingen aan de wet van 5 augustus 1992 op het politieambt	
Art. 42	**Art. 42**
Wanneer hij in gevaar gebracht wordt bij het vervullen van zijn opdracht of wanneer personen in gevaar zijn, kan ieder lid van het operationeel kader de hulp of bijstand vorderen van de ter plaatse aanwezige personen en in geval van absolute noodzaak kan hij eveneens de hulp of bijstand vorderen van enig ander nuttig persoon.	***§ 1er.*** Wanneer hij in gevaar gebracht wordt bij het vervullen van zijn opdracht of wanneer personen in gevaar zijn, kan ieder lid van het operationeel kader de hulp of bijstand vorderen van de ter plaatse aanwezige personen en in geval van absolute noodzaak kan hij eveneens de hulp of bijstand vorderen van enig ander nuttig persoon.
De gevorderde hulp of bijstand mag de persoon die ze verleent niet in gevaar brengen.	De gevorderde hulp of bijstand mag de persoon die ze verleent niet in gevaar brengen.
	§ 2. Een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kan, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood en de opsporing van personen van wie de verdwijning onrustwekkend is, en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon opvorderen.
	Enkel de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen en met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, betreffende de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan de opvordering, worden meegedeeld.
	De vordering wordt via de officier van gerechtelijke politie bedoeld in paragraaf 2, eerste lid 1, gericht aan:
	- **-de operator van een elektronisch communicatienetwerk; of**
	- **iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt,**

	die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.
	§ 3. De Cel Vermiste Personen stelt het Controleorgaan uiterlijk binnen 48 uur na de vordering in kennis van de vordering en de motivering ervan.
	Indien het Controleorgaan van oordeel is dat niet aan de voorwaarden voor de uitvoering van deze vordering is voldaan, beveelt zij, met opgave van redenen, dat de aldus verkregen gegevens niet mogen worden gebruikt en vernietigd moeten worden
	Deze met redenen omklede beslissing wordt door het Controleorgaan zo spoedig mogelijk meegedeeld aan de Cel Vermiste Personen.
HOOFDSTUK 7 - Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten	
Artikel 3	**Artikel 3**
In deze wet wordt verstaan onder:	In deze wet wordt verstaan onder:
1° "Nationale Veiligheidsraad": de binnen de Regering opgerichte Raad die belast is met de door de Koning vastgestelde taken van nationale veiligheid;	1° "Nationale Veiligheidsraad": de binnen de Regering opgerichte Raad die belast is met de door de Koning vastgestelde taken van nationale veiligheid;
2° "agent": ieder lid van het statutair of contractueel personeel en iedere militair die zijn functie uitoefent binnen één van de in artikel 2 genoemde inlichtingen- en veiligheidsdiensten;	2° "agent": ieder lid van het statutair of contractueel personeel en iedere militair die zijn functie uitoefent binnen één van de in artikel 2 genoemde inlichtingen- en veiligheidsdiensten;
3° "lid van het interventieteam":	3° "lid van het interventieteam":
a) voor de Veiligheid van de Staat, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Veiligheid van de Staat;	a) voor de Veiligheid van de Staat, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Veiligheid van de Staat;

b) voor de Algemene Dienst Inlichting en Veiligheid, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Algemene Dienst Inlichting en Veiligheid;	b) voor de Algemene Dienst Inlichting en Veiligheid, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Algemene Dienst Inlichting en Veiligheid;
4° "Algemene Dienst Inlichting en Veiligheid": de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht;	4° "Algemene Dienst Inlichting en Veiligheid": de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht;
5° "de Minister": de Minister van Justitie voor wat de Veiligheid van de Staat betreft, en de Minister van Landsverdediging voor wat de algemene Dienst Inlichting en Veiligheid van de Krijgsmacht betreft;	5° "de Minister": de Minister van Justitie voor wat de Veiligheid van de Staat betreft, en de Minister van Landsverdediging voor wat de algemene Dienst Inlichting en Veiligheid van de Krijgsmacht betreft;
6° "de commissie": de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, die wordt opgericht bij artikel 43/1;	6° "de commissie": de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, die wordt opgericht bij artikel 43/1;
7° "het Vast Comité I": het Vast Comité van Toezicht op de inlichtingendiensten, zoals bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;	7° "het Vast Comité I": het Vast Comité van Toezicht op de inlichtingendiensten, zoals bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;
8° "het diensthoofd": enerzijds, de administrateur-generaal van de Veiligheid van de Staat of, bij verhindering, de dienstdoende administrateur-generaal, en anderzijds, het hoofd van de algemene Dienst inlichting en veiligheid van de Krijgsmacht of, bij verhindering, het dienstdoende hoofd;	8° "het diensthoofd": enerzijds, de administrateur-generaal van de Veiligheid van de Staat of, bij verhindering, de dienstdoende administrateur-generaal, en anderzijds, het hoofd van de algemene Dienst inlichting en veiligheid van de Krijgsmacht of, bij verhindering, het dienstdoende hoofd;
9° "de inlichtingenofficier":	9° "de inlichtingenofficier":
a) voor de Veiligheid van de Staat, de agent die ten minste de graad van commissaris heeft;	a) voor de Veiligheid van de Staat, de agent die ten minste de graad van commissaris heeft;
b) voor de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht, de aan deze dienst toegewezen officier, alsook de burgerambtenaar die ten minste de graad van commissaris heeft;	b) voor de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht, de aan deze dienst toegewezen officier, alsook de burgerambtenaar die ten minste de graad van commissaris heeft;

10° "communicatie": elke overbrenging, uitzending, of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-elektriciteit, optische seingeving of een ander elektromagnetisch systeem; de communicatie per telefoon, gsm, mobilofoon, telex, telefax of elektronische gegevensoverdracht via computer of computernetwerk, evenals iedere andere privécommunicatie;	10° "communicatie": elke overbrenging, uitzending, of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-elektriciteit, optische seingeving of een ander elektromagnetisch systeem; de communicatie per telefoon, gsm, mobilofoon, telex, telefax of elektronische gegevensoverdracht via computer of computernetwerk, evenals iedere andere privécommunicatie**, ongeacht de aard van de afzender of de ontvanger**;
11° "elektronische communicatienetwerken": de elektronische communicatienetwerken als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;	11° "elektronische communicatienetwerken": de elektronische communicatienetwerken als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
11° /1 "verstrekker van een elektronische communicatiedienst": iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden;	11° /1 "verstrekker van een elektronische communicatiedienst": iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden;
12° "voor het publiek toegankelijke plaats": elke plaats, openbaar of privé, waartoe het publiek toegang kan hebben;	12° "voor het publiek toegankelijke plaats": elke plaats, openbaar of privé, waartoe het publiek toegang kan hebben;
12° /1 "niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is": elke plaats waartoe het publiek geen toegang heeft en die voor iedereen zichtbaar is vanaf de openbare weg zonder hulpmiddel of kunstgreep, met uitzondering van de binnenkant van gebouwen die niet voor het publiek toegankelijk zijn;	12° /1 "niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is": elke plaats waartoe het publiek geen toegang heeft en die voor iedereen zichtbaar is vanaf de openbare weg zonder hulpmiddel of kunstgreep, met uitzondering van de binnenkant van gebouwen die niet voor het publiek toegankelijk zijn;
13° "post": de postzending zoals gedefinieerd in artikel 131, 6°, 7° en 11°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;	13° "post": de postzending zoals gedefinieerd in artikel 131, 6°, 7° en 11°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
14° "technisch middel": een configuratie van componenten die signalen detecteert, deze overbrengt, hun registratie activeert en de signalen registreert, met uitzondering van:	14° "technisch middel": een configuratie van componenten die signalen detecteert, deze overbrengt, hun registratie activeert en de signalen registreert, met uitzondering van:

a) een apparaat dat gebruikt wordt voor het nemen van foto's;	a) een apparaat dat gebruikt wordt voor het nemen van foto's;
b) een mobiel apparaat dat gebruikt wordt voor de opname van bewegende beelden indien het nemen van foto's de discretie en de veiligheid van de agenten niet kan verzekeren en op voorwaarde dat dit gebruik voorafgaand is toegestaan door het diensthoofd of zijn gedelegeerde. Enkel relevant geachte vaste beelden worden bewaard. De overige beelden worden vernietigd binnen een maand na de dag van de opname;	b) een mobiel apparaat dat gebruikt wordt voor de opname van bewegende beelden indien het nemen van foto's de discretie en de veiligheid van de agenten niet kan verzekeren en op voorwaarde dat dit gebruik voorafgaand is toegestaan door het diensthoofd of zijn gedelegeerde. Enkel relevant geachte vaste beelden worden bewaard. De overige beelden worden vernietigd binnen een maand na de dag van de opname;
15° "radicaliseringsproces": een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen;	15° "radicaliseringsproces": een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen;
16° "journalist" : een journalist die gerechtigd is de titel van beroepsjournalist te dragen overeenkomstig de wet van 30 december 1963 betreffende de erkenning en de bescherming van de titel van beroepsjournalist;	16° "journalist" : een journalist die gerechtigd is de titel van beroepsjournalist te dragen overeenkomstig de wet van 30 december 1963 betreffende de erkenning en de bescherming van de titel van beroepsjournalist;
17° "bronnengeheim": het geheim zoals omschreven in de wet van 7 april 2005 tot bescherming van de journalistieke bronnen;	17° "bronnengeheim": het geheim zoals omschreven in de wet van 7 april 2005 tot bescherming van de journalistieke bronnen;
18° "Directeur Operaties van de Veiligheid van de Staat": de agent van de buitendiensten van de Veiligheid van de Staat, bekleed met de graad van commissaris-generaal, die belast is met de leiding van de buitendiensten van de Veiligheid van de Staat;	18° "Directeur Operaties van de Veiligheid van de Staat": de agent van de buitendiensten van de Veiligheid van de Staat, bekleed met de graad van commissaris-generaal, die belast is met de leiding van de buitendiensten van de Veiligheid van de Staat;
19° "vergrendeld voorwerp": een voorwerp dat geopend moet worden met behulp van een valse sleutel of via braak;	19° "vergrendeld voorwerp": een voorwerp dat geopend moet worden met behulp van een valse sleutel of via braak;
20° "observatie": het waarnemen van één of meerdere personen, hun aanwezigheid of gedrag, of van zaken, plaatsen of gebeurtenissen;	20° "observatie": het waarnemen van één of meerdere personen, hun aanwezigheid of gedrag, of van zaken, plaatsen of gebeurtenissen;
21° "doorzoeking": het betreden, bezichtigen en onderzoeken van een plaats alsook het bezichtigen en onderzoeken van een voorwerp.	21° "doorzoeking": het betreden, bezichtigen en onderzoeken van een plaats alsook het bezichtigen en onderzoeken van een voorwerp.

Artikel 7	**Artikel 7**
De Veiligheid van de Staat heeft als opdracht:	De Veiligheid van de Staat**, belast met de nationale veiligheid,** heeft als opdracht :
1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;	1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;
2° het uitvoeren van de veiligheidsonderzoeken die haar overeenkomstig de richtlijnen van de Nationale Veiligheidsraad worden toevertrouwd;	2° het uitvoeren van de veiligheidsonderzoeken die haar overeenkomstig de richtlijnen van de Nationale Veiligheidsraad worden toevertrouwd;
3° […]	3° […]
3° /1 het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied;	3° /1 het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied;
4° het uitvoeren van alle andere opdrachten die haar door of krachtens de wet worden toevertrouwd.	4° het uitvoeren van alle andere opdrachten die haar door of krachtens de wet worden toevertrouwd.
Artikel 11	**Artikel 11**
§1. De Algemene Dienst Inlichting en Veiligheid heeft als opdracht:	§1. De Algemene Dienst Inlichting en Veiligheid**, belast met de nationale veiligheid,** heeft als opdracht:
1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:	1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:

a) de onschendbaarheid van het nationaal grondgebied of de bevolking,	a) de onschendbaarheid van het nationaal grondgebied of de bevolking,
b) de militaire defensieplannen,	b) de militaire defensieplannen,
c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,	c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,
d) de vervulling van de opdrachten van de strijdkrachten,	d) de vervulling van de opdrachten van de strijdkrachten,
e) de veiligheid van de Belgische onderdanen in het buitenland,	e) de veiligheid van de Belgische onderdanen in het buitenland,
f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;	f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;
en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;	en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;
2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten;	2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten;

3° het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de Minister van Landsverdediging beheert;	3° het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de Minister van Landsverdediging beheert;
4° het uitvoeren van de veiligheidsonderzoeken die hem overeenkomstig de richtlijnen van de Nationale Veiligheidsraad worden toevertrouwd.	4° het uitvoeren van de veiligheidsonderzoeken die hem overeenkomstig de richtlijnen van de Nationale Veiligheidsraad worden toevertrouwd.
5° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied.	5° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied
§2. Voor de toepassing van § 1 wordt verstaan onder:	§2. Voor de toepassing van § 1 wordt verstaan onder:
1° "activiteit die de onschendbaarheid van het nationaal grondgebied of de bevolking bedreigt of zou kunnen bedreigen": elke uiting van het voornemen om, met middelen van militaire aard, het gehele grondgebied of een gedeelte ervan, alsook het luchtruim boven dat grondgebied of de territoriale wateren, in te nemen, te bezetten of aan te vallen, of de bescherming of het voortbestaan van de gehele bevolking of een gedeelte ervan, het nationaal patrimonium of het economisch potentieel van het land in gevaar te brengen;	1° "activiteit die de onschendbaarheid van het nationaal grondgebied of de bevolking bedreigt of zou kunnen bedreigen": elke uiting van het voornemen om, met middelen van militaire aard, het gehele grondgebied of een gedeelte ervan, alsook het luchtruim boven dat grondgebied of de territoriale wateren, in te nemen, te bezetten of aan te vallen, of de bescherming of het voortbestaan van de gehele bevolking of een gedeelte ervan, het nationaal patrimonium of het economisch potentieel van het land in gevaar te brengen;
2° "activiteit die de militaire defensieplannen bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om op ongeoorloofde wijze kennis te nemen van de plannen betreffende de militaire verdediging van het nationaal grondgebied, van het luchtruim boven dat grondgebied of van de territoriale wateren en van de vitale belangen van de Staat, of betreffende de gemeenschappelijke militaire verdediging in het kader van een	2° "activiteit die de militaire defensieplannen bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om op ongeoorloofde wijze kennis te nemen van de plannen betreffende de militaire verdediging van het nationaal grondgebied, van het luchtruim boven dat grondgebied of van de territoriale wateren en van de vitale belangen van de Staat, of betreffende de gemeenschappelijke militaire verdediging in het kader van een

bondgenootschap of een internationaal of supranationaal samenwerkingsverband;	bondgenootschap of een internationaal of supranationaal samenwerkingsverband;
2°/1 "activiteit die het wetenschappelijk en economisch potentieel bedreigt of zou kunnen bedreigen met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren en die opgenomen zijn in een op voorstel van de Minister van Justitie en de Minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst": elke uiting van het voornemen om de essentiële elementen van het wetenschappelijk en economisch potentieel van deze actoren in het gedrang te brengen;	2°/1 "activiteit die het wetenschappelijk en economisch potentieel bedreigt of zou kunnen bedreigen met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren en die opgenomen zijn in een op voorstel van de Minister van Justitie en de Minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst": elke uiting van het voornemen om de essentiële elementen van het wetenschappelijk en economisch potentieel van deze actoren in het gedrang te brengen;
3° "activiteit die de vervulling van de opdrachten van de strijdkrachten bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om de paraatstelling, de mobilisatie en de aanwending van de Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensie-organisaties te neutraliseren, te belemmeren, te saboteren, in het gedrang te brengen of te verhinderen bij opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband;	3° "activiteit die de vervulling van de opdrachten van de strijdkrachten bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om de paraatstelling, de mobilisatie en de aanwending van de Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensie-organisaties te neutraliseren, te belemmeren, te saboteren, in het gedrang te brengen of te verhinderen bij opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband;
4° "activiteit die de veiligheid van Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen": elke uiting van het voornemen om het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden collectief te schaden.	4° "activiteit die de veiligheid van Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen": elke uiting van het voornemen om het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden collectief te schaden.
§3. Op verzoek van de Algemene Dienst Inlichting en Veiligheid verleent de Veiligheid van de Staat zijn medewerking bij het inwinnen van inlichtingen wanneer personen die niet ressorteren onder de Minister van Landsverdediging of niet behoren tot ondernemingen die overeenkomsten uitvoeren, welke met hem, met internationale militaire organisaties of met derde landen worden gesloten in militaire aangelegenheden, of die deelnemen aan een gunningsprocedure van een overheidsopdracht die door de laatstgenoemden werd uitgeschreven,	§3. Op verzoek van de Algemene Dienst Inlichting en Veiligheid verleent de Veiligheid van de Staat zijn medewerking bij het inwinnen van inlichtingen wanneer personen die niet ressorteren onder de Minister van Landsverdediging of niet behoren tot ondernemingen die overeenkomsten uitvoeren, welke met hem, met internationale militaire organisaties of met derde landen worden gesloten in militaire aangelegenheden, of die deelnemen aan een gunningsprocedure van een overheidsopdracht die door de laatstgenoemden werd uitgeschreven,

betrokken zijn bij activiteiten bedoeld in paragraaf 1, 1°, 2°, 3° en 5°.	betrokken zijn bij activiteiten bedoeld in paragraaf 1, 1°, 2°, 3° en 5°.
De maatregelen inzake industriële bescherming worden enkel genomen wanneer de Minister van Landsverdediging, derde landen of de organisaties waarmee België verdragsrechtelijk of contractueel verbonden is, hierom verzoeken.	De maatregelen inzake industriële bescherming worden enkel genomen wanneer de Minister van Landsverdediging, derde landen of de organisaties waarmee België verdragsrechtelijk of contractueel verbonden is, hierom verzoeken.
	Afdeling 3/1 - Vorderingen tot bewaring
	Artikel 13/6
	§1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst om over te gaan tot:
	1° de bewaring van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen waarover hij beschikt op het tijdstip van de vordering;
	2° de bewaring van de verkeers- en lokalisatiegegevens die hij op basis van de vordering genereert en verwerkt.
	De in het eerste lid bedoelde vordering is gebaseerd op een schriftelijke en gemotiveerde beslissing van het diensthoofd of zijn gedelegeerde.
	§2. De vordering is gericht aan de in §1, eerste lid bedoelde operator of verstrekker en vermeldt:
	1° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;
	2° de personen, groeperingen, geografische gebieden, communicatiemiddelen en/of gebruikswijze waarvan de verkeers- en lokalisatiegegevens moeten bewaard worden;
	3° voor de maatregel bedoeld in § 1, eerste lid, 1°, de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen

	vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;
	4° voor de maatregel bedoeld in § 1, eerste lid, 2°:
	- de duur van de maatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;
	- de bewaartermijn die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;
	5° de datum van de vordering;
	6° de handtekening van het diensthoofd of van zijn gedelegeerde;
	§3. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de bewaring mondeling vorderen. Deze mondelinge vordering wordt schriftelijk bevestigd uiterlijk op de eerstvolgende werkdag.
	§4. De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring.
	Elke beslissing tot vordering en de motivering ervan worden ter kennis gebracht van het Vast Comité I. Indien het Vast Comité I een onwettigheid vaststelt, maakt het een einde aan de vordering.
	Indien de vordering voortijdig wordt beëindigd, wordt de gevorderde operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst daarvan zo spoedig mogelijk op de hoogte gebracht.
	§5. Voor de uitvoering van de vordering kan het diensthoofd of zijn gedelegeerde de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni

	2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag.
	§6. Eenieder die weigert zijn medewerking te verlenen aan de in § 1 en § 5 bedoelde vorderingen, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.
	§7. De Koning kan, op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de elektronische communicatie, de nadere regels bepalen voor de samenwerking van de operatoren en de verstrekkers.
	Artikel 13/7
	§1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, de medewerking vorderen van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronisch communicatiedienst om over te gaan tot de algemene en ongedifferentieerde bewaring van de door hen gegenereerde en verwerkte verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen.
	§2. De in § 1 bedoelde vordering kan enkel ingesteld worden mits een voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar akkoord binnen vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.
	§3. De vraag van het diensthoofd om een vordering tot bewaring in te stellen vermeldt, op straffe van onwettigheid:
	1° de ernstige dreiging tegen de nationale veiligheid die reëel en actueel of voorzienbaar is;

	2° de feitelijke omstandigheden die de ongedifferentieerde en algemene bewaring van de verkeers- en lokalisatiegegevens rechtvaardigen;
	3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;
	4° de duur van de bewaringsmaatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering. Hij kan volgens dezelfde procedure worden verlengd;
	5° de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie. Hij kan volgens dezelfde procedure worden verlengd;
	6° in voorkomend geval, de redenen die de in § 5 bedoelde hoogdringendheid rechtvaardigen;
	7° de datum van de vraag;
	8° de handtekening van het diensthoofd.
	§4. De vordering is gericht aan de in § 1 bedoelde operatoren en verstrekkers en vermeldt:
	1° de datum van het akkoord van de Commissie;
	2° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;
	3° de duur van de maatregel en de bewaartermijn van de gegevens;
	4° de datum van de vordering;
	5° de handtekening van het diensthoofd of zijn gedelegeerde.
	§5. In geval van hoogdringendheid vraagt het diensthoofd vooraf om het mondelinge akkoord van de voorzitter van de Commissie of, indien deze niet beschikbaar is, een ander lid van de Commissie. De auteur van het akkoord

	informeert onmiddellijk de andere commissieleden. Het diensthoofd bevestigt zijn vraag schriftelijk binnen 24 uur volgend op het akkoord. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord is gedurende vijf dagen geldig.
	§6. De vordering tot een algemene en ongedifferentieerde bewaring wordt bevestigd bij koninklijk besluit.
	Het koninklijk besluit vermeldt enkel:
	1° de datum van het akkoord van de Commissie;
	2° de datum van de vordering;
	3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;
	4° de duur van de maatregel en de bewaartermijn van de gegevens;
	Bij gebrek aan bevestiging bij koninklijk besluit binnen een maand na de vordering, eindigt de vordering.
	De gevorderde operatoren van een elektronisch communicatienetwerk of verstrekkers van een elektronische communicatiedienst worden hiervan zo spoedig mogelijk op de hoogte gebracht.
	§7. Voor de uitvoering van de vordering kan het diensthoofd de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag en het akkoord van de Commissie.
	§8. Eenieder die weigert zijn medewerking te verlenen aan de in § 1 en § 7 bedoelde vorderingen wordt gestraft met een geldboete van zesentwintig tot twintigduizend euro.

	§9. De Commissie geeft onverwijld de vraag van het diensthoofd en haar akkoord door aan het Vast Comité I.
	§10. De inlichtingen- en veiligheidsdienst brengt om de twee weken verslag uit aan de Commissie over de evolutie van de dreiging. Dit verslag belicht de elementen die ofwel de handhaving van de algemene en ongedifferentieerde bewaring, ofwel de beëindiging ervan rechtvaardigen.
	§11. Het diensthoofd beëindigt de vordering, niettegenstaande de bevestiging bij koninklijk besluit, wanneer de bewaring niet langer van nut is voor de bestrijding van de reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, wanneer deze dreiging is verdwenen of wanneer hij een onwettigheid vaststelt.
	Wanneer de Commissie of het Vast Comité I een onwettigheid vaststelt, wordt een einde gemaakt aan de vordering niettegenstaande de bevestiging bij koninklijk besluit.
	Indien voortijdig aan de vordering een einde wordt gemaakt, worden de gevorderde operatoren van elektronisch communicatienetwerken of de verstrekkers van elektronische communicatiediensten daarvan zo spoedig mogelijk op de hoogte gebracht.
	§12. De Koning bepaalt, op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de elektronische communicatie, de nadere regels voor de samenwerking van de operatoren en de verstrekkers.
Artikel 18/7	**Artikel 18/7**
§1. In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing, overgaan of doen overgaan tot:	§1. **De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,** overgaan of doen overgaan tot:
1° de identificatie of de lokalisatie, met behulp van een technisch middel, van de elektronische	1° de identificatie of de lokalisatie, met behulp van een technisch middel, van de elektronische

communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt;	communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt;
2° de vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst. Een inlichtingen- en veiligheidsdienst kan de bedoelde gegevens ook verkrijgen met behulp van toegang tot de bestanden van de klanten van de operator of van de verstrekker van de dienst.	2° de vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van **de mededeling van de facturen met betrekking tot de geïdentificeerde abonnementen,** de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst. Een inlichtingen- en veiligheidsdienst kan de bedoelde gegevens ook verkrijgen met behulp van toegang tot de bestanden van de klanten van de operator of van de verstrekker van de dienst.
§2. […]	§2. […]
§3. Iedere operator van een communicatienetwerk en iedere verstrekker van een communicatiedienst die wordt gevorderd om de in § 1 bedoelde gegevens mee te delen, verstrekt aan het diensthoofd de gegevens waarom werd verzocht binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op het voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de elektronische communicatie.	§3. Iedere operator van een communicatienetwerk en iedere verstrekker van een communicatiedienst die wordt gevorderd om de in § 1 bedoelde gegevens mee te delen, verstrekt aan het diensthoofd de gegevens waarom werd verzocht binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op het voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de elektronische communicatie.
De Koning bepaalt, op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de elektronische communicatie, de voorwaarden waaronder de in § 1 bedoelde toegang mogelijk is voor het diensthoofd.	De Koning bepaalt, op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de elektronische communicatie, de voorwaarden waaronder de in § 1 bedoelde toegang mogelijk is voor **de betrokken dienst.**
Elke in het eerste lid bedoelde persoon die weigert de aldus gevraagde gegevens mee te delen, wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.	Elke in het eerste lid bedoelde persoon die weigert de aldus gevraagde gegevens mee te delen, wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.
Artikel 18/8	**Artikel 18/8**
§1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van	§1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van

hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:	hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:
1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;	1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;
2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.	2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.
In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de [verkeersgegevens] worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.	In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de [verkeersgegevens] worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.
De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.	De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.
§2. Wat betreft de toepassing van de methode bedoeld in paragraaf 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing:	**§2. [Vernietigd door het Grondwettelijk Hof]**
1° voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd in zijn beslissing de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing;	
2° voor een potentiële dreiging, andere dan deze bedoeld in de bepalingen onder 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing;	

3° voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van twaalf maanden voorafgaand aan de beslissing.	
§3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de Elektronische Communicatie.	§3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in § 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de Minister van Justitie, de Minister van Landsverdediging en de Minister bevoegd voor de Elektronische Communicatie.
Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.	Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.
§4. […]	§4. […]
Artikel 18/14	**Artikel 18/14**
§1. In het belang van de uitoefening van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten de al dan niet aan een postoperator toevertrouwde post openmaken en kennisnemen van de inhoud ervan.	§1. **De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,** de al dan niet aan een postoperator toevertrouwde post openmaken en kennisnemen van de inhoud ervan.
De in het eerste lid bedoelde postoperator is ertoe gehouden de post waarop de machtiging betrekking heeft tegen ontvangstbewijs af te geven aan een agent van de dienst, op vertoon van zijn legitimatiebewijs en een schriftelijke vraag van het diensthoofd. Deze vraag vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.	De in het eerste lid bedoelde postoperator is ertoe gehouden de post waarop de machtiging betrekking heeft tegen ontvangstbewijs af te geven aan een agent van de dienst, op vertoon van zijn legitimatiebewijs en een schriftelijke vraag van het diensthoofd. Deze vraag vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.
§2. De diensten zien erop toe dat een door een postoperator afgegeven postzending, na onderzoek ervan, onverwijld aan de	§2. De diensten zien erop toe dat een door een postoperator afgegeven postzending, na onderzoek ervan, onverwijld aan de

postoperator wordt teruggegeven voor verdere verzending.	postoperator wordt teruggegeven voor verdere verzending.
§3. De postoperator die weigert de medewerking te verlenen als bedoeld in de § § 1 en 2 wordt gestraft met geldboete van zesentwintig tot twintigduizend euro.	§3. De postoperator die weigert de medewerking te verlenen als bedoeld in de § § 1 en 2 wordt gestraft met geldboete van zesentwintig tot twintigduizend euro.
§4. De Staat is burgerrechtelijk aansprakelijk jegens de postoperator voor de schade toegebracht aan de hem toevertrouwde post.	§4. De Staat is burgerrechtelijk aansprakelijk jegens de postoperator voor de schade toegebracht aan de hem toevertrouwde post.
Artikel 18/17	**Artikel 18/17**
§1. In het belang van de uitvoering van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten communicaties onderscheppen, er kennis van nemen en ze registreren.	§1. **De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,** communicaties onderscheppen, er kennis van nemen en ze registreren.
§2. Hiertoe kunnen de inlichtingen- en veiligheidsdiensten, zonder medeweten of toestemming van de eigenaar of zijn rechthebbende, op ieder ogenblik, al dan niet voor het publiek toegankelijke plaatsen betreden, teneinde:	§2. Hiertoe kunnen de inlichtingen- en veiligheidsdiensten, zonder medeweten of toestemming van de eigenaar of zijn rechthebbende, op ieder ogenblik, al dan niet voor het publiek toegankelijke plaatsen betreden, teneinde:
1° er een technisch middel te installeren, dat middel te bedienen of het terug te nemen;	1° er een technisch middel te installeren, dat middel te bedienen of het terug te nemen;
2° een vergrendeld voorwerp te openen om er een technisch middel in te plaatsen;	2° een vergrendeld voorwerp te openen om er een technisch middel in te plaatsen;
3° het voorwerp mee te nemen waarop het technisch middel zal worden geïnstalleerd, dat voorwerp te bedienen en het terug te plaatsen.	3° het voorwerp mee te nemen waarop het technisch middel zal worden geïnstalleerd, dat voorwerp te bedienen en het terug te plaatsen.
Het technisch middel of het meegenomen voorwerp wordt zo spoedig mogelijk na de onderschepping teruggenomen respectievelijk teruggeplaatst, tenzij dit het goede verloop van de opdracht in de weg staat.	Het technisch middel of het meegenomen voorwerp wordt zo spoedig mogelijk na de onderschepping teruggenomen respectievelijk teruggeplaatst, tenzij dit het goede verloop van de opdracht in de weg staat.
§3. Indien er een ingreep nodig is op een elektronisch communicatienetwerk, wordt de operator van het netwerk of de verstrekker van een elektronische communicatiedienst met een schriftelijke vraag van het diensthoofd gevorderd en is hij, als gevolg van deze aanvraag ertoe gehouden zijn technische medewerking te verlenen. Deze vraag vermeldt, naargelang het	§3. Indien er een ingreep nodig is op een elektronisch communicatienetwerk, wordt de operator van het netwerk of de verstrekker van een elektronische communicatiedienst met een schriftelijke vraag van het diensthoofd gevorderd en is hij, als gevolg van deze aanvraag ertoe gehouden zijn technische medewerking te verlenen. Deze vraag vermeldt, naargelang het

geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.	geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.
Eenieder die zijn technische medewerking weigert te verlenen aan de in het eerste lid bedoelde vorderingen, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro. De nadere regels en termijnen voor deze technische medewerking worden door de Koning vastgesteld, op voorstel van de Ministers van Justitie, van Landsverdediging en van de Minister bevoegd voor de Elektronische Communicatie.	Eenieder die zijn technische medewerking weigert te verlenen aan de in het eerste lid bedoelde vorderingen, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro. De nadere regels en termijnen voor deze technische medewerking worden door de Koning vastgesteld, op voorstel van de Ministers van Justitie, van Landsverdediging en van de Minister bevoegd voor de Elektronische Communicatie.
§4. De communicaties die verzameld werden aan de hand van de in §1 bedoelde uitzonderlijke methode worden opgenomen. Het voorwerp van de uitzonderlijke methode alsook de dagen en uren waarop deze is uitgevoerd, worden opgenomen bij het begin en op het einde van iedere opname die erop betrekking heeft.	§4. De communicaties die verzameld werden aan de hand van de in §1 bedoelde uitzonderlijke methode worden opgenomen. Het voorwerp van de uitzonderlijke methode alsook de dagen en uren waarop deze is uitgevoerd, worden opgenomen bij het begin en op het einde van iedere opname die erop betrekking heeft.
Alleen die delen van de opname van communicaties die door het diensthoofd of, naargelang het geval, in zijn opdracht door de directeur Operaties of de persoon die hij daartoe heeft aangewezen voor de Veiligheid van de Staat, of door de officier of de burgerambtenaar, die minstens de graad van commissaris heeft, voor de Algemene Dienst Inlichting en Veiligheid relevant worden geacht, kunnen worden overgeschreven.	Alleen die delen van de opname van communicaties die door het diensthoofd of, naargelang het geval, in zijn opdracht door de directeur Operaties of de persoon die hij daartoe heeft aangewezen voor de Veiligheid van de Staat, of door de officier of de burgerambtenaar, die minstens de graad van commissaris heeft, voor de Algemene Dienst Inlichting en Veiligheid relevant worden geacht, kunnen worden overgeschreven.
Iedere notitie die in het kader van de uitvoering van de uitzonderlijke methode door de daartoe aangewezen personen werd genomen en die niet werd opgenomen in een verslag, wordt vernietigd door de in het tweede lid vermelde personen of door de persoon die zij hiertoe aanwijzen. Deze vernietiging maakt het voorwerp uit van een vermelding in het bijzondere register waarin wordt voorzien in §6.	Iedere notitie die in het kader van de uitvoering van de uitzonderlijke methode door de daartoe aangewezen personen werd genomen en die niet werd opgenomen in een verslag, wordt vernietigd door de in het tweede lid vermelde personen of door de persoon die zij hiertoe aanwijzen. Deze vernietiging maakt het voorwerp uit van een vermelding in het bijzondere register waarin wordt voorzien in §6.
§5. De opnamen worden samen met de eventuele overschrijving van de relevant geachte communicaties of de eventuele vertaling bewaard, op een beveiligde plaats die het diensthoofd aanduidt overeenkomstig de	§5. De opnamen worden samen met de eventuele overschrijving van de relevant geachte communicaties of de eventuele vertaling bewaard, op een beveiligde plaats die het diensthoofd aanduidt overeenkomstig de

vereisten van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.	vereisten van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.
§6. Een regelmatig bijgehouden bijzonder register bevat een overzicht van elk van de in de §§ 1 en 2 bedoelde maatregelen.	§6. Een regelmatig bijgehouden bijzonder register bevat een overzicht van elk van de in de §§ 1 en 2 bedoelde maatregelen.
Het overzicht vermeldt de datum en het uur waarop de maatregel is gestart en waarop hij werd beëindigd.	Het overzicht vermeldt de datum en het uur waarop de maatregel is gestart en waarop hij werd beëindigd.
§7. De opnamen van communicaties worden volgens de door de Koning vastgestelde nadere regels en onder het toezicht van de Commissie en van een door het diensthoofd hiertoe aangestelde agent, vernietigd binnen een termijn van vijf jaar die aanvangt op de dag van de opname. Met het voorafgaand schriftelijk akkoord van de Commissie kan het diensthoofd beslissen om de bewaringsperiode te verlengen wanneer de opname nog noodzakelijk is in het kader van een inlichtingenonderzoek of van een gerechtelijke procedure. De totale bewaringsperiode mag tien jaar niet te boven gaan behalve wanneer een opname nog noodzakelijk is in het kader van een gerechtelijke procedure. De vernietiging wordt vermeld in het in paragraaf 6 vermelde bijzonder register.	§7. De opnamen van communicaties worden volgens de door de Koning vastgestelde nadere regels en onder het toezicht van de Commissie en van een door het diensthoofd hiertoe aangestelde agent, vernietigd binnen een termijn van vijf jaar die aanvangt op de dag van de opname. Met het voorafgaand schriftelijk akkoord van de Commissie kan het diensthoofd beslissen om de bewaringsperiode te verlengen wanneer de opname nog noodzakelijk is in het kader van een inlichtingenonderzoek of van een gerechtelijke procedure. De totale bewaringsperiode mag tien jaar niet te boven gaan behalve wanneer een opname nog noodzakelijk is in het kader van een gerechtelijke procedure. De vernietiging wordt vermeld in het in paragraaf 6 vermelde bijzonder register.
De overschrijvingen van de relevant geachte communicaties en de eventuele vertalingen worden bewaard en vernietigd overeenkomstig artikel 21.	De overschrijvingen van de relevant geachte communicaties en de eventuele vertalingen worden bewaard en vernietigd overeenkomstig artikel 21.
HOOFDSTUK 8 – Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten	
Art. 84	**Art. 84**
§ 1. Voor de doeleinden bedoeld in artikel 82, 2°, en mits de voorafgaandelijke toestemming van een onderzoeksrechter, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur wanneer hij van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische	§ 1. Voor de doeleinden bedoeld in artikel 82, 2°, en mits de voorafgaandelijke toestemming van een onderzoeksrechter, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur wanneer hij van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische

communicatie noodzakelijk maken om de waarheid aan de dag te brengen:	communicatie noodzakelijk maken om de waarheid aan de dag te brengen:
1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties werden gedaan;	1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties werden gedaan;
2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren, met inbegrip van de telefoonnummers en netwerkadressen.	2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren, met inbegrip van de telefoonnummers en netwerkadressen.
3° de betalingsdetails van de elektronische communicatiediensten opvragen.	3° de betalingsdetails van de elektronische communicatiediensten opvragen.
Hiertoe kan hij de medewerking vorderen van:	Hiertoe kan hij de medewerking vorderen van:
1° de operator van een elektronisch communicatienetwerk;	1° de operator van een elektronisch communicatienetwerk;
2° iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.	2° iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.
In de gevallen bedoeld in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de elektronische communicatie vastgesteld en opgenomen in een proces-verbaal.	In de gevallen bedoeld in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de elektronische communicatie vastgesteld en opgenomen in een proces-verbaal.
De auditeur, of, in zijn afwezigheid, de adjunct-auditeur doet in zijn beslissing opgave van de feitelijke omstandigheden die de maatregel rechtvaardigen en hij houdt rekening met het evenredigheids- en subsidiariteitsbeginsel bij de motivering van zijn beslissing.	De auditeur, of, in zijn afwezigheid, de adjunct-auditeur doet in zijn beslissing opgave van de feitelijke omstandigheden die de maatregel rechtvaardigen en hij houdt rekening met het evenredigheids- en subsidiariteitsbeginsel bij de motivering van zijn beslissing.

Hij vermeldt ook de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 1bis.	Hij vermeldt ook de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 1bis.
§ 1*bis*. De gegevens bedoeld in paragraaf 1, eerste lid, kunnen worden opgevraagd voor een periode van twaalf maanden voorafgaand aan de beslissing van de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, en voor een periode van zes maanden voor de overige inbreuken waarvoor de auditeur deze gegevens kan opvragen.	§ 1*bis*. De gegevens bedoeld in paragraaf 1, eerste lid, kunnen worden opgevraagd voor een periode van twaalf maanden voorafgaand aan de beslissing van de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, en voor een periode van zes maanden voor de overige inbreuken waarvoor de auditeur deze gegevens kan opvragen.
	§ 1*bis*/1. Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de in paragraaf 1, tweede lid, bedoelde actoren bevelen om de gegevens bedoeld in paragraaf 1, eerste lid, die riskeren te worden verwijderd of anoniem gemaakt, te bewaren totdat hij de toestemming van een onderzoeksrechter heeft bekomen om de mededeling van deze gegevens te vorderen
	Paragrafen 1, vierde en vijfde lid, en 3 zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.
	De in paragraaf 1, tweede lid, bedoelde actoren zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.
	De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, verzoekt onverwijld de voorafgaande toestemming van een onderzoeksrechter om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens die het voorwerp uitmaken van een in het eerste lid bedoeld bevel tot bewaring en bezorgt dit bevel aan de onderzoeksrechter. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel tot bewaring betrekking heeft of oordeelt dat dit bevel niet wettig of niet gerechtvaardigd was, vervalt het

	bevel. In dat geval brengt de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de bestemmeling van het bevel tot bewaring er onverwijld van op de hoogte dat het vervallen is.
§ 1*ter*. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht wordt een inbreuk te hebben gepleegd waarvoor de auditeur de gegevens bedoeld in paragraaf 1, eerste lid, kan opvragen, of indien precieze feiten doen vermoeden dat derden die ervan verdacht worden dergelijke inbreuk te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.	§ 1*ter*. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht wordt een inbreuk te hebben gepleegd waarvoor de auditeur de gegevens bedoeld in paragraaf 1, eerste lid, kan opvragen, of indien precieze feiten doen vermoeden dat derden die ervan verdacht worden dergelijke inbreuk te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.
De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is. Diezelfden zullen door de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet gebruikt.	De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is. Diezelfden zullen door de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet gebruikt.
§ 2. De actoren bedoeld in § 1, tweede lid, delen, na ontvangst van de in § 1 bedoelde vordering, onverwijld aan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur de schatting van de kostprijs mee van de gevraagde inlichtingen en van de termijn die nodig is om de informatie te verzamelen.	§ 2. De actoren bedoeld in § 1, tweede lid, delen, na ontvangst van de in § 1 bedoelde vordering, onverwijld aan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur de schatting van de kostprijs mee van de gevraagde inlichtingen en van de termijn die nodig is om de informatie te verzamelen.
Na ontvangst van de bevestiging van de vordering van de auditeur, of, in zijn afwezigheid, de adjunct-auditeur verschaffen de in het eerste lid bedoelde actoren, de gevraagde gegevens binnen een door de auditeur, of, in zijn afwezigheid, de adjunct-auditeur bepaalde termijn.	Na ontvangst van de bevestiging van de vordering van de auditeur, of, in zijn afwezigheid, de adjunct-auditeur verschaffen de in het eerste lid bedoelde actoren, de gevraagde gegevens binnen een door de auditeur, of, in zijn afwezigheid, de adjunct-auditeur bepaalde termijn.
§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

HOOFDSTUK 9 – Wijzigingen aan de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk-en informatiesystemen van algemeen belang voor de openbare veiligheid (“NIS-wet”)	
Art. 62	**Art. 62**
§ 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.	**§ 1. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.**
	§ 2. Indien dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, a) tot e), van deze wet, kan het nationale CSIRT gegevens over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie verkrijgen van een operator als bedoeld in artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die deze gegevens bewaart.
	De doeleinden van voornoemde taken zijn:
	- het voorkomen van ernstige bedreigingen voor de openbare veiligheid;
	- het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen;
	- het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten.
	Indien het nationale CSIRT een operator een verzoek om gegevens over de gebruiker of abonnee bedoeld in artikel 2, 5°, van de wet van 17 januari 2003 met betrekking tot het

	statuut van de regulator van de Belgische post- en telecommunicatiesector stuurt, wordt dat verzoek toegestaan door de hiërarchische meerdere.
	Indien het nationale CSIRT een operator een verzoek om elektronische-communicatiemetagegevens als bedoeld in artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie die geen in het vorige lid bedoelde gegevens zijn, stuurt, moet dat verzoek vooraf worden gecontroleerd door de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017.
	In dringende en naar behoren gemotiveerde gevallen kan het nationale CSIRT optreden zonder de voorafgaande controle bedoeld in het vorige lid, en de gegevens rechtstreeks opvragen. Dit verzoek wordt onverwijld naar de in het vorige lid bedoelde overheid gestuurd om een latere controle mogelijk te maken.
	De directeur van het nationale CSIRT wijst uitdrukkelijk de personen aan die gemachtigd zijn om deze elektronische-communicatiegegevens te verwerken.
	Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd.
§ 3. Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.	**§ 3. Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.**
§ 4. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd dat de	**§ 4. Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd**

werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.	**dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.**
De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.	**De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.**
Art. 65	**Art. 65**
§ 1. Overeenkomstig artikel 5.1.c) van Verordening EU 2016/679 zorgt de verwerkingsverantwoordelijke, bij de verwerking van persoonsgegevens in het kader van de uitvoering van deze wet, ervoor dat de verwerking tot het noodzakelijke minimum beperkt blijft en in verhouding staat tot het nagestreefde doeleinde.	§ 1. Overeenkomstig artikel 5.1.c) van Verordening EU 2016/679 zorgt de verwerkingsverantwoordelijke, bij de verwerking van persoonsgegevens in het kader van de uitvoering van deze wet, ervoor dat de verwerking tot het noodzakelijke minimum beperkt blijft en in verhouding staat tot het nagestreefde doeleinde.
§ 2. Overeenkomstig dat beginsel kunnen de verwerkte persoonsgegevens allerhande gegevens zijn in verband met de beveiliging van netwerk- en informatiesystemen, namelijk in voorkomend geval nominatieve informatie, gegevens over de medewerkers van een organisatie of externe personen, verbindingsgegevens of -identificatoren, locatie-gegevens, identificatie- of authenticatiegegevens, in voorkomend geval met behulp van beveiligde systemen.	§ 2. Overeenkomstig dat beginsel kunnen de verwerkte persoonsgegevens allerhande gegevens zijn in verband met de beveiliging van netwerk- en informatiesystemen, namelijk in voorkomend geval nominatieve informatie, gegevens over de medewerkers van een organisatie of externe personen, verbindingsgegevens of -identificatoren, **elektronische communicatiegegevens,** locatie-gegevens, identificatie- of authenticatiegegevens, in voorkomend geval met behulp van beveiligde systemen.
§ 3. De belangrijkste verwerkingen van persoonsgegevens in het kader van deze wet kunnen als volgt worden ingedeeld:	§ 3. De belangrijkste verwerkingen van persoonsgegevens in het kader van deze wet kunnen als volgt worden ingedeeld:
- algemene informatie-uitwisseling tussen aanbieders van essentiële diensten en digitaledienstverleners, enerzijds, en de autoriteit bedoeld in artikel 7, anderzijds;	- algemene informatie-uitwisseling tussen aanbieders van essentiële diensten en digitaledienstverleners, enerzijds, en de autoriteit bedoeld in artikel 7, anderzijds;
- de verwerking van specifieke informatie tussen de entiteiten bedoeld in het eerste streepje in het kader van incidentmeldingen of andere specifieke uitwisselingen;	- de verwerking van specifieke informatie tussen de entiteiten bedoeld in het eerste streepje in het kader van incidentmeldingen of andere specifieke uitwisselingen;
- de verwerking door inspectiediensten overeenkomstig titel 4;	- de verwerking door inspectiediensten overeenkomstig titel 4;

- de verwerking door hoven en rechtbanken of sectorale overheden in het kader van de uitvoering van de wet en met name de opsporing, vervolging en bestraffing van inbreuken;	- de verwerking door hoven en rechtbanken of sectorale overheden in het kader van de uitvoering van de wet en met name de opsporing, vervolging en bestraffing van inbreuken;
- de uitwisseling en andere verwerking van informatie door het nationale en sectorale CSIRT voor hun opdrachten respectievelijk bedoeld in de artikelen 60 tot 62, 63 en 64.	- de uitwisseling en andere verwerking van informatie door het nationale en sectorale CSIRT voor hun opdrachten respectievelijk bedoeld in de artikelen 60 tot 62, 63 en 64.
HOOFDSTUK 10 – Wijziging aan de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten	
Art. 11	**Art. 11**
§ 1. Onverminderd de ambtsbevoegdheden van de officieren van gerechtelijke politie, zien de daartoe door de Koning aangewezen statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu toe op de uitvoering van de bepalingen van deze wet en van zijn uitvoeringsbesluiten evenals van de verordeningen van de Europese Unie en die behoren tot de bevoegdheden van Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu door, voorzien van behoorlijke legitimatiebewijzen die door de Koning verder worden uitgewerkt, onaangekondigde inspecties uit te voeren.	§ 1. Onverminderd de ambtsbevoegdheden van de officieren van gerechtelijke politie, zien de daartoe door de Koning aangewezen statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu toe op de uitvoering van de bepalingen van deze wet en van zijn uitvoeringsbesluiten evenals van de verordeningen van de Europese Unie en die behoren tot de bevoegdheden van Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu door, voorzien van behoorlijke legitimatiebewijzen die door de Koning verder worden uitgewerkt, onaangekondigde inspecties uit te voeren.
De contractuele personeelsleden leggen voorafgaand aan de uitoefening van hun functie, de eed af in handen van de minister of van zijn aangestelde.	De contractuele personeelsleden leggen voorafgaand aan de uitoefening van hun functie, de eed af in handen van de minister of van zijn aangestelde.
De door de Koning aangewezen statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu belast met het toezicht op de toepassing van deze wet en op de ter uitvoering ervan getroffen besluiten hebben, binnen de perken van de uitoefening van hun bevoegdheid, zonder voorafgaande verwittiging, toegang tot alle plaatsen die worden gebruikt voor de handel van voedingsmiddelen of andere in deze wet bedoelde producten en tot de daaraan grenzende opslagplaatsen en tot andere	De door de Koning aangewezen statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu belast met het toezicht op de toepassing van deze wet en op de ter uitvoering ervan getroffen besluiten hebben, binnen de perken van de uitoefening van hun bevoegdheid, zonder voorafgaande verwittiging, toegang tot alle plaatsen die worden gebruikt voor de handel van voedingsmiddelen of andere in deze wet bedoelde producten en tot de daaraan grenzende opslagplaatsen en tot andere

plaatsen die aan hun toezicht onderworpen zijn of waarvan zij redelijkerwijze vermoeden dat er inbreuken gepleegd worden op de bepalingen van de wetgevingen waarop zij toezicht uitoefenen. Zij kunnen deze doorzoeken, zelfs indien deze voor het publiek niet toegankelijk zijn.	plaatsen die aan hun toezicht onderworpen zijn of waarvan zij redelijkerwijze vermoeden dat er inbreuken gepleegd worden op de bepalingen van de wetgevingen waarop zij toezicht uitoefenen. Zij kunnen deze doorzoeken, zelfs indien deze voor het publiek niet toegankelijk zijn.
Zij hebben zonder voorafgaande verwittiging te allen tijde toegang tot de plaatsen die dienen voor de fabricage van voedingsmiddelen of andere in deze wet bedoelde producten die voor de handel bestemd zijn, alsook tot de plaatsen waar deze zijn opgeslagen.	Zij hebben zonder voorafgaande verwittiging te allen tijde toegang tot de plaatsen die dienen voor de fabricage van voedingsmiddelen of andere in deze wet bedoelde producten die voor de handel bestemd zijn, alsook tot de plaatsen waar deze zijn opgeslagen.
Het bezoek aan plaatsen die uitsluitend als woning dienen is slechts toegestaan tussen 5 uur `s ochtends en 9 uur `s avonds en kan slechts gebeuren met verlof van de rechter.	Het bezoek aan plaatsen die uitsluitend als woning dienen is slechts toegestaan tussen 5 uur `s ochtends en 9 uur `s avonds en kan slechts gebeuren met verlof van de rechter.
Zij mogen de overlegging eisen van alle handelsdocumenten en bescheiden betreffende voedingsmiddelen en andere bij deze wet bedoelde producten en van alle documenten verplicht gesteld bij de krachtens deze wet uitgevaardigde besluiten.	Zij mogen de overlegging eisen van alle handelsdocumenten en bescheiden betreffende voedingsmiddelen en andere bij deze wet bedoelde producten en van alle documenten verplicht gesteld bij de krachtens deze wet uitgevaardigde besluiten.
Zij mogen overgaan tot de controle van transporten, openbaar vervoer en vervoermiddelen.	Zij mogen overgaan tot de controle van transporten, openbaar vervoer en vervoermiddelen.
	Zij mogen natuurlijke en rechtspersonen identificeren aan de hand van het telefoonnummer van de betrokkene of het IP-adres dat aan de bron van de elektronische communicatie ligt.
	Hiertoe mogen zij met gemotiveerd verzoek de verstrekking van de identificatiedocumenten en gegevens vorderen van :
	1° de operator van een elektronisch communicatienetwerk; en
	2° iedereen die binnen het Belgisch grondgebied, op welke wijze ook een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen

	of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.
	Onverminderd een eventuele delegatie, dient elk identificatieverzoek voorafgaand, door het diensthoofd van de Inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu schriftelijk goedgekeurd te worden.
§ 2. Zij stellen de overtredingen van de desbetreffende wetten en besluiten vast in processen-verbaal die gelden tot het tegendeel bewezen is.	§ 2. Zij stellen de overtredingen van de desbetreffende wetten en besluiten vast in processen-verbaal die gelden tot het tegendeel bewezen is.
Ze kunnen overgaan tot het verhoor van de overtreder en tot elk ander nuttig verhoor.	Ze kunnen overgaan tot het verhoor van de overtreder en tot elk ander nuttig verhoor.
Een afschrift van het proces-verbaal wordt binnen dertig dagen na de vaststelling van de overtreding aan de geverbaliseerde overgezonden.	Een afschrift van het proces-verbaal wordt binnen dertig dagen na de vaststelling van de overtreding aan de geverbaliseerde overgezonden.
Ze kunnen, bij de uitoefening van hun opdrachten, de hulp van de politiemacht inroepen.	Ze kunnen, bij de uitoefening van hun opdrachten, de hulp van de politiemacht inroepen.
Zij kunnen overgaan tot de verzegeling van automatische distributieapparaten die niet voldoen aan artikel 6, §§ 4 en 6. De voorwaarden hiervoor worden uitgewerkt door de minister.	Zij kunnen overgaan tot de verzegeling van automatische distributieapparaten die niet voldoen aan artikel 6, §§ 4 en 6. De voorwaarden hiervoor worden uitgewerkt door de minister.
Zij kunnen overgaan tot elk onderzoek, controle en verhoor en alle inlichtingen inwinnen die zij nodig achten om zich ervan te vergewissen dat de bepalingen van de wetgeving waarop zij toezicht uitoefenen, werkelijk worden nageleefd, en inzonderheid de identiteit opnemen van gelijk welke persoon, wiens verhoor zij nodig achten voor de uitoefening van het toezicht.	Zij kunnen overgaan tot elk onderzoek, controle en verhoor en alle inlichtingen inwinnen die zij nodig achten om zich ervan te vergewissen dat de bepalingen van de wetgeving waarop zij toezicht uitoefenen, werkelijk worden nageleefd, en inzonderheid de identiteit opnemen van gelijk welke persoon, wiens verhoor zij nodig achten voor de uitoefening van het toezicht.
§ 3. Het proces-verbaal houdende vaststelling van de overtredingen bedoeld in artikel 19 en opgesteld door de door de Koning aangestelde toezichthoudende personen, bedoeld in § 1, wordt overgemaakt aan de krachtens artikel 19 aangestelde ambtenaar. Indien dit proces-	§ 3. Het proces-verbaal houdende vaststelling van de overtredingen bedoeld in artikel 19 en opgesteld door de door de Koning aangestelde toezichthoudende personen, bedoeld in § 1, wordt overgemaakt aan de krachtens artikel 19 aangestelde ambtenaar. Indien dit proces-

verbaal is opgemaakt door de burgemeester of diens gemachtigde kan het eveneens aan deze ambtenaar worden toegezonden.	verbaal is opgemaakt door de burgemeester of diens gemachtigde kan het eveneens aan deze ambtenaar worden toegezonden.
Wanneer toepassing wordt gemaakt van artikel 11bis, wordt het proces-verbaal aan de procureur des Konings pas toegezonden, wanneer aan de waarschuwing geen gevolg is gegeven.	Wanneer toepassing wordt gemaakt van artikel 11bis, wordt het proces-verbaal aan de procureur des Konings pas toegezonden, wanneer aan de waarschuwing geen gevolg is gegeven.
§ 4. De Koning kan andere regelen voor de inspectie en controle vaststellen, ten einde te voldoen aan de verplichtingen die voortvloeien uit de internationale verdragen en de krachtens die verdragen tot stand gekomen internationale akten	§ 4. De Koning kan andere regelen voor de inspectie en controle vaststellen, ten einde te voldoen aan de verplichtingen die voortvloeien uit de internationale verdragen en de krachtens die verdragen tot stand gekomen internationale akten
§ 5. De bepalingen van dit artikel zijn niet van toepassing op de controles die worden verricht met toepassing van de wet van 4 februari 2000 houdende oprichting van het Federaal Agentschap voor de Veiligheid van de Voedselketen.	§ 5. De bepalingen van dit artikel zijn niet van toepassing op de controles die worden verricht met toepassing van de wet van 4 februari 2000 houdende oprichting van het Federaal Agentschap voor de Veiligheid van de Voedselketen.

ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA210014		21/05/2020

Objet : Avis relatif :

a) **à un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités ;**
a) **à un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques**

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e al., l'article 71 et le Titre VII, en particulier l'article 236 §2, 3ième al 236 LPD.
Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après la 'LAPD').
Vu la loi du 5 août 1992 sur la fonction de police (ci-après la 'LFP').
Vu la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ci-après la 'LPI').
Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après la *LED*).
Vu la demande du vice-premier ministre et ministre de la Justice et de la Mer du Nord, reçue par e-mail par l'Organe de contrôle le 7 mai 2021 à 20.08 h.
Vu la notification du Conseil des Ministres du 7 mai 2021.

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 21 mai 2021, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

...

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la LAPD dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

2. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice ou *LED*). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG'), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou « RGPD »).

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).

[3] Article 4 §2, 4e alinéa de la LAPD.

[4] Article 71 §1er, 3e alinéa de la LPD.

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.

4. Enfin, l'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *sur les douanes et accises* du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 "*modifiant diverses dispositions relatives au traitement des données des passagers*".

II. Objet de la demande

5. Le demandeur produit un "*avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités*" (ci-après 'l'avant-projet'), dont les déposants, outre le demandeur lui-même, sont le Premier Ministre, le Ministre des Finances, le Ministre des Affaires Sociales et de la Santé Publique, le Ministre des Télécommunications, le Ministre de la Défense, le Ministre de l'Intérieur et le Secrétaire d'État chargé de la Vie Privée. Est produit en même temps pour avis un projet d'arrêté d'exécution modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'l'arrêté d'exécution').

6. Le demandeur demande à l'Organe de Contrôle d'émettre un avis urgent, à savoir endéans le délai minimal de 15 jours fixé par la LPD[7]. Cette urgence n'a pas été notifiée en tant que telle par le Conseil des Ministres. Il n'est pas non plus clair pour le COC si l'urgence a été demandée dans la note au Conseil des Ministres. L'Organe de Contrôle comprend toutefois l'urgence à la lumière des motifs invoqués dans la lettre d'accompagnement du demandeur du 7 mai 2021. Vu toutefois le bref délai endéans lequel l'avis est demandé et doit être fourni sur deux textes substantiels, cet avis se limite aux remarques les plus essentielles.

7. Attendu que l'avant-projet et l'arrêté d'exécution ne traitent pas exclusivement et même pas en premier lieu de traitements de police, l'avis se limite aux articles des deux textes qui sont en rapport avec le traitement de données personnelles par la police intégrée (GPI), ce pourquoi l'Organe de Contrôle est exclusivement compétent.

Pour les autres dispositions, soit l'APD, soit le Comité permanent R sont compétents et il peut être fait référence aux avis respectifs des deux institutions.

III. Discussion de la demande

A. Remarques générales

[7] Art. 236 § 2, 3de alinéa LPD.

8. Pour le contenu général et la portée de l'avant-projet et de l'arrêté d'exécution, le COC se réfère à l'Exposé des Motifs approfondi (ci-après 'EdM'). L'objectif du rédacteur des textes produits consiste, en bref, à formuler une réponse à l'annulation par la Cour Constitutionnelle, par arrêté n° 57/2021, des articles 2,b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, suite à quoi le fonctionnement du système jusqu'alors en vigueur de conservation générale et non-différenciée de dites 'données de trafic et de localisation' a été rendu impossible, le tout suite à la jurisprudence de la Cour de Justice de l'Union européenne, plus amplement identifié dans l'EdM. La réponse du rédacteur de l'avant-projet et de l'arrêté d'exécution consiste en une réglementation qui impose une conservation plus 'orientée' des données de communication précitées aux opérateurs de télécommunication à des fins de *law enforcement*.

9. La plus grande partie de la législation qui est modifiée et des modifications qui sont visées concerne les traitements par les autorités ou les acteurs privés qui ne tombent pas sous la compétence de contrôle du COC. Les opérateurs, la FSMA[8], le CSIRT[9], etc. … sont de la compétence de l'APD, de sorte qu'à ce sujet, le COC se réfère à l'avis à émettre par l'APD. Les services de renseignements tombent sous la compétence du Comité permanent R, de sorte que, en ce qui concerne ces aspects, il faut se référer à l'avis du Comité précité.

10. Le COC limite dans cet avis son examen aux articles qui concernent directement ou indirectement les traitements de police de données personnelles qui sont repris dans l'avant-projet et l'arrêté d'exécution ou qui ont (peuvent avoir) directement ou indirectement une influence sur le fonctionnement de la police intégrée au sens large de la tenue des informations de police.

11. Dans ce projet, l'Organe de Contrôle reçoit une nouvelle compétence importante qui est directement en rapport avec le thème de la rétention de données et de leur utilisation dans le cadre de la fonction de police judiciaire. Le COC est chargé d'une forme de contrôle *a priori* des statistiques provenant de la Banque Générale Nationale de Données (ci-après 'BNG'), visée à l'article 44/7 LFP et prévus dans le projet d'article 126/1 de la Loi du 13 juin 2015 relative aux communications électroniques (ci-après 'LCE') par la GPI et plus précisément la direction de l'information policière et des moyens ICT de la police fédérale (ci-après 'DRI').

12. Le COC considère les nouvelles missions qui lui sont confiées comme une forme de reconnaissance et de valorisation de tout le travail qu'il a accompli sur une très brève durée, et plus précisément depuis le démarrage le 5 septembre 2018 (date de l'entrée en vigueur de la LPD), entre autres comme autorité de protection des données de la GPI. L'octroi de nouvelles compétences constitue un continuum caractérisé par de nouvelles missions qui ont été confiées au fil des années à l'Organe de Contrôle. L'option prise par le rédacteur de l'avant-projet se raccorde également à la vision de la Cour

[8] *Financial Services and Market Authority* (Autorité des Services et Marchés financiers).

[9] *Computer Security Incident Response Team*.

Constitutionnelle, qui, dans deux arrêts, a déjà dépeint le rôle fondamental de l'Organe de Contrôle. On peut en effet se référer aux arrêts 108/2016 du 14 juillet 2016 et 27/2020 du 20 février 2020 dans lesquels a été mis en lumière le rôle du COC, notamment en ce qui concerne la protection du droit fondamental à la vie privée et à la protection des données dans le cadre du traitement des données de police.

13. Il va toutefois de soi qu'il y a des limites à la capacité restreinte du COC – on peut se référer au rapport annuel 2016-2019[10] et 2020[11] du COC – où tout ceci est exposé et l'organisation est expliqué – de sorte qu'il faudra également prêter attention tant à l'octroi de moyens budgétaires suffisants qu'aux moyens en personnel.

Tout ceci évidemment à un moment où en même temps, d'une part, un des déposants de cet avant-projet et arrêté d'exécution, à savoir le Secrétaire d'État à la Vie Privée, est en pleine évaluation de la LPD sur base de l'article 286 LPD (auquel le COC a également transmis, à sa demande, une note et un avis circonstanciés dans lesquels sont reprises les lignes directrices des modifications et améliorations qui pourraient être apportées à la LPD) et d'autre part, la Chambre des Représentants insiste de son côté, dans le cadre d'un audit de la Cour des Comptes (qui a débuté en 2018 avec un suivi en 2020), pour obtenir des résultats tangibles sur le plan des synergies et de la *clustering* des compétences ou même du *clustering* d'institutions bénéficiant d'une dotation[12], avec toutes les conséquences potentielles pour le fonctionnement de l'Organe de Contrôle.

Les deux projets en cours viennent s'ajouter à de nombreux dossiers réactifs et proactifs que le COC doit déjà traiter dans lesquels le citoyen et la GPI se tournent toujours davantage vers l'Organe de Contrôle.
L'Organe de Contrôle demande aux décideurs d'y prêter l'attention nécessaire.

14. Il est enfin indiqué au rédacteur de l'avant-projet qu'une révision de la version néerlandaise des textes est encore nécessaire. Ceci vaut tant pour le corps des textes que pour l'Exposé des Motifs et le Rapport au Roi. Par ex. dans le corps, le projet d'art. 126/1 LCE doit être revu dans sa version néerlandaise ("*pour ce qui concerne*" est p.ex. mal traduit par "*voor*"). Ainsi, p.ex., dans l'EdM de la version française, à propos du critère géographique, il est question de "*… arrondissement par arrondissement, ou zones de police par zones de police* …" (p. 8), alors que le texte néerlandais parle de "*… wijk voor wijk of politiezone voor politiezone …*". Un quartier (wijk) n'est pas un arrondissement et inversement. "*… à charge de X"* est erronément traduit par "*onder de verantwoordelijkheid van x …"* (p. 10); "*arrondissement*" est traduit par "*district*" (p. 48), "*les opérateurs qui doivent effectuer les réquisitions* » est traduit par « *de operatoren die de opvordering moeten doen*" (p. 62), etc. …

[10] Voir, www.controleorgaan.be, https://www.organedecontrole.be/files/Rapports-dactivites-COC_Executive-Summary_FR.pdf

[11] Voir www.controleorgaan.be, à paraître fin mai 2021.

[12] Voir, La Chambre, pièce CRIV 55 plén. 100, du 29.04.2021, p. 41 et 42; DOC 55, 1924/001, p. 1-43, www.lachambre.be, https://www.lachambre.be/doc/flwb/pdf/55/1924/55k1924001.pdf

B. Remarques par article

B.1. Projet d'article 126/1 LCE (art. 8 avant-projet)

B.1.1. Généralités

15. Le projet d'article 126/1, important pour l'Organe de Contrôle, prévoit un système de sauvegarde différenciée sur base de zones géographiques. Celles-ci sont soit des arrondissements judiciaires dans le cas où il est question d'au moins 3 faits punissables en vertu de l'art. 90ter C.i.cr. (dénommés ci-après les 'délits graves') par 1.000 habitants/an sur une moyenne des 3 années calendrier précédentes, soit les zones de police qui font partie des arrondissements judiciaires précités où on a toutefois constaté moins de 3 délits graves par 1.000 habitants/an sur une moyenne des 3 dernières années précédentes. Dans l'EdM, il est exposé pour un certain nombre d'arrondissements de combien de délits graves il doit s'agir *in concreto* par an.

Le COC n'a pas de remarques particulières à ce sujet et comprend que les rédacteurs de l'avant-projet ont ainsi recherché au maximum à obtenir des critères objectifs en ligne avec la jurisprudence précitée de l'UE de la Cour de Justice. Il est évident que ce faisant, on tente également d'instaurer des critères réalisables. Les descriptions territoriales des arrondissements judiciaires et zones de police sont des descriptions connues avec lesquelles on peut rapidement se mettre au travail. Ladite 'liste des écoutes' de l'art. 90*ter* C.i.cr. est, *de lege lata*, en droit belge, le seul véritable critère utilisable pour pouvoir différencier lesdits 'délits graves' de la 'criminalité ordinaire'.

16. Le défi sera, également en ce qui concerne le contrôle par le COC, l'application pratique de cela, puisque la correction, la précision et l'exactitude des enregistrements BNG reçoivent une dimension et un intérêt supplémentaires. Ce principe fondamental de droit de protection des données, qui est déjà essentiel, gagne en effet encore en importance. Non seulement, l'obligation de conservation de données de trafic et de localisation en dépend en tant que telle, mais le délai de l'obligation de conservation a été modulé en fonction de seuils supplémentaires tels que prévus dans les projets de §3, 2e et 3e alinéa, a), b), c). Les défis concrets pour la GPI dans son ensemble et les autorités administratives et judiciaires sont ici entre autres les suivants:
- tout d'abord, le COC se pose la question de savoir s'il est techniquement possible de pouvoir isoler les délits de la liste d'écoute de l'art. 90*ter* C.i.cr. dans la BNG et si cela peut se faire de manière suffisamment précise, ce qui est, *in casu,* une *conditio sine qua non*. On ne peut tirer de la BNG moins, et évidemment pas plus d'enregistrements *'art. 90ter C.i.cr'* qu'il n'y en a effectivement eu. Les rédacteurs de l'avant-projet sont invités à confirmer avec 100% de certitude qu'une telle extraction correcte 'art. 90*ter* C.i.cr.' est possible;

- vient ensuite l'intérêt d'une qualification pénale correcte des faits au niveau de la police sur le vif et donc dès le début des constatations ou l'établissement du procès-verbal initial. Ce n'est un secret pour personne qu'il y avait assez bien de friture sur la ligne en ce qui concerne l'exactitude (permanente) des enregistrements policières. La qualification donnée par le fonctionnaire de police n'est de toute manière qu'une qualification provisoire qui peut entre-autres être modifiée par le parquet au cours de l'enquête. En théorie, il devrait y avoir un feedback de la justice vers la GPI pour lui permettre d'adapter et si nécessaire de rectifier les qualifications. Ce feedback est prévu tant par l'article 646 C.i.cr. que par l'art. 44/5 §6 LFP, et peut éventuellement impliquer une mise à jour des enregistrements de la BNG, mais est en pratique déjà lettre morte depuis des années, bien qu'il s'agisse déjà d'une obligation légale depuis avril 2018. L'Organe de Contrôle insiste déjà depuis des années sur cette problématique, et ceci sans succès. Mais également au niveau de la police proprement dit, le maintien de l'exactitude des enregistrements BNG dans le temps reste tout un défi;
- Il y a aussi la nécessité d'une meilleure formation des fonctionnaires de police qui qualifient pour la première fois les faits tels que repris dans la BNG. Dire que sur ce point, la connaissance juridique du droit pénal par la GPI (à travers tous les cadres) peut être améliorée revient aussi à enfoncer une porte ouverte. Ceci doit aussi aller de pair avec un meilleur contrôle par la hiérarchie et par la gestion fonctionnelle avant que les saisis de base ne soient transmises à la BNG. Dans tous ces domaines, il faut donc absolument des améliorations, indépendamment même de cet avant-projet et arrêté d'exécution. Il s'agit toutefois d'arguments supplémentaires, pour autant que de besoin, pour passer à la vitesse supérieure à propos de ce qui est indiqué ci-dessus;
- Il faut enfin prêter l'attention nécessaire au danger potentiel que des faits punissables risquent à l'avenir d'être trop facilement qualifiés de délits graves selon l'art. 90*ter* C.i.cr puisqu'à l'avenir ils 'compteront' dans le calcul des seuils prévus par le projet d'art. 126/1 LCE. Les mauvaises langues pourraient prétendre que la GPI aurait à l'avenir tout 'intérêt' à qualifier au maximum des faits punissables de 'criminalité grave' et de les saisir ainsi dans la BNG.

Le rôle et la responsabilité de la hiérarchie policière et du Ministère public ne peuvent pas être surestimés quant à cela. Le principe de précision tel que prévu e.a. à l'art. 28, 4° LPD et son respect par tous les membres de la GPI trouve une autre dimension suite à cet avant-projet.

17. Le critère géographique utilisé est l'arrondissement judiciaire. Il n'est toutefois pas exact, comme l'exposé des motifs l'affirme à tort[13], qu'il existe une PJF (Police Judiciaire Fédérale) par arrondissement judiciaire. L'arrondissement judiciaire du Hainaut a deux PJF, celle de Mons et celle de Charleroi. L'arrondissement judiciaire de Bruxelles a également deux PJF (Halle-Vilvorde et Bruxelles). En toute clarté : les statistiques tirées de la BNG concerneront donc Bruxelles et le Hainaut et pas les descriptions des PJF respectives.

[13] Exposé des motifs, avant-projet, p. 49.

En outre, on ne peut pas ignorer que ce sont surtout les grands services de police locale (grandes villes et centres urbains) qui font aussi des enquêtes sur des délits art. 90 C.i.cr.

Plutôt que l'argumentation précitée, le COC est d'avis que la description géographique de l'arrondissement et de la zone de police est rationnelle et logique en fonction de l'organisation étatique, judiciaire et policière.

B.1.2. Intervention de l'Organe de Contrôle

Contrôle des statistiques fournies

18. En ce qui concerne spécifiquement le rôle de la COC, le projet d'article 126/1 § 3, 1° dispose in fine : " *La direction visée à l'article 44/11 de la loi sur la fonction de police transmet chaque année, à la date déterminée par le Roi, ces statistiques à l'Organe de contrôle de l'information policière qui, dans les [quinze] jours après leur réception, vérifie leur exactitude et en informe le service désigné par le Roi.*". Ce "*service désigné par le Roi*" est désigné à l'article 10/1 du projet d'arrêté d'exécution comme ladite *National Technical & Tactical Support Unit* (*NTSU*) des unités spéciales de la police fédérale.

19. Les remarques suivantes s'imposent à ce sujet:

- le délai de 15 jours est encore entre crochets dans les textes communiqués aux autorités de protection des données compétentes, ce qui indique que celui-ci n'est pas encore arrêté d'un point de vue politique. Quoi qu'il en soit, un délai de 15 jours est trop court pour pouvoir fournir un travail sérieux. L'EdM ne donne aucune indication à propos de cet alinéa et donc à propos du délai choisi et dispose uniquement que " *Ces statistiques seront vérifiées et validées par l'Organe de contrôle de l'information policière. Dès que cet Organe aura validé ces statistiques, elles seront transmises à la NTSU (National Technical & Tactical Support Unit) qui indiquera à l'aide d'une carte aux opérateurs quels arrondissements/zones de police sont soumis à la conservation de données ainsi que la durée de conservation.*"[14]. Il n'y a aucune raison de maintenir un délai aussi court pour faire une analyse correcte pour une opération parfaitement planifiable à l'avance pour DRI (à savoir l'établissement de statistiques BNG). Le projet d'article est complexe, avec plusieurs seuils, pour lesquels le COC (qui n'a pas de statisticien à son service) doit avoir le temps de vérifier le processus et l'analyse. Un délai de 1 mois est donc un minimum. Un délai qui ne peut non plus commencer à courir qu'après que le COC soit en possession de toutes les informations pertinentes. Le COC suggère ici de reprendre les termes de l'article 236 §2, 2ième alinéa LPD (cfr. Plus loin, numéro 20, *in fine*).

[14] Exposé des Motifs, avant-projet, p. 52.

- la portée exacte de l'intervention du COC consiste à "***valider***" les statistiques, donc, en d'autres termes à octroyer une autorisation préalable, comme indiqué dans l'EdM. Le COC demande de la clarté à propos de la portée de son intervention et demande à utiliser également ces termes dans le texte de l'article lui-même. En effet, alors qu'on affirme dans l'avant-projet que l'Organe de Contrôle "*vérifie l'exactitude des statistiques*" la question se pose de savoir quel sera la procédure suivie si et aussi longtemps que le COC estime que ces statistiques ne sont pas "*exactes*". Le COC peut-il imposer à la GPI de faire certaines choses, d'apporter des modifications au processus, etc.., dans le but d'avoir plus de certitude à propos de l'exactitude des statistiques? Le COC peut-il donner une validation conditionnelle (de sorte que le *NTSU* et les opérateurs puissent en tout cas poursuivre) avec, p.ex., un délai pour se mettre en règle? Tout ceci n'est pas réglé mais laisse présager que des questions et des problèmes pourront se poser. Le rôle et les compétences du COC doivent donc au moins être précisés.

20. Comme il a été dit, le COC doit être en état non seulement d'apprécier les statistiques en tant que telles, mais aussi et surtout l'ensemble du processus sur base duquel elles ont été tirées. Le COC n'intervient ici en effet **pas** comme autorité de protection des données (les statistiques ne sont en principe pas des données personnelles), mais reçoit ici un rôle et une mission *sui generis*. Cela signifie également que le COC ne pourrait pas exercer ses compétences correctrices (art. 247 LPD), ce qui est problématique. On pourrait trouver de l'inspiration à propos des possibilités d'action du COC dans l'article 281, § 4, de la loi générale du 18 juillet 1977 "*sur les douanes et accises*", telle que modifiée par la loi du 2 mai 2019 "*portant des dispositions diverses en matière de traitement des données des passagers* " et dans les articles relatifs à l'utilisation non visible de caméras dans la LPD (les articles 46/6, 2° et 3° alinéa, 46/10, 2° et 3° alinéa LPD). Il semble encore plus simple de déclarer toutes les compétences du COC applicables dans l'exercice de la mission de validation, ce qui peut être plus amplement commenté dans l'EdM à travers cet avis et plus précisément que le but est que le COC puisse exercer toutes les compétences précitées à l'égard non seulement des données personnelles, mais aussi de toutes les autres informations de police, en ce compris les données statistiques.

Sur base des remarques précédentes, et à la lumière du souhait justifié des rédacteurs de l'avant-projet d'octroyer un rôle de contrôle de *trusted third party* – d'autant plus que les rédacteurs de l'avant-projet semblent (ce n'est pas si clair à la lecture des textes) indiquer que les statistiques précitées ne seront pas nécessairement publiques[15] - sur les statistiques fournies par la police qui

[15] EdM, p. 61: "*Ceci dit, le fait que les catégories de zones géographiques doivent être déterminées de manière précise et objective, n'implique pas que la loi ou l'Arrêté royal identifie très précisément quels sont les lieux répondant à ces catégories. C'est notamment le cas pour le critère relatif aux statistiques. Cette catégorie est précise et objective, mais il est indispensable de disposer de statistiques, qui ne sont pas publiques, à ce sujet, pour déterminer quelles sont concrètement les communes visées.* " (c'est nous qui soulignons). D'un autre côté, le projet d'article 216/1 §3 dernier alinéa dispose que "*La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1er, point 1°*." (c'est nous qui soulignons), ce qui peut difficilement être interprété autrement que d'affirmer que les statistiques seront bel et bien publiques (voir aussi EdM, p. 62, en-dessous).

seront à la base d'un système de rétention orientée des données, le COC demande donc de reformuler comme suit le projet d'article 126/1 §3, 1°, *in fine* LCE:

"*La direction, telle que visée par l'article 44/11 de la loi sur la fonction de police, envoie annuellement, à la date fixée par le Roi, ces statistiques à l'Organe de contrôle des informations de police qui, dans le mois, après que toutes les données nécessaires à cette fin ont été communiquées à l'Organe de Contrôle, les valide et informe le service désigné par le Roi de cette validation. Cette validation peut être liée à des conditions ou peut aller de pair avec un ordre de se mettre en règle dans un délai fixé par le COC. L'Organe de Contrôle peut également, ce faisant, exercer toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, tant à propos de données personnelles qu'à propos de données anonymes".*

Avis sur le rapport d'évaluation

21. L'Organe de Contrôle reçoit un double rôle d'avis:

- d'une part, sur les arrêtés d'exécution prévus dans le projet de §5 de l'art. 126/1. Ce faisant, seul l'arrêté d'exécution relatif aux " *modalités de communication des informations par les autorités compétentes vers le service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er* " semble pertinent, puisque le COC intervient comme *trusted third party* dans la phase de communication de l'information par les autorités compétentes au *NTSU*.
- d'autre part, sur un rapport d'évaluation annuel des ministres compétents qui est adressé à la Chambre des représentants. Ce même rapport d'évaluation est ensuite également envoyé au COC. Pour être complets, il faut se référer dans l'EdM (p. 64, 3° alinéa) aux "*autorités de protection des données compétentes*" et non à "*L'autorité de protection des données*" (seule l'APD, donc), dans le cadre de la fourniture d'avis sur une éventuelle modification d'arrêté d'exécution.

Le COC n'a pas de remarques particulières relatives aux interventions prévues aux §§5 et 6.

B.2. Le projet d'article 42 §2 LFP (article 19 avant-projet)

22. Le nouveau §2 de l'article 42 LFP instaure une possibilité de réquisition pour l'officier de police judiciaire (OPJ) de la Cellule Personnes Disparues de la police fédérale et reprend l'art. 126 §2, 5° LCE existant. Cette modification légale est l'opportunité pour le COC de rectifier une anomalie. Dans la grande majorité des cas, les disparitions inquiétantes ne sont pas ou ne semblent pas être un fait

pénal (suicide, accident, etc. …)[16]. On ne voit donc pas clairement pourquoi la réquisition devrait émaner d'un OPJ puisqu'il n'est souvent pas certain ou pas certain du tout, au moment de la réquisition, qu'il soit question de l'exercice de la fonction de police judiciaire. Le COC demande de rectifier cette anomalie et d'octroyer la compétence de réquisition à "*un fonctionnaire de police*" appartenant à la Cellule des Personnes Disparues de la police fédérale.

Pour être complets, le terme néerlandais "*opvorderen*" doit être remplacé par le terme "*vorderen*" (*requérir*).

a) <u>B.3. projet d'Arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques</u>

23. Le projet d'article 10/1 de l'arrêté d'exécution prévoit que la date ultime à laquelle les autorités compétentes communiquent les informations nécessaires à la *NTSU* est fixée au 5 mai de chaque année. Le COC n'est naturellement pas une "*autorité compétente*", mais doit bien communiquer à la *NTSU* la validation ou non des statistiques conformément à l'art. 126/1 §3, 1°, dernier alinéa LCE. Ceci semble signifier qu'entre le 1er janvier et le 5 mai de chaque année, le COC doit avoir octroyé sa validation, après avoir reçu lui-même au préalable (voir numéro 19) les informations nécessaires de DRI pour pouvoir effectuer cette validation de manière sérieuse. L'avant-projet lui-même n'impose pas de date ultime à laquelle le COC doit faire parvenir ou non sa validation au *NTSU*. Il semble également qu'il s'agisse du 5 mai de chaque année au plus tard, mais ce n'est pas clair.

Le Rapport au Roi dans son ensemble ne parle pas de ce nouvel article.

Le COC insiste pour que la ligne du temps soit fixée de manière correcte, et qu'il soit indiqué quand il est attendu du COC qu'il ait au plus tard transmis la validation au *NTSU*. Ceci doit, en ce qui concerne l'Organe de Contrôle, avoir lieu dans le projet d'article 126/1 §3, 1° dernier alinéa LCE et non dans l'arrêté d'exécution[17], mais bien en sorte qu'une ligne du temps logique soit mise en place.

24. L'Organe de Contrôle constate enfin une absence de règles à propos de l'entrée en vigueur. Le COC ne voit actuellement pas clairement quand la première application des nouvelles règles de validation aura lieu, *a fortiori* quand, au plus tard, la première validation devra être transmise au *NTSU* et/ou quand elle recevra les statistiques de DRI.

---

[16] Voir aussi l'explication dans l'Exposé des Motifs, p. 101, avec un renvoi au législateur en 2016 (Doc. Parl., 54-1567/001, p. 29).

[17] Il ne revient en effet pas au pouvoir exécutif d'imposer des obligations à un organe parlementaire indépendant et à une autorité de protection des données indépendante.

Le COC demande aux rédacteurs de l'avant-projet et de l'arrêté d'exécution de prêter l'attention nécessaire à cette *première* application des nouvelles règles de rétention des données après l'entrée en vigueur des deux textes.

PAR CES MOTIFS,
L'Organe de Contrôle de l'Information Policière,
demande de donner suite à toutes les remarques de cet avis.

Ainsi approuvé par l'Organe de contrôle de l'information policière le 21 mai 2021.

Pour l'Organe de contrôle,
Le Président,
(sé.) Philippe ARNOULD

CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DA210014		21/05/2020

<u>Betreft</u>: Advies betreffende:

a) **een voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie -, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten;**
b) **ontwerp van Koninklijk besluit tot wijziging van het Koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie**

Het Controleorgaan op de politionele informatie (hierna afgekort 'COC' of 'Controleorgaan');

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als 'WGB'), artikel 71 en Titel VII, inzonderheid artikel 236 § 2, 3de lid WGB.
Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG').
Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').
Gelet op de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (hierna 'WGP').
Gelet op de '*Law Enforcement Directive*' 2016/680 van 27 april 2016 (hierna '*LED*').
Gelet op het verzoek van de Vice-eersteminister en minister van Justitie en Noordzee, door het Controleorgaan ontvangen per e-mail op 7 mei 2021 om 20.08 u.
Gelet op de notificatie van de Ministerraad van 7 mei 2021.

Gelet op het verslag van de heer Frank Schuermans, lid-raadsheer in het Controleorgaan.

Brengt op 21 mei 2021 het volgend advies uit.

I. <u>Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan</u>

...

1. In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2] heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid van de WOG bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan.

2. Het Controleorgaan moet geraadpleegd worden bij de voorbereiding van wetgeving of een regelgevende maatregel die verband houdt met de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikel 59 §1, 2e lid en 236 §2 WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie of *LED*). Daarbij heeft het Controleorgaan de opdracht om te onderzoeken of de voorgenomen verwerkingsactiviteit door de politiediensten in overeenstemming is met de bepalingen van Titel 1 (voor de niet-operationele verwerkingen)[3] en Titel 2 (voor de operationele verwerkingen) van de WGB[4]. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan advies uit, hetzij uit eigen beweging, hetzij op verzoek van de Regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid of van een politiedienst, inzake iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer zoals geregeld in Afdeling 12 van Hoofdstuk 4 van de wet op het politieambt[5].

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BELPIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de GBW en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend[6].

---

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming of 'AVG').

[2] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (hierna 'Richtlijn politie-justitie' of *LED*).

[3] Artikel 4 §2, vierde lid WOG.

[4] Artikel 71 §1, derde lid WGB.

[5] Artikelen 59 §1, 2e lid en 236 § 2 WGB.

[6] Artikel 71 §1, derde lid juncto 236 § 3, WGB.

4. Het Controleorgaan is tot slot ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van passagiersgegevens*" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

II. Voorwerp van de aanvraag

5. De aanvrager legt een "*voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie -, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten*" voor (hierna het 'voorontwerp'), waarvan de indieners, naast de aanvrager zelf, de Eerste Minister, de Minister van Financiën, de Minister van Sociale Zaken en Volksgezondheid, de Minister van Telecommunicatie, de Minister van defensie, de Minister van Binnenlandse Zaken en de Staatssecretaris belast met Privacy zijn. Tegelijk wordt een ontwerp van uitvoeringsbesluit tot wijziging van het Koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie voor advies voorgelegd (hierna 'het uitvoeringsbesluit').

6. De aanvrager verzoekt het Controleorgaan om een advies bij hoogdringendheid uit te brengen, met name binnen de door de WGB minimum vastgelegde termijn van 15 dagen[7]. Deze urgentie werd niet als zodanig genotificeerd door de Ministerraad. Het is het COC ook niet duidelijk of de urgentie werd gevraagd in het nota aan de Ministerraad. Het Controleorgaan begrijpt evenwel de urgentie in het licht van de door de aanvrager in zijn begeleidend schrijven van 7 mei 2021 uiteengezette motieven. Gelet evenwel op de korte termijn waarbinnen het advies wordt gevraagd en moet worden geleverd op twee substantiële teksten, beperkt het zich echter tot de meest essentiële opmerkingen.

7. Aangezien het voorontwerp en uitvoeringsbesluit niet uitsluitend en zelfs niet in de eerste plaats over politionele verwerkingen handelt, is het advies beperkt tot die artikelen in beide teksten die in verband staan met de verwerking van de persoonsgegevens door de geïntegreerde politie (GPI) waarvoor het Controleorgaan exclusief bevoegd is.

Voor de andere bepalingen is hetzij de GBA, hetzij het Vast Comité I bevoegd en kan worden verwezen naar de respectievelijke adviezen van beide instellingen.

III. Bespreking van de aanvraag

A. Algemene opmerkingen

[7] Art. 236 § 2, 3de lid WGB.

8. Voor de algemene inhoud en strekking van het voorontwerp en uitvoeringsbesluit verwijst het COC naar de uitgebreide Memorie van Toelichting (hierna 'MvT'). De bedoeling van de steller van de voorgelegde teksten bestaat er in, kort gezegd, een antwoord te formuleren op de vernietiging door het Grondwettelijk Hof, bij arrest nr. 57/2021 van 22 april 2021, van de artikelen 2,b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, waardoor het tot dan geldende systeem van ongedifferentieerde en algemene bewaring van de zgn. 'verkeers- en locatiegegevens' onmogelijk werd gemaakt, één en ander in navolging van de rechtspraak van het Hof van Justitie van de Europese Unie, nader geïdentificeerd en uiteengezet in de MvT. Het antwoord van de steller van het voorontwerp en het uitvoeringsbesluit bestaat in een regeling die een meer 'gerichte' bewaring van voornoemde communicatiegegevens oplegt aan de telecomoperatoren voor doeleinden van.

9. Het leeuwendeel van de wetgeving die wordt gewijzigd en van de verwerkingen die worden beoogd betreffen verwerkingen door autoriteiten of private spelers die niet onder de controlebevoegdheid vallen van het COC. De operatoren, de FSMA[8], het CSIRT[9], enz. … vallen onder de bevoegdheid van de GBA, zodat het COC dienaangaande verwijst naar het door de GBA uit te brengen advies. De inlichtingendiensten vallen onder de bevoegdheid van het Vast Comité I zodat, wat deze aspecten betreft, moet verwezen worden naar het advies van voormeld Comité.

10. Het COC beperkt in dit advies zijn onderzoek tot die artikelen die rechtstreeks of onrechtstreeks betrekking hebben op de politionele verwerkingen van persoonsgegevens die in het voorontwerp en uitvoeringsbesluit werden opgenomen of die rechtstreeks of onrechtstreeks een invloed (kunnen) hebben op het functioneren van de geïntegreerde politie in het ruimere kader van de politionele informatiehuishouding.

11. Het Controleorgaan krijgt in dit ontwerp een belangrijke nieuwe bevoegdheid die in rechtstreeks verband staat met het thema van de dataretentie en het gebruik ervan in het kader van de gerechtelijke politiefunctie. Het COC wordt belast met een vorm van *a priori* controle op de door de GPI, en meer bepaald de directie van de politionele informatie en de ICT middelen van de federale politie (hierna 'DRI'), geproduceerde statistieken afkomstig van de Algemene Nationale Gegevensbank (hierna 'ANG') bedoeld in art. 44/7 WPA en vervat in het ontworpen artikel 126/1 van de Wet van 13 juni 2015 betreffende de elektronische communicatie (hierna 'WEC').

12. Het COC beschouwt de haar nieuwe toevertrouwde opdrachten als een vorm van erkenning en waardering voor het vele werk dat het op zeer korte termijn, en meer bepaald sinds de doorstart op 5 september 2018 (datum van inwerkingtreding van de WGB) als onder meer de dataprotectie autoriteit van de GPI, heeft neergezet. De toekenning van nieuwe bevoegdheden vormt een continuüm gekenmerkt door de over de jaren heen bijkomende opdrachten die aan het Controleorgaan werden

[8] *Financial Services and Market Authority* (Autoriteit voor Financiële Diensten en Markten).

[9] *Computer Security Incident Response Team*.

en worden toevertrouwd. De door de steller van het voorontwerp genomen optie sluit ook aan bij de visie van het Grondwettelijk Hof die reeds in twee arresten de fundamentele rol van het Controleorgaan in de verf heeft gezet. Er kan inderdaad verwezen worden naar de arresten 108/2016 van 14 juli 2016 en 27/2020 van 20 februari 2020 waarin de rol van het COC, onder meer op het vlak van de bescherming van het grondrecht op privacy en gegevensbescherming in het licht van de politionele gegevensverwerkingen, op diverse plaatsten in de verf werd gezet.

13. Het spreekt evenwel voor zich dat er limieten zijn aan de beperkte capaciteit van het COC – er kan verwezen worden naar het jaarverslag 2016-2019[10] en 2020[11] van het COC - waar één en ander wordt uiteengezet en de organisatie wordt toegelicht - zodat er ook aandacht zal dienen te gaan, zowel naar het verlenen van afdoende budgettaire als naar personeelsmatige middelen.

Eén en ander overigens op een ogenblik dat terzelfder tijd enerzijds één van de indieners van dit voorontwerp en uitvoeringsbesluit, met name de Staatssecretaris voor Privacy, volop bezig is met de evaluatie van de WGB op grond van artikel 286 WGB (aan wie het COC op diens verzoek een uitgebreide nota en advies heeft overgemaakt, waarin de krachtlijnen zijn opgenomen van de wijzigingen en verbeteringen die aan de WGB zouden kunnen aangebracht te worden) en anderzijds de Kamer van Volksvertegenwoordigers dat van zijn kant, in het kader van een audit van het Rekenhof (die aan aanvang nam in 2018 met een opvolging in 2020), aandringt op tastbare resultaten op het vlak van synergiën en *clustering* van bevoegdheden of zelfs *clustering* van dotatiegerechtigde instellingen[12], met alle mogelijke gevolgen voor de werking van het Controleorgaan.

Beide lopende projecten komen bovenop de vele reactieve en proactieve dossiers die het COC reeds te behandelen heeft waarbij de burger en de GPI de weg naar het Controleorgaan steeds meer vinden. Het Controleorgaan vraagt de beleidsmakers hiervoor de nodige aandacht te hebben.

14. De steller van het voorontwerp wordt er tot slot op gewezen dat een revisie van de Nederlandstalige versie van de teksten nog noodzakelijk is. Dit geldt zowel voor het corpus van de teksten als voor de Memorie van Toelichting en het Verslag aan de Koning. In het corpus dient bv. het ontworpen art. 126/1 WEC op zijn Nederlandstalige versie herzien te worden ("*pour ce qui concerne*" wordt bv. verkeerdelijk vertaald door "*voor*"). Zo bv. wordt in de MvT in de Franstalige versie, m.b.t. het geografisch criterium, gesproken van "*… arrondissement par arrondissement, ou zones de police par zones de police …*" (p. 8), terwijl de Nederlandstalige tekst het heeft over "*… wijk voor wijk of politiezone voor politiezone …*". Een wijk is geen arrondissement en omgekeerd. "*… à charge de X "* wordt verkeerdelijk vertaald als "*onder de verantwoordelijkheid van x …"* (p. 10); "*arrondissement*" wordt vertaald als "*district*" (p. 48), "*les opérateurs qui doivent effectuer les réquisitions* » wordt vertaald als « *de operatoren die de opvordering moeten doen*" (p. 62), enz. …

[10] Zie, www.controleorgaan.be, https://www.controleorgaan.be/files/Activiteiten-verslag_COC_2016-2019_NL.pdf

[11] Zie www.controleorgaan.be, te verschijnen uiterlijk eind mei 2021.

[12] Zie, Kamer, stuk CRIV 55 plen 100, dd. 29.04.2021, p. 41 en 42; DOC 55, 1924/001, p. 1-43, www.dekamer.be, https://www.dekamer.be/FLWB/PDF/55/1924/55K1924001.pdf

B. Artikelsgewijze opmerkingen

B.1. Ontworpen artikel 126/1 WEC (art. 8 voorontwerp)

B.1.1. Algemeen

15. Het voor het Controleorgaan belangrijke ontwerp artikel 126/1 WEC voorziet een systeem van gedifferentieerde bewaring op grond van geografische zones. Deze zijn hetzij gerechtelijke arrondissementen in de gevallen dat er sprake is van minstens 3 strafbare feiten ex. art. 90ter Sv. (hierna verder ook 'zware misdrijven' genoemd) per 1.000 inwoners/jaar over een gemiddelde van de 3 voorbije kalenderjaren, hetzij politiezones die deel uitmaken van voornoemde gerechtelijke arrondissementen waar evenwel minder dan 3 zware misdrijven per 1.000 inwoners/jaar zijn vastgesteld over een gemiddelde van de 3 voorbije kalenderjaren. In de MvT wordt voor een aantal arrondissementen uiteengezet over hoeveel zware misdrijven gemiddeld per jaar dit *in concreto* moet gaan.

Het COC heeft hier geen bijzondere opmerkingen en begrijpt dat de stellers van het voorontwerp zo maximaal mogelijk hebben gezocht naar objectieve criteria in lijn met voormelde rechtspraak van het EU Hof van Justitie. Dat daarbij getracht is ook praktisch haalbare criteria in te voeren ligt voor de hand. De territoriale omschrijvingen van de gerechtelijke arrondissementen en politiezones zijn gekende omschrijvingen waarmee men snel aan de slag kan. De zgn. 'taplijst' van art. 90*ter* Sv. is de *lege lata* naar Belgische recht het enige echt bruikbare criterium om zgn. 'zware misdrijven' te kunnen onderscheiden van 'gewone criminaliteit'.

16. De uitdaging zal, ook wat de controle door het COC betreft, liggen in de praktische toepassing ervan, nu de correctheid, nauwkeurigheid en juistheid van de ANG registraties een bijkomende dimensie en belang krijgen. Dit fundamenteel principe van gegevensbeschermingsrecht, dat al essentieel is, wordt immers nog belangrijker. Niet alleen hangt thans de bewaarplicht van verkeers – en locatiegegevens op zich ervan af, maar ook de termijn van de bewaarplicht werd afhankelijk gemaakt van bijkomende drempels zoals voorzien in de ontworpen §3, 2e en 3e lid, a), b), c). De concrete uitdagingen waarvoor de hele GPI en de bestuurlijke en gerechtelijke overheden staan zijn in deze onder meer de volgende:
- vooreerst stelt het COC zich de vraag of het actueel technisch mogelijk is om de taplijstmisdrijven van art. 90*ter* Sv. te kunnen isoleren in de ANG en of dat accuraat genoeg kan gebeuren wat *in casu* een *conditio sine qua non* is. Uit de ANG mogen niet minder, maar evident ook niet meer 'art. 90*ter* Sv.' registraties gehaald worden dan er effectief geweest zijn. De stellers van het voorontwerp worden uitgenodigd te bevestigen dat met 100% zekerheid dergelijke correcte 'art. 90*ter* Sv. extractie mogelijk is;

- vervolgens komt ook hier het belang van een correcte strafrechtelijke kwalificatie van de feiten op politioneel niveau op de proppen en dus bij de aanvang van de vaststellingen of de opmaak van het aanvankelijk proces-verbaal. Het is een publiek geheim dat er nogal wat ruis op de lijn zit wat de (blijvende) correctheid van de politionele registraties betreft. De door de politieambtenaar verleende kwalificatie is sowieso altijd maar een voorlopige kwalificatie die onder meer door het parket in de loop van het onderzoek kan worden en ook wordt gewijzigd. In theorie zou er daarnaast een feedback moeten zijn vanuit justitie naar de GPI om deze toe te laten de kwalificaties zo nodig aan te passen en te rectificeren. Deze feedback voorzien zowel door artikel 646 Sv. als door art. 44/5 §6 WPA, die een eventuele bijwerking van de ANG registraties met zich kan of moet brengen, is in de praktijk al jaren en nog steeds dode letter, hoewel reeds een wettelijke verplichting sedert april 2018. Het Controleorgaan hamert al enkele jaren op deze problematiek en dit manco. Maar ook op louter politioneel niveau is het in de tijd nauwkeurig houden van de ANG vattingen een hele uitdaging;
- Daarnaast is er de noodzaak van een betere opleiding van de politieambtenaren die de feiten zoals opgenomen in de ANG voor het eerst kwalificeren. Dat er ook op het vlak van de juridische kennis van het strafrecht bij de GPI (over alle kaders heen) veel ruimte voor verbetering is, is evenzeer een open deur intrappen. Dat moet ook gepaard gaan met een betere controle door de hiërarchie en door het functioneel beheer vooraleer de basisvattingen door te sturen naar de ANG. Op al deze domeinen dient er dus absoluut vooruitgang geboekt te worden, overigens zelfs los van dit voorontwerp en uitvoeringsbesluit. Deze laatsten zijn evenwel bijkomende argumenten, voor zoveel als nodig, om van wat hoger werd gesteld nu echt werk te maken en een versnelling hoger te schakelen;
- Tot slot dient de nodige aandacht te worden geschonken aan een potentieel gevaar dat strafbare feiten in de toekomst te gemakkelijk als zware misdrijven ex. art. 90*ter* Sv. riskeren gekwalificeerd te worden vermits zij nu in de toekomst zullen 'meetellen' bij de berekening van de drempels voorzien in het ontworpen art. 126/1 WEC. Kwade tongen zouden kunnen beweren dat de GPI er in de toekomst alle 'belang' bij heeft strafbare feiten maximaal als 'zware criminaliteit' te kwalificeren en als dusdanig te vatten in de ANG.

De rol en verantwoordelijkheid van de politiehiërarchie en het Openbaar Ministerie kan hier nauwelijks overschat worden. Het nauwkeurigheidsbeginsel zoals o.a. vervat in art. 28, 4° WGB en de naleving ervan door alle leden van de GPI krijgt met dit voorontwerp een bijkomende dimensie.

17. Het gehanteerde geografisch criterium is het gerechtelijke arrondissement. Het is evenwel niet zo, zoals de toelichting ten onrechte stelt[13], dat er één FGP (Federale Gerechtelijke Politie) per gerechtelijk arrondissement is. Het gerechtelijk arrondissement Henegouwen heeft twee FGP's, die van Bergen en die van Charleroi. Het gerechtelijk arrondissement Brussel heeft evenzeer twee FGP's (Halle-Vilvoorde en Brussel). Voor alle duidelijkheid: de statistieken die uit de ANG worden getrokken zullen dus het arrondissement Brussel en Henegouwen betreffen en niet de omschrijvingen van de

[13] Memorie van Toelichting, voorontwerp, p. 49.

respectievelijke FGP's. Daarnaast kan niet ontkend worden dat vooral ook grote lokale politiediensten (grootsteden en centrumsteden) evenzeer onderzoeken doen naar art. 90*ter* Sv. misdrijven.

Eerder dan voormelde argumentatie is het COC van oordeel dat de geografische omschrijving van het arrondissement en de politiezone rationeel en logisch is in functie van de gekende staatkundige, gerechtelijke en politionele organisatie.

B.1.2. Tussenkomst van het Controleorgaan

Controle van de aangeleverde statistieken

18. Wat nu specifiek de rol van het COC betreft stelt het ontworpen artikel 126/1 §3, 1° in fine: "*De directie, zoals bedoeld in artikel 44/11 van de wet op het politieambt, zendt jaarlijks op de door de Koning vastgestelde datum deze statistieken toe aan het Controleorgaan op de politionele informatie dat, binnen de [vijftien] dagen na ontvangst, de juistheid ervan controleert en de door de Koning aangewezen dienst ervan in kennis stelt*". Deze "*door de Koning aangewezen dienst*" wordt in artikel 10/1 van het ontwerp van uitvoeringsbesluit aangeduid en is de zgn. *National Technical & Tactical Support Unit* (*NTSU*) van de speciale eenheden van de federale politie.

19. De volgende opmerkingen dringen zich ter zake op:

- de termijn van 15 dagen staat nog tussen haakjes in de aan de bevoegde gegevensbeschermingsautoriteiten meegedeelde teksten, wat erop wijst dat deze niet beleidsmatig lijkt te zijn afgeklopt. Hoe dan ook is een termijn van 15 dagen te kort om ernstig werk te kunnen leveren. De MvT geeft bij dit lid en dus ook niet bij de gekozen termijn enige duiding en stelt enkel dat "*deze statistieken gecontroleerd (zullen worden) door het Controleorgaan op de politionele informatie. Zodra deze instantie deze statistieken heeft gevalideerd, zullen zij worden toegezonden aan de NTSU (National Technical & Tactical Support Unit)), die de operatoren door middel van een kaart zal aangeven voor welke gemeenten/politiezones gegevens worden bewaard en voor hoe lang*"[14]. Er is geen enkele reden om die termijn zo kort te houden om een gedegen analyse te maken op een voor DRI op voorhand perfect planbare operatie (met name het opmaken van de ANG statistieken). Het ontworpen artikel is complex, met meerdere drempels, waarbij het COC (die geen statisticus in huis heeft) de tijd moet krijgen om het proces en de analyse te doorgronden. Een termijn van 1 maand is dan ook het minimum. Een termijn die ook maar kan beginnen lopen nadat het COC in het bezit is gesteld van alle relevant informatie. Het COC suggereert hier de bewoordingen van art. 236 §2, 2e lid WGB over te nemen (cf. verder onder randnummer 20, *in fine*).

[14] Memorie van Toelichting, voorontwerp, p. 52.

- de exacte draagwijdte van de tussenkomst van het COC bestaat erin de statistieken te "***valideren***", dus m.a.w. een voorafgaande machtiging te verlenen, zoals in de MvT wordt gesteld. Het COC verkiest helderheid omtrent de draagwijdte van zijn tussenkomst en verzoekt dan ook deze bewoordingen te gebruiken in de tekst van het artikel zelf. Waar immers wordt gesteld in het voorontwerp dat het Controleorgaan "*de juistheid van de statistieken controleert*" is maar de vraag hoe het proces verloopt wanneer en tot zolang het COC van oordeel is dat de statistieken niet "*juist*" zijn. Kan het COC de GPI opleggen bepaalde zaken te doen, wijzigingen aan het proces aan te brengen, e.d.m., met de bedoeling meer zekerheid te bereiken omtrent de correctheid van de statistieken. Kan het COC een voorwaardelijke validatie geven (zodat *NTSU* en de operatoren alvast verder kunnen) met bv. een termijn om zich in regel te stellen? Dit alles wordt niet geregeld waar het zich laat voorspellen dat die vragen en problemen zich kunnen stellen. De rol en bevoegdheden van het COC moeten dus minimaal verduidelijkt worden.

20. Zoals gezegd moet het COC in staat worden gesteld niet enkel de statistieken op zich te beoordelen maar ook en wel vooral het hele proces op grond waarvan ze werden getrokken. Het COC treedt hier immers **niet** meer op als dataprotectie autoriteit (statistieken zijn in beginsel geen persoonsgegevens) maar bekomt hier een *sui generis* rol en opdracht. Dat betekent ook dat het COC zijn corrigerende bevoegdheden (art. 247 WGB) niet zou kunnen uitoefenen wat problematisch is. Inspiratie m.b.t. de actiemogelijkheden van het COC kan mogelijks gevonden worden in artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van passagiersgegevens*" en in de artikelen rond het niet zichtbaar cameragebruik in de WPA (de artikelen 46/6, 2e en 3e lid, 46/10, 2e en 3e lid WPA). Nog eenvoudiger lijkt het alle bevoegdheden van het COC van toepassing te verklaringen bij de uitoefening van de opdracht van validering wat nader kan toegelicht worden in de MvT aan de hand van dit advies en meer bepaald dat het de bedoeling is het COC alle voormelde bevoegdheden te laten uitoefenen ten aanzien van niet alleen persoonsgegevens, maar ook alle andere politionele informatie, waaronder statistische gegevens.

Op grond van voorgaande opmerkingen en in het licht van de terechte wens van de stellers van het voorontwerp om een *trusted third party* een controlerol toe te bedelen – te meer daar de stellers van het voorontwerp lijken (het is bij lezing van de teksten niet zo éénduidig) aan te geven dat voormelde statistieken niet noodzakelijk openbaar zullen zijn[15] - op de door de politie aangeleverde statistieken

[15] MvT, p. 61: "*Dat de categorieën van geografische gebieden op precieze en objectieve wijze moeten worden vastgesteld, impliceert evenwel niet dat de wet of het koninklijk besluit zeer nauwkeurig vaststelt welke plaatsen onder deze verschillende categorieën vallen. Dit is met name het geval voor het criterium inzake statistieken. Deze categorie is nauwkeurig en objectief, maar het is van essentieel belang over statistieken te beschikken, die niet noodzakelijk openbaar zijn, om te kunnen bepalen welke gemeenten daadwerkelijk onder de regeling vallen*" (eigen onderlijning). Langs de andere kant bepaalt het ontworpen artikel 216/1 §3 laatste lid dat "*De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°*" (eigen onderlijning), wat moeilijk anders kan geïnterpreteerd worden dan dat de statistieken wel degelijk publieke zullen zijn (zie ook MvT, p. 62, onderaan).

die de basis zullen vormen voor een systeem van gerichte dataretentie verzoekt het COC dan ook voormeld ontworpen artikel 126/1 §3, 1°, *in fine* WEC als volgt te herformuleren:

"*De directie, zoals bedoeld in artikel 44/11 van de wet op het politieambt, zendt jaarlijks, op de door de Koning vastgestelde datum, deze statistieken toe aan het Controleorgaan op de politionele informatie dat, binnen de maand, nadat alle daartoe noodzakelijke gegevens aan het Controleorgaan zijn meegedeeld, deze valideert en de door de Koning aangewezen dienst van deze validatie in kennis stelt. Deze validatie kan aan voorwaarden worden gekoppeld of kan gepaard gaan met een bevel zich in regel te stellen binnen een door het COC bepaalde termijn. Het Controleorgaan kan hierbij eveneens alle haar bij titel 7 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens toegekende bevoegdheden uitoefenen, zowel inzake persoonsgegevens als anonieme gegevens".*

Advies op het evaluatierapport

21. Het Controleorgaan bekomt ook een dubbele adviesrol:

- enerzijds op de uitvoeringsbesluiten voorzien in de ontworpen §5 van art. 126/1. Hierbij lijkt voor het COC enkel het uitvoeringsbesluit betreffende "*de procedures voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de procedures voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen*" relevant, vermits het COC als *trusted third party* tussenkomst in fase van de mededeling van informatie door de bevoegde autoriteiten aan *NTSU*.
- anderzijds op een jaarlijks evaluatieverslag van de bevoegde ministers dat aan de Kamer van volksvertegenwoordigers wordt uitgebracht. Datzelfde evaluatieverslag wordt naderhand ook naar het COC gestuurd. Volledigheidshalve dient in de MvT (p. 64, 3e lid) te worden verwezen naar de "*bevoegde gegevensbeschermingsautoriteiten*" en niet naar "*de Gegevensbeschermingsautoriteit*" (enkel de GBA dus) in kader van de adviesverlening op een eventueel gewijzigd uitvoeringsbesluit.

Het COC heeft geen bijzondere opmerkingen betreffende zijn in §§5 en 6 voorziene tussenkomsten.

B.2. Ontworpen 42 §2 WPA (artikel 19 voorontwerp)

22. De nieuwe §2 van artikel 42 WPA voert een vorderingsmogelijkheid in voor de officier van gerechtelijke politie (OGP) van de Cel Vermiste Personen van de federale politie en is de overname van het bestaande art. 126 §2, 5° WEC. Deze wetswijziging is voor het COC de gelegenheid om een anomalie recht te zetten. In de overgrote meerderheid van de gevallen zijn of blijken onrustwekkende

verdwijningen geen strafbaar feit te zijn (zelfdoding, ongeval, enz. …)[16]. Het is dan ook onduidelijk waarom de vordering zou moeten uitgaan van een OGP vermits er veelal niet en al zeker niet op het moment van de vordering sprake is van de uitoefening van de gerechtelijke politiefunctie. Het COC verzoekt deze anomalie recht te zetten en de vorderingsbevoegdheid te verlenen aan "*een politieambtenaar*" behorende tot de Cel Vermiste Personen van de federale politie.

Volledigheidshalve dient in het Nederlands ook de term "*opvorderen*" vervangen te worden door "*vorderen*" (*requérir*).

B.3. ontwerp van Koninklijk besluit tot wijziging van het Koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie

23. Het ontworpen artikel 10/1 van het uitvoeringsbesluit voorziet dat de uiterste datum waarop de bevoegde autoriteiten aan de *NTSU* de vereiste informatie meedelen wordt vastgesteld op 5 mei van elk jaar. Het COC is uiteraard geen "*bevoegde autoriteit*" maar moet wel de al dan niet validering van de statistieken conform het ontworpen art. 126/1 §3, 1°, laatste lid WEC meedelen aan *NTSU*. Dit lijkt te betekenen dat tussen 1 januari en 5 mei van elk jaar het COC zijn validatie moet hebben verleend, nadat het zelf op voorhand tijdig (zie randnummer 19) de noodzakelijke gegevens van DRI moet hebben ontvangen om die validatie op een ernstige manier te kunnen doen. Het voorontwerp zelf legt geen uiterste datum vast waarop het COC zijn al dan niet validatie aan *NTSU* moet laten geworden. Het lijkt erop dat dit evenzeer uiterlijk op 5 mei van elk jaar ligt, maar helder is het niet.

Het Verslag aan de Koning bespreekt dit nieuwe artikel in het geheel niet.

Het COC dringt erop aan op een behoorlijke manier de tijdslijn vast te leggen waaruit blijkt wanneer van het COC verwacht wordt de validatie aan *NTSU* uiterlijk te hebben overgemaakt. Dat dient, wat het Controleorgaan betreft, te gebeuren in het ontworpen artikel 126/1 §3, 1°, laatste lid WEC en niet in het uitvoeringsbesluit[17], maar wel zodanig dat er een logische tijdslijn wordt gecreëerd.

24. Het Controleorgaan stelt tot slot een gebrek aan regels rond de inwerkingtreding vast. Het is voor het COC alvast op dit ogenblik niet helder wanneer de eerste toepassing van de nieuwe dataretentie regels zal plaatsvinden, *a fortiori* wanneer het uiterlijk de eerste validatie zal dienen over te maken aan *NTSU* en/of wanneer het de statistieken zal aangeleverd krijgen van DRI.

[16] Zie ook de uiteenzetting in de Memorie van Toelichting, p. 101 met verwijzing naar de wetgever in 2016 (Parl. St., 54-1567/001, p. 29).

[17] Het komt immers niet aan de uitvoerende macht toe verplichtingen op te leggen aan een onafhankelijk parlementair orgaan en onafhankelijke dataprotectie autoriteit.

Het COC verzoekt de stellers van het voorontwerp en uitvoeringsbesluit de nodige aandacht te hebben voor deze *primo* toepassing van de hernieuwde dataretentie regels na inwerkingtreding van de beide teksten.

OM DEZE REDENEN,

Het Controleorgaan op de Politionele Informatie,

verzoekt gevolg te geven aan alle opmerkingen van dit advies.

Aldus goedgekeurd door het Controleorgaan op de Politionele Informatie op 21 mei 2021.

Voor het Controleorgaan,
De Voorzitter,
(get.) Philippe ARNOULD

Comité Permanent de Contrôle
des services de renseignements et de sécurité
Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

AVIS n° 003/CPR/2021 DU 15 juin 2021

RÉTENTION DES DONNÉES

Vu le courrier du 7 mai 2021 dans lequel le ministre de la Justice introduit une demande d'avis concernant l'avant-projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités' (ci-après : le projet de loi) ;

Compétence Comité permanent R

Vu l'article 33, alinéa 8 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace ;

Vu les articles 73 et 95 de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données.

Avis du Comité permanent R

NORME JURIDIQUE À MODIFIER

1. Le projet de loi modifie différentes lois. Dans son avis, le Comité permanent R se concentre sur les modifications de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après : la Loi relative aux services de renseignement, en abrégé : L.R&S), ainsi que sur les modifications de la Loi du 13 juin 2005 relative aux

ADVIES nr. 003/VCI/2021 VAN 15 juni 2021

DATARETENTIE

Gelet op het schrijven dd. 7 mei 2021 waarbij de Minister van Justitie bij het Vast Comité I een adviesaanvraag indient met betrekking tot het voorontwerp van wet 'betreffende het verzamelen en het bewaren van de identificatie-, verkeer- en localisatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten' (hierna: het wetsontwerp);

Bevoegdheid Vast Comité I

Gelet op artikel 33, achtste lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

Gelet op de artikelen 73 en 95 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

Gelet op het Samenwerkingsprotocol tussen de Belgische federale toezichthoudende autoriteiten op het vlak van dataprotectie.

Advies van het Vast Comité I

TE WIJZIGEN RECHTSNORM

1. Het wetsontwerp wijzigt diverse wetten. Het Vast Comité I richt zijn advies op de wijzigingen aan de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna: de Inlichtingenwet; afgekort: W.I&V), alsook op de wijzigingen aan de Wet van 13 juni 2005 betreffende de elektronische communicatie

communications électroniques (ci-après : la Loi Télécom, en abrégé : LCE), là où le présent projet de loi vise à définir de nouvelles tâches et de nouvelles compétences pour le Comité. Conformément à sa mission légale, le Comité se concentre sur la conformité et le respect des modifications législatives proposées par le gouvernement avec les normes juridiques supérieures, ainsi que sur l'efficacité de ces modifications.

2. Le Comité ne se prononce pas quant à la question de savoir si les modifications apportées à la Loi Télécom par le projet rencontrent ou pas les exigences consacrées dans les jurisprudences de la Cour de justice et de la Cour constitutionnelle belge. Le Comité se limite dans ce contexte à l'exercice de sa compétence en tant qu'autorité compétente en matière de protection des données (DPA) dans le domaine de la 'sécurité nationale'[1].[2]

(hierna: de Telecomwet; afgekort: WEC) daar waar voorliggend wetsontwerp nieuwe taken en bevoegdheden beoogt in te stellen voor het Comité. Indachtig zijn wettelijke opdracht richt het Comité zich hierbij zowel op de naleving en het respect van de door de regering voorgestelde wetswijzigingen met de hogere rechtsnormen alsook op de doelmatigheid ervan.

2. Het Comité spreekt zich niet uit over de vraag of de door het wetsontwerp in de Telecomwet aangebrachte wijzigingen al dan niet voldoen aan de vereisten van de rechtspraak van het Hof van Justitie en het Belgische Grondwettelijk Hof. Het Comité beperkt zich in deze tot de uitoefening van zijn bevoegdheid als bevoegde gegevensbeschermingsautoriteit (DPA) binnen het 'nationale veiligheid'-domein[3].[4]

A. Modifications à la Loi relative aux services de renseignement

INSERTION DU CONCEPT DE « SÉCURITÉ NATIONALE »

3. Les articles 21 et 22 du projet de loi modifient les articles 7 et 11 L.R&S en ajoutant les mots *« chargée de la sécurité nationale »* à la phrase introductive des dernières dispositions législatives citées. Le Comité comprend et approuve l'objectif de cet ajout, mais souhaite faire remarquer que dans sa formulation actuelle, il n'y a pas de lien immédiat avec les missions de renseignement et de sécurité énumérées dans ces dispositions. Le Comité recommande donc de remplacer les mots *« chargée de la sécurité nationale »* par les mots *« pour la sauvegarde*

A. Wijzigingen aan de Inlichtingenwet

INVOEGING BEGRIP "NATIONALE VEILIGHEID"

3. De artikelen 21 en 22 van het wetsontwerp wijzigen de artikelen 7 en 11 W.I&V door de woorden "*belast met de nationale veiligheid*" toe te voegen aan de inleidende zin van laatstgenoemde wetsbepalingen. Het Comité begrijpt en onderschrijft het doel van deze toevoeging, maar wenst wel op te merken dat in de actuele bewoording van deze toevoeging er geen onmiddellijk verband is met de in deze bepalingen opgesomde inlichtingen- en veiligheidsopdrachten. Het Comité beveelt daarom aan om de woorden "*belast met de nationale veiligheid*" te vervangen door de

[1] Les articles 95, 107 *i.o.* 128 et 185 LPD, et l'article 71 LPD *i.o.* articles 44/11/3*bis* à 44/11/3*quinquies*/2 LFP.

[2] Voir également : le Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données 'Accord entre l'Autorité de protection des données (APD), l'Organe de contrôle de l'information policière (C.O.C.), le Comité permanent de Contrôle des services de renseignement et de sécurité (CPR) et le Comité permanent de Contrôle des services de police (CPP)'.

[3] De artikelen 95, 107 *i.o.* 128, 184 en 185 GBW, en artikel 71 GBW *i.o.* artikelen 44/11/3bis tot 44/11/3quinquies/2 WPA.

[4] Zie eveneens: het Samenwerkingsprotocol tussen de Belgische federale toezichthoudende autoriteiten op het vlak van dataprotectie 'overeenkomst tussen de Gegevensbeschermingsautoriteit (GBA), het Controleorgaan op de politionele informatie (COC), het Vast Comité van Toezicht op de inlichtingendiensten (VCI) en het Vast Comité van Toezicht op de politiediensten (VCP)'.

de la sécurité nationale ».[5] Cette formulation permet de préciser que l'exécution des missions de renseignement et de sécurité énumérées aux articles 7 et 11 L.R&S sert à sauvegarder la sécurité nationale. Elle précise que la finalité des activités des deux services de renseignement s'inscrit dans le cadre des préoccupations en matière de gestion nationale de la sécurité. Cependant, la phrase proposée *« chargée de la sécurité nationale »* laisse trop de place au doute quant à l'existence éventuelle d'autres tâches de sécurité nationale pour la VSSE et le SGRS en dehors de celles énumérées dans (ou basées sur) les articles 7 et 11 L.R&S. Ce n'est absolument pas le cas.

Enfin, le Comité estime que le dispositif nécessite une adaptation. Une simple précision dans l'exposé des motifs est insuffisante.

4. Le fait que cet ajout ne puisse en aucun cas donner lieu à une extension des compétences est significatif, entre autres, pour la portée correcte du nouvel article 18/17/1 L.R&S à insérer (conservation généralisée et indifférenciée des données de trafic et de localisation ; *infra*).

CONSERVATION CIBLÉE DES DONNÉES DE TRAFIC ET DE LOCALISATION

5. À l'article 24 du projet de loi, le gouvernement propose d'inclure dans la Loi relative aux services de renseignement une nouvelle méthode ordinaire de conservation ciblée des données de trafic et de localisation dans le secteur des communications électroniques. Plus précisément, le projet d'article 16/2/1, alinéa 1er L.R&S prévoit que « *(l)es services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur pour procéder à la conservation des :*

woorden *"ter vrijwaring van de nationale veiligheid"*.[6] Via deze schrijfwijze wordt namelijk beter verduidelijkt dat de uitvoering van de in de artikelen 7 en 11 W.I&V opgesomde inlichtingen- en veiligheidsopdrachten de vrijwaring van de nationale veiligheid dient. Het verduidelijkt dat de finaliteit van de werkzaamheden van de beide inlichtingendiensten kadert binnen de nationale veiligheidszorg. De voorgestelde zinsnede "*belast met de nationale veiligheid"* laat echter te veel ruimte open als zouden er nog andere taken van nationale veiligheid in hoofde van de VSSE en de ADIV bestaan andere dan deze opgesomd in of gegrond op de artikelen 7 en 11 W.I&V. Dit is geenszins het geval.
Het Comité is tot slot van oordeel dat een aanpassing zich opdringt in het dispositief. Een loutere verduidelijking in de memorie van toelichting is onvoldoende.

4. Dat de toevoeging geenszins een bevoegdheidsuitbreiding ten gevolge mag hebben, is onder meer betekenisvol voor de juiste reikwijdte van het nieuw in te voegen artikel 18/17/1 W.I&V (algemene en ongedifferentieerde bewaring van verkeers- en lokalisatiegegevens; *infra*).

GERICHTE BEWARING VAN VERKEERS- EN LOKALISATIEGEGEVENS

5. De regering stelt in artikel 24 van het wetsontwerp voor om in het kader van het gericht bewaren van verkeers- en lokalisatiegegevens in de sector van de elektronische communicatie een nieuwe gewone methode in de Inlichtingenwet in te schrijven. Meer in het bijzonder bepaalt het ontworpen artikel 16/2/1, eerste lid W.I&V dat *"(d)e inlichtingen- en veiligheidsdiensten (…), in het belang van de uitoefening van hun opdrachten, de medewerking (kunnen) vorderen van een operator voor het bewaren van :*

[5] D'un point de vue grammatical, la conséquence d'une telle modification est que, contrairement au projet de disposition actuel, une telle partie de phrase doit figurer après le verbe dans la phrase introductive des articles 7 et 11 L.R&S.

[6] Grammaticaal gezien, heeft een dergelijke wijziging ten gevolge dat dergelijke zinsnede, in tegenstelling tot huidige ontwerp bepaling, na het werkwoord in de inleidende zin van de artikelen 7 en 11 W.I&V dient te komen.

1° données de trafic et de localisation de moyens de communications électroniques conservées au moment de la réquisition et qui font l'objet de celle-ci ;

2° données de trafic et de localisation qu'il génère et traite et qui font l'objet de la réquisition. ». [7]

Niveau de protection juridique : pas de contrôle judiciaire

6. Le Comité constate que le projet de loi ne prévoit pas le même niveau de protection juridique pour la compétence figurant dans le projet d'article 16/2/1 L.R&S que pour la compétence figurant dans le projet d'article 39*quinquies* CIC. Les deux dispositions concernent pourtant la même compétence. Le Comité considère qu'il n'y a pas de justification objective à ce que les citoyens soient moins protégés dans la procédure d'information que dans la procédure pénale.

7. Une comparaison entre les deux dispositions légales montre qu'il existe une grande divergence entre les mentions obligatoires dans la décision du dirigeant du service imposées dans le projet d'article 16/2/1 L.R&S et celles imposées dans le projet d'article 39*quinquies* CIC. Du reste, les

1° de verkeers- en lokalisatiegegevens van de elektronische communicatiemiddelen die op het ogenblik van de vordering worden bewaard en die het voorwerp uitmaken van de vordering;

2° de verkeers- en lokalisatiegegevens die hij genereert en verwerkt en die het voorwerp uitmaken van de vordering.".[8]

Niveau rechtsbescherming: geen effectieve rechterlijke controle

6. Het Comité stelt vast dat niet eenzelfde niveau van rechtsbescherming in het wetsontwerp wordt ingebouwd tegenover de bevoegdheid in het ontworpen artikel 16/2/1 W.I&V als het niveau van rechtsbescherming tegenover de bevoegdheid in het ontworpen artikel 39*quinquies* Sv. Nochtans gaat het in beide bepalingen om dezelfde bevoegdheid. Het Comité is van oordeel dat er geen objectieve rechtvaardiging bestaat om de burger minder te beschermen in de inlichtingenprocedure dan in de strafprocedure.

7. Een vergelijking tussen beide wetsbepalingen leert dat er vooreerst een grote discrepantie bestaat tussen de verplichte vermeldingen in de beslissing van het diensthoofd opgelegd in het ontworpen artikel 16/2/1 W.I&V en deze opgelegd in het ontworpen artikel 39*quinquies* Sv. De

---

[7] D'un point de vue grammatical, le Comité constate que dans la version néerlandaise du projet d'article 16/2/1, les mots *« pour procéder à »* ne sont pas traduits, comme c'est le cas aux articles 16/2, 18/7 et 18/8 L.R&S, par *« om over te gaan tot »*. Ceci a néanmoins une incidence sur le fond, puisque dans certaines dispositions, le service de renseignement a également la compétence *« om over te gaan tot »* (à savoir dans les articles 18/7 et 18/8). En outre, dans les articles 16/2, 18/7 et 18/8 actuels de la loi, les actes d'enquête proprement dits – en d'autres termes, les verbes « identifier », « localiser » et « repérer » – sont placés sous les points 1° et 2°, ce qui rend clairement les articles concernés plus lisibles. Le Comité ne comprend pas pourquoi le verbe « conserver » figure dans la phrase introductive du projet d'article 16/2/1. Plus généralement, le Comité constate que dans ce projet de loi, comme d'ailleurs dans les derniers projets de loi visant à modifier la Loi relative aux services de renseignement, trop peu d'attention a été accordée à la version néerlandaise (traduction) des modifications concernées.

[8] Grammaticaal gezien, stelt het Comité vast dat in de Nederlandse versie van het ontworpen artikel 16/2/1 de woorden *"pour procéder à"* niet, zoals dit wel het geval is in de artikelen 16/2, 18/7 en 18/8 W.I&V, vertaald worden als *"om over te gaan tot"*. Nochtans heeft dit een inhoudelijke draagwijdte gezien de inlichtingendienst in sommige bepalingen eveneens de bevoegdheid heeft om "te doen overgaan tot" (m.n. in de artt. 18/7 en 18/8). Verder worden in de actuele artikelen 16/2, 18/7 en 18/8 W.I&V de eigenlijke onderzoekshandeling – m.a.w. het werkwoord "identificeren", "lokaliseren", "opsporen" – ondergebracht onder de punten 1° en 2°. Dit komt de leesbaarheid van betrokken artikelen duidelijk ten goede. Het Comité begrijpt niet waarom in het ontworpen artikel 16/2/1 het werkwoord "bewaren" in de inleidende zin staat. Meer algemeen, stelt het Comité vast dat bij dit wetsontwerp, net zoals overigens bij de laatste wetsontwerpen tot wijziging van de Inlichtingenwet, te weinig aandacht besteed wordt aan de Nederlandstalige versie (vertaling) van de betrokken wijzigingen.

mentions obligatoires de ces dernières dispositions correspondent largement à celles établies dans une décision du dirigeant du service pour une méthode spécifique (*cf.* article 18/2, § 2 L.R&S).

8. La procédure proposée dans le projet d'article 16/2/1 L.R&S comme mécanisme de contrôle – à savoir une notification mensuelle des méthodes utilisées (donc après la mise en œuvre de plusieurs méthodes) – est, de l'avis du Comité, en décalage avec le degré d'ingérence qu'une telle méthode entraînerait. Plus généralement, le gouvernement rappelle lui-même dans l'exposé des motifs que dans son arrêt du 6 octobre 2020, la Cour de justice exige que la conservation ciblée des données de trafic et de localisation nécessite que *« (l)a décision de l'autorité compétente doit être soumise à un contrôle juridictionnel effectif »*.[9] Selon le Comité, le contrôle prévu dans le projet d'article 16/2/1 L.R&S ne répond aucunement à cette exigence.

9. Le Comité rappelle également au gouvernement qu'en 2010, un niveau inférieur de protection juridique était déjà prévu pour « l'accès » aux données de trafic et de localisation électroniques par les services de renseignement. La loi MRD du 4 février 2010 a intégré cette méthode dans la Loi relative aux services de renseignement à l'article 18/8 L.R&S.[11] Le législateur a repris cette compétence comme une méthode spécifique dans le cadre de la procédure de renseignement. Dans la procédure pénale, cependant, la même compétence est inscrite à l'article 88*bis* CIC, c'est-à-dire comme une mesure d'enquête relevant du juge d'instruction et non du procureur du Roi. En comparant le niveau de protection juridique de la procédure de renseignement et de la procédure pénale, les procédures MRD correspondent, pour les méthodes spécifiques, au niveau de compétence du procureur du Roi et, pour les méthodes

verplichte vermeldingen in laatstgenoemde bepalingen komen overigens grotendeels overeen met deze gesteld in een beslissing van het diensthoofd voor een specifieke methode (*cf.* artikel 18/2, §2 W.I&V).

8. Ook de in het ontworpen artikel 16/2/1 W.I&V als controlemechanisme voorgestelde procedure – m.n. een maandelijkse notificatie van de gedane methodes (dus na de uitvoering van meerdere methodes) – correspondeert volgens het Comité geheel niet met de graad van inmenging die een dergelijke methode met zich meebrengt. Meer algemeen, is het de regering zelf die er in de memorie van toelichting eraan herinnert dat het Hof van Justitie in zijn arrest van 6 oktober 2020 eist dat een gerichte bewaring van verkeers- en lokalisatiegegeven vereist dat *"(h)et besluit van de bevoegde autoriteit (…) onderworpen (is) aan een effectieve rechterlijke toetsing"*.[10] De controle uitgewerkt in het ontworpen artikel 16/2/1 W.I&V voldoet volgens het Comité geenszins aan deze verplichting.

9. Het Comité brengt de regering er daarnaast in herinnering dat in 2010 reeds een lagere rechtsbescherming werd ingebouwd met betrekking tot de "toegang" tot elektronische verkeers- en lokalisatiegegevens door de inlichtingendiensten. Via de BIM-wet van 4 februari 2010 werd deze methode in de Inlichtingenwet ingeschreven in artikel 18/8 W.I&V.[12] De wetgever kwalificeerde betrokken bevoegdheid binnen de inlichtingenprocedure als specifieke methode. Eenzelfde bevoegdheid werd echter in de strafprocedure ingeschreven in artikel 88*bis* Sv, m.a.w. als onderzoeksmaatregel die toebehoort aan de onderzoeksrechter en niet aan de procureur des Konings. Wanneer we een vergelijking maken tussen de inlichtingenprocedure en de strafprocedure voor wat betreft het niveau van rechtsbescherming corresponderen de BIM-procedures voor specifieke methoden met het bevoegdheidsniveau van de procureur des

9 Exposé des motifs du projet de loi, p. 97.
10 Memorie van toelichting bij het wetsontwerp, pag. 97.
11 Cette méthode est d'ailleurs également traitée dans le présent projet de loi.
12 Deze methode maakt overigens eveneens het voorwerp van behandeling in voorliggend wetsontwerp.

exceptionnelles, au niveau de compétence du juge d'instruction. Si le législateur avait voulu prévoir un même niveau de protection juridique entre la procédure de renseignement et la procédure pénale, la méthode visée à l'article 18/8 L.R&S aurait dû être reprise comme une méthode exceptionnelle.

Étant donné que la procédure de renseignement offre déjà des niveaux inférieurs de protection juridique pour « l'accès » aux données relatives au trafic et à la localisation, le Comité estime qu'il est absolument indéfendable que la conservation de ces données bénéficie également de niveaux inférieurs de protection juridique à la suite de l'introduction de l'article 16/2/1 L.R&S. De cette manière, la protection juridique des données concernées est fixée à un niveau très bas. Nous rappelons également au gouvernement qu'il s'agit ici de données relatives au trafic et à la localisation, une catégorie de données à caractère personnel pour laquelle la CEDH et la Cour constitutionnelle ont jugé que la conservation et l'accès impliquaient une grave intrusion dans la vie privée.

Pouvoir de délégation

10. Le Comité note également que le régime élaboré dans le projet d'article 16/2/1 L.R&S prévoit un pouvoir de délégation. Plus précisément, le gouvernement propose que le pouvoir de réquisition en question puisse être exercé par *« le dirigeant de service ou son délégué ».*

11. Le Comité constate que cette disposition s'inspire de l'article 16/2 L.R&S. Cette dernière disposition prévoit également la possibilité de faire signer la réquisition des opérateurs de télécommunications par un délégué du dirigeant du service. Le Comité estime qu'une comparaison entre les deux procédures est inappropriée. La réquisition visée à l'article 16/2 L.R&S concerne la réquisition des données d'identification, qui sont moins intrusives. La conservation demandée dans le

Konings en voor uitzonderlijke methoden met het bevoegdheidsniveau van de onderzoeksrechter. Had de wetgever eenzelfde rechtsbescherming wensen in te richten tussen de inlichtingenprocedure en de strafprocedure dan had de methode bedoeld in artikel 18/8 W.I&V gekwalificeerd dienen te worden als uitzonderlijke methode.

Doordat de inlichtingenprocedure reeds een lagere rechtsbescherming organiseert voor "de toegang" tot verkeers- en lokalisatiegegevens is voor het Comité absoluut niet verdedigbaar dat nu ook via de instelling van het ontworpen artikel 16/2/1 W.I&V "de bewaring" van dergelijke gegevens een lagere rechtsbescherming genieten. Op deze manier wordt de rechtsbescherming rond betrokken gegevens wel zeer laag ingericht. We brengen de regering hierbij tevens in herinnering dat het in deze toch gaat over verkeers- en lokalisatiegegevens, een categorie van persoonsgegevens waarvan zowel het EHRM als het Grondwettelijk Hof heeft geoordeeld dat de bewaring en de toegang ervan gepaard gaan met een grote inmenging in de persoonlijke levenssfeer.

Delegatiebevoegdheid

10. Het Comité stelt verder vast dat de regeling uitgewerkt in het ontworpen artikel 16/2/1 W.I&V voorziet in een delegatiebevoegdheid. Meer in het bijzonder stelt de regering voor dat de betrokken vorderingsbevoegdheid uitgeoefend mag worden door *"het diensthoofd of zijn gedelegeerde"*.

11. Het Comité stelt vast dat voor deze regeling inspiratie werd gevonden in artikel 16/2 W.I&V. Ook laatstgenoemde bepaling voorziet namelijk in de mogelijkheid om de vordering van de telecomoperatoren te laten ondertekenen door een gedelegeerde van het diensthoofd. Het Comité is van oordeel dat een vergelijking tussen beide procedures evenwel niet opgaat. De vordering bedoeld in artikel 16/2 W.I&V betreft het vorderen van identificatiegegevens. Dergelijke gegevens zijn

projet d'article 16/2/1 L.R&S concerne cependant les données de trafic et de localisation relatives aux communications électroniques. Comme la Cour constitutionnelle et la CEDH, le Comité est d'avis que de telles données sont très intrusives. Par conséquent, aucune justification ne peut être trouvée à l'article 16/2 pour prévoir le pouvoir de délégation dans le projet d'article 16/2/1 L.R&S également.

minder intrusief in de persoonlijke levenssfeer. De in het ontworpen artikel 16/2/1 W.I&V gevorderde bewaring betreft echter verkeers- en lokalisatiegegevens inzake elektronische communicatie. Net zoals het Grondwettelijk Hof en het EHRM is het Comité van oordeel dat dergelijke gegevens zeer intrusief zijn. Er kan bijgevolg geen rechtvaardiging gevonden worden in artikel 16/2 om de delegatiebevoegdheid eveneens te voorzien in het ontworpen artikel 16/2/1 W.I&V.

12. Pour une bonne compréhension de la disposition proposée, il est important de savoir que la Loi relative aux services de renseignement fournit une description de la notion de dirigeant du service, à savoir : *« d'une part, l'administrateur général de la Sûreté de l'Etat ou, en cas d'empêchement, l'administrateur général faisant fonction et, d'autre part, le chef du Service Général du Renseignement et de la Sécurité ou, en cas d'empêchement, le chef faisant fonction »* (art. 3, 8° L.R&S). Cette notion a été introduite par la Loi MRD du 4 février 2010 afin de placer clairement la compétence de décision de l'utilisation de méthodes spécifiques et exceptionnelles (collectivement : les « méthodes de recueil de données », ou en abrégé : les « MRD ») entre les mains des dirigeants des services de renseignement. Il est significatif que la définition juridique de la notion de dirigeant du service contienne déjà un pouvoir de délégation : *en cas d'empêchement* de l'Administrateur général de la VSSE ou du Chef du SGRS, les dirigeants des service respectifs ont la possibilité de déléguer leur pouvoir de décision à, respectivement, l'Administrateur général ou au chef de service *faisant fonction*. Cette délégation n'est pas limitée à l'Administrateur général adjoint de la VSSE et au Chef adjoint du SGRS. En cas d'empêchement de ces derniers, une nouvelle délégation peut être faite à un niveau inférieur de la hiérarchie.

12. Voor een goed begrip van voorgestelde bepaling is het van belang te weten dat de Inlichtingenwet voorziet in een omschrijving van het begrip diensthoofd, zijnde: *"enerzijds, de administrateur-generaal van de Veiligheid van de Staat of, bij verhindering, de dienstdoende administrateur-generaal, en anderzijds, het hoofd van de algemene Dienst inlichting en veiligheid van de Krijgsmacht of, bij verhindering, het dienstdoende hoofd"* (art. 3, 8° W.I&V). Het betrokken begrip werd ingevoerd door de BIM-wet van 4 februari 2010, en dit om de beslissingsbevoegdheid tot het aanwenden van specifieke en uitzonderlijke methoden (gezamenlijk: de "bijzondere inlichtingenmethoden", kortweg: de "BIM-methoden") op duidelijk wijze in handen te leggen van de hoofden van de inlichtingendiensten. Betekenisvol is dat de wettelijke definitie van het begrip diensthoofd reeds een delegatiebevoegdheid in zich draagt: *bij verhindering* van de administrateur-generaal van de VSSE of van de chef van de ADIV, hebben de respectievelijke hoofden de mogelijkheid om hun beslissingsbevoegdheid te delegeren naar de *dienstdoende* administrateur-generaal respectievelijk de *dienstdoende* chef. Een dergelijke delegatie beperkt zich niet tot de adjunct-administrateur-generaal van de VSSE en de adjunct-chef van de ADIV. Wanneer laatstgenoemden op hun beurt verhinderd zijn, kan opnieuw een delegatie toegekend worden aan een hiërarchisch lager niveau.

13. Le projet d'article 16/2/1 L.R&S prévoit la possibilité d'un pouvoir de délégation supplémentaire, en plus du pouvoir de

13. Het ontworpen artikel 16/2/1 W.I&V voorziet in de mogelijkheid om, bovenop de delegatiebevoegdheid krachtens artikel 3, 8°

délégation prévu à l'article 3, 8° L.R&S lors de la mise en œuvre de la méthode de renseignement en question. Le Comité estime qu'une telle possibilité soulève des questions, et ce pour plusieurs raisons. Comme indiqué ci-dessus, la méthode développée dans le projet d'article 16/2/1 L.R&S implique une ingérence importante dans la vie privée des personnes visées. Dans le cadre de la procédure pénale (à savoir dans le projet d'article 39*quinquies* CIC – *supra*), ce pouvoir est donc également accordé au procureur du Roi. Il n'est pas question d'un quelconque pouvoir de délégation dans la disposition pénale concernée. Le Comité demande au gouvernement quelle est la justification objective de l'exigence d'un pouvoir de délégation supplémentaire dans la procédure de renseignement, justification qui n'existe manifestement pas dans la procédure pénale. Ceci est d'autant plus vrai que la première réglementation citée inclut déjà un pouvoir de délégation dans la description juridique de la notion de dirigeant du service.

Le Comité trouve également incompréhensible que le projet de loi ne propose pas de description de la notion de délégué. Il est ainsi possible à toute personne, quel que soit son niveau ou son diplôme, d'être désignée comme *« délégué »*. C'est problématique, vu qu'il s'agit ici d'une délégation de pouvoirs qui, comme mentionné ci-dessus, sont en premier lieu directement accordés à l'Administrateur général de la VSSE et au Chef du SGRS.

14. Au regard de ce qui précède, le Comité permanent R recommande de supprimer les mots *« ou son délégué »*. Si le gouvernement considère qu'il existe une justification objective pour laquelle une telle possibilité supplémentaire de délégation est indispensable et doit être introduite – et compte tenu du fait que la méthode reprise dans le projet d'article 16/2/1 L.R&S ne devient pas une méthode spécifique (ce que le Comité considère comme problématique pour plusieurs raisons (*supra*)) – le Comité estime qu'une définition juridique du terme

W.I&V, bij de uitoefening van de betrokken inlichtingenmethode te voorzien in een extra delegatiebevoegdheid. Het Comité is van oordeel dat een dergelijke mogelijkheid om meerdere redenen vragen doet rijzen. Zoals gezegd, brengt de in het ontworpen artikel 16/2/1 W.I&V uitgewerkte methode een omstandige inmenging teweeg in de persoonlijke levenssfeer van de geviseerde personen. Binnen de strafprocedure (m.n. in het ontworpen artikel 39*quinquies* Sv – *supra*) wordt deze bevoegdheid daarom ook toegekend aan de procureur des Konings. Van enige delegatiebevoegdheid is geen sprake in betrokken strafbepaling. Het Comité vraagt aan de regering wat de objectieve rechtvaardiging is die een extra delegatiebevoegdheid noodzakelijk maakt in de inlichtingenprocedure, rechtvaardiging die kennelijk niet aanwezig is in de strafprocedure. Dit temeer omdat in eerstgenoemde regeling reeds een delegatiebevoegdheid ligt besloten in de wettelijke omschrijving van het begrip diensthoofd.

Het is voor het Comité daarenboven onbegrijpelijk dat in het wetsontwerp geen omschrijving van het begrip gedelegeerde wordt voorgesteld. Hierdoor is het mogelijk dat eenieder, ongeacht zijn niveau of graad, kan aangewezen worden als *"gedelegeerde"*. Dit is problematisch. Het gaat hier tenslotte over een delegatie van bevoegdheden die, zoals gezegd, in eerste instantie rechtstreeks worden toekend aan de administrateur-generaal van de VSSE en de chef van de ADIV.

14. In het licht van bovenstaande beveelt het Comité I aan om de woorden "of zijn gedelegeerde" te schappen. Indien er volgens de regering alsnog een objectieve rechtvaardiging zou zijn waarom een dergelijke extra delegatiemogelijkheid onmisbaar is en moet ingericht worden – en indachtig dat de in het ontworpen artikel 16/2/1 W.I&V bepaalde methode niet vertaald wordt tot een specifieke methode (wat om meerdere redenen volgens het Comité problematisch is (*supra*)) – is het Comité van oordeel dat een wettelijke

« délégué » doit figurer à l'article 3 L.R&S. Dans ce cas, le Comité recommande vivement que la délégation soit limitée au niveau de directeur, c'est-à-dire au niveau juste inférieur à celui de l'Administrateur général adjoint de la VSSE et juste inférieur à celui du Chef adjoint du SGRS. Vu le degré d'intrusion dans la vie privée, déléguer cette compétence à un officier de renseignement n'est pas défendable.

Le Comité recommande également de décrire la relation entre le dirigeant du service (en cas d'empêchement de l'Administrateur général de la VSSE ou du Chef du SGRS) et la personne déléguée (directeur). Dans sa formulation actuelle, le projet d'article 16/2/1 L.R&S ne précise pas quelle est la personne qui exerce la compétence et porte donc la responsabilité finale de la mise en œuvre ou non de la méthode en question.

Objet de la méthode

15. Enfin, le Comité demande au gouvernement de déterminer plus clairement les cas qui peuvent être soumis à la méthode en question. Bien que trois exemples soient donnés dans l'exposé des motifs, le champ d'application semble néanmoins plus restreint que la compétence comparable visée à l'article 39*quinquies* CIC.

ACCÈS AUX DONNÉES DE TRAFIC ET DE LOCALISATION

16. Par le biais de l'article 28 du projet de loi, le gouvernement entend rétablir l'article 18/8 L.R&S, qui a été en grande partie annulé par la Cour constitutionnelle (voir l'arrêt n° 57/2021 du 22 avril 2021). Cette disposition règle l'accès aux données relatives au trafic et à la localisation des communications électroniques par les services de renseignement.

definitie van het begrip "gedelegeerde" moet worden ingeschreven in artikel 3 W.I&V. In dergelijk geval beveelt het Comité sterk aan om delegatie te beperken tot het niveau van directeur, zijnde het niveau net onder de adjunct-administrateur-generaal VSSE en net onder de adjunct-chef ADIV. Gelet op de graad van inmenging op de persoonlijke levenssfeer is het niet verdedigbaar dat deze bevoegdheid kan gedelegeerd worden aan een inlichtingenofficier.

Het Comité beveelt daarnaast aan dat beschreven wordt wat de verhouding is tussen het dienstdoende hoofd (bij verhindering van de administrateur-generaal VSSE of de chef ADIV) en de gedelegeerde (directeur). Het ontworpen artikel 16/2/1 W.I&V voorziet in zijn actuele bewoording immers niet welke persoon de bevoegdheid dient uit te oefenen en die zodoende de eindverantwoordelijkheid draagt bij het al dan niet inzetten van betrokken methode.

Voorwerp van de methode

15. Het Comité verzoekt tot slot de regering duidelijker te omschrijven welk gevallen het voorwerp van betrokken methode kunnen zijn. Hoewel er reeds in de memorie van toelichting een drietal voorbeelden worden meegegeven, lijkt het toepassingsgebied desalniettemin enger te worden ingevuld dan de vergelijkbare bevoegdheid bedoeld in artikel 39*quinquies* Sv.

TOEGANG TOT VERKEERS- EN LOKALISATIEGEGEVENS

16. Via artikel 28 van het wetsontwerp beoogt de regering het grotendeels door het Grondwettelijk Hof vernietigde artikel 18/8 W.I&V te herstellen (zie arrest nr. 57/2021 van 22 april 2021). Betrokken bepaling regelt de toegang tot de verkeers- en lokalisatiegegevens met betrekking tot elektronische communicatie door de inlichtingendiensten.

17. Le gouvernement a choisi de rétablir l'article 18/8 tel qu'il était avant l'annulation, à l'exception du paragraphe 2.

Ce paragraphe annulé stipulait que, dans le cadre du suivi
- des organisations criminelles ou des organisations sectaires nuisibles : le dirigeant du service ne peut, dans sa décision, requérir les données que pour une période de six mois préalable à la décision ;
- de l'ingérence et de l'espionnage : il s'agissait d'une période de neuf mois préalable à la décision ;
- du terrorisme ou de l'extrémisme: il s'agissait d'une période de douze mois préalable à la décision.

L'exposé des motifs reprend les arguments suivants concernant cette modification :
« Dans son arrêt du 22 avril 2021, la Cour constitutionnelle a décidé d'annuler les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.

Elle justifie l'annulation de l'ensemble de ces dispositions par le fait qu'elles sont indissociablement liées à l'obligation de conservation générale et indifférenciée des données relatives aux communications électroniques par les opérateurs (voir points B.18 et B.20), principe considéré comme disproportionnel par la Cour de justice de l'Union européenne dans ses arrêts du 6 octobre 2020.

L'article 14 de cette loi du 29 mai 2016 modifiait l'article 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cet article 18/8 porte sur l'accès aux données de communications électroniques par les services de renseignement et de sécurité et non sur la conservation de ces données. Seul le paragraphe 2 de cet article fait référence à l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.

17. De regering heeft ervoor geopteerd om het artikel 18/8 te herstellen als voor de vernietiging, met uitzondering van paragraaf 2. Deze vernietigde paragraaf stelde dat, in het kader van de opvolging van:

- criminele organisaties of schadelijke sektarische organisaties: het diensthoofd in zijn beslissing de gegevens slechts kon vorderen voor een periode van zes maanden voorafgaand aan de beslissing;
- inmenging en spionage: was dit een periode van negen maanden voorafgaand aan de beslissing;
- terrorisme of extremisme: was dit een periode van twaalf maanden voorafgaand aan de beslissing.

De memorie van toelichting geeft volgende argumentatie omtrent deze wijziging:
"Bij arrest van 22 april 2021 heeft het Grondwettelijk Hof beslist om de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie te vernietigen.

Het Hof verantwoordt de vernietiging van het geheel van deze bepalingen door het feit dat deze onlosmakelijk verbonden zijn met de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie door de operatoren (zie punten B.18 en B.20), hetgeen door het Hof van Justitie van de Europese Unie als disproportioneel werd bevonden in haar arresten van 6 oktober 2020.

Artikel 14 van deze wet van 29 mei 2016 wijzigde artikel 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Dit artikel 18/8 betreft de toegang tot de gegevens met betrekking tot elektronische communicatie door de inlichtingen- en veiligheidsdiensten en niet de bewaring van deze gegevens. Enkel in paragraaf 2 van dit artikel werd gerefereerd naar artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Dès lors, seule l'annulation de ce paragraphe se justifie eu égard aux arrêts précités.

Les autres modifications visées à l'article 14 doivent donc être réintégrées.

L'article 18/8 ayant encore été modifié après la loi du 29 mai 2016, il est difficile de restituer la version en vigueur suite à l'annulation effectuée par la Cour. Les auteurs du projet ont donc décidé, par sécurité juridique, de remplacer entièrement l'article 18/8.

Néanmoins, il convient de préciser qu'aucune modification n'est apportée à l'accès par les services de renseignement et de sécurité aux données de communications électroniques, ni à ses modalités.

Les deux seules modifications portent sur la 'disparation' du paragraphe 2 logiquement annulé par la Cour constitutionnelle et sur le remplacement de la notion de « opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique » par le mot « opérateur » suite à la nouvelle définition insérée à l'article 3, 10°/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

L'accès aux données par les services de renseignement et de sécurité visé à l'article 18/8 porte bien entendu sur toutes les données conservées par les opérateurs, peu importe pour quelle finalité.

En effet, comme le précise la Cour de Justice de l'Union européenne dans son arrêt du 6 octobre 2020, en ses points 166 et 167, un accès à des données conservées pour un objectif de lutte contre la criminalité ou pour les besoins propres des opérateurs (facturation, marketing, sécurité des réseaux,

Bijgevolg dringt zich enkel de vernietiging van deze paragraaf op in het licht van voormelde arresten.

De overige wijzigingen doorgevoerd door artikel 14 dienen bijgevolg opnieuw geïntegreerd te worden.

Gezien artikel 18/8 na de wet van 29 mei 2016 nogmaals werd gewijzigd, is het moeilijk om de versie van kracht ten gevolge van de vernietiging door het Hof te herstellen. De auteurs van het ontwerp hebben bijgevolg ervoor geopteerd om het volledige artikel 18/8 te vervangen omwille van redenen van rechtszekerheid.

Het is echter aangewezen om te preciseren dat geen enkele wijziging werd aangebracht aan de toegang tot de gegevens met betrekking tot de elektronische communicatie door de inlichtingen- en veiligheidsdiensten, noch aan de modaliteiten ervan.

De enige twee wijzigingen betreffen de "verdwijning" van paragraaf 2, die logischerwijze werd vernietigd door het Grondwettelijk Hof en de vervanging van het begrip "operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst" door het woord "operator" ten gevolge van de nieuwe definitie die werd ingevoegd in artikel 3, 10°/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

De toegang tot de gegevens door de inlichtingen- en veiligheidsdiensten bedoeld in artikel 18/8, heeft betrekking op alle gegevens bewaard door de operatoren, ongeacht de doelstelling.

Zoals het Hof van Justitie van de Europese Unie in zijn arrest van 6 oktober 2020 in de punten 166 en 167 heeft verklaard, is de toegang tot de gegevens die zijn bewaard met het oog op de bestrijding van criminaliteit of voor de eigen behoeften van de operatoren (facturatie, marketing, netwerkbeveiliging, enz.) a fortiori

…) est a fortiori justifié par l'objectif de sauvegarde de la sécurité nationale.

Le Comité souhaite rappeler au gouvernement que la Cour constitutionnelle a annulé l'intégralité de l'article 18/8 L.R&S. De l'avis du Comité, il est prématuré de conclure, comme le fait le gouvernement, que seule l'annulation du paragraphe 2 s'impose à la lumière des arrêts pertinents de la Cour constitutionnelle et de la CEDH. Ce sont les garanties juridiques procédurales dans leur ensemble qui doivent être prises en considération. L'introduction de garanties en ce qui concerne la conservation des données relatives aux données de trafic et de localisation en question ne signifie pas que l'accès modulé à ces données peut automatiquement être supprimé.

18. À l'article 26 du projet de loi, le point 12° de l'article 18/3, § 2 L.R&S a été supprimé. Cette disposition prévoit que *« la motivation de la durée de la période à laquelle a trait la collecte de données »* doit être mentionnée dans la décision du dirigeant du service en vue de la mise en œuvre de la méthode visée à l'article 18/8 L.R&S. Le Comité n'approuve pas du tout cette suppression. Même si le paragraphe 2 de l'article 18/8 L.R&S tombe, cette référence garde une grande valeur au regard du contrôle, par la Commission BIM, de l'exigence de proportionnalité pour les méthodes spécifiques (*cf.* art. 18/3, § 1er L.R&S). En outre, le Comité peut constater que le gouvernement suit le même raisonnement en ce qui concerne l'article 88*bis* CIC. L'alinéa 5 de cette disposition n'envisage en effet nullement la suppression de cette référence obligatoire.

CONSERVATION GÉNÉRALISÉE ET INDIFFÉRENCIÉE DES DONNÉES DE TRAFIC ET DE LOCALISATION

19. Le gouvernement propose, à l'article 31 du projet de loi, d'inscrire dans la Loi relative aux services de renseignement une nouvelle

gerechtvaardigd ter vrijwaring van de nationale veiligheid."

Het Comité wenst de regering in herinnering te brengen dat het Grondwettelijk Hof het gehele artikel 18/8 W.I&V heeft vernietigd. Stellen – zoals de regering doet – dat enkel de vernietiging van paragraaf 2 zich opdringt in het licht van de betrokken arresten van het Grondwettelijk Hof en het EHRM, is naar het oordeel van het Comité een voorbarige conclusie. Het is het geheel aan procedurele rechtswaarborgen dat in overweging genomen moet worden. Het instellen van waarborgen op het vlak van de bewaring van betrokken verkeers- en lokalisatiegegevens brengt niet met zich mee dat de gemoduleerde toegang tot betrokken gegevens automatisch kan wegvallen.

18. In artikel 26 van het wetsontwerp wordt punt 12° van artikel 18/3, §2 W.I&V geschrapt. Deze bepaling stelt dat *"de motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft"* verplicht moet vermeld worden in de beslissing van het diensthoofd tot het aanwenden van de methode bedoeld in artikel 18/8 W.I&V. Het Comité onderschrijft geenszins beoogde schrapping. Zelfs wanneer paragraaf 2 van artikel 18/8 W.I&V wordt weggelaten, blijft betrokken vermelding een grote meerwaarde hebben in het licht van de door de BIM-Commissie uitgevoerde controle op de proportionaliteitsvereiste gesteld tegenover specifieke methoden (*cf*. art. 18/3, §1 W.I&V). Het Comité kan daarenboven vaststellen dat de regering eenzelfde redenering volgt voor wat betreft artikel 88*bis* Sv. In het vijfde lid van deze bepaling wordt namelijk de schrapping van deze verplichte vermelding geenszins vooropgesteld.

ALGEMENE EN ONGEDIFFERENTIEERDE BEWARING VAN VERKEERS- EN LOKALISATIEGEGEVENS

19. De regering stelt in artikel 31 van het wetsontwerp voor om in het kader van het bewaren van verkeers- en lokalisatiegegevens

méthode exceptionnelle dans le cadre de la conservation des données relatives au trafic et à la localisation dans le secteur des communications électroniques. Plus précisément, le projet d'article 18/17/1, alinéa 1er L.R&S prévoit que *« (l)es services de renseignement et de sécurité p(uissent), dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux. ».*[13] [14]

in de sector van de elektronische communicatie een nieuwe uitzonderlijke methode in de Inlichtingenwet in te schrijven. Meer in het bijzonder bepaalt het ontworpen artikel 18/17/1, eerste lid W.I&V dat *"(d)e inlichtingen- en veiligheidsdiensten (…), in het belang van de uitoefening van hun opdrachten en in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid, de medewerking (kunnen) vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt."*.[15] [16]

20. Le Comité souscrit pleinement à la proposition du gouvernement de soumettre l'utilisation de cette compétence à tous les mécanismes de contrôle inhérents aux méthodes exceptionnelles.

20. Het Comité onderschrijft ten volle het voorstel van de regering om de aanwending van deze bevoegdheid te onderwerpen aan alle controlemechanismen eigen aan de uitzonderlijke methoden.

21. Conformément aux articles 7 et 11 L.R&S, la compétence de la VSSE et du SGRS dans le cadre de la mission de renseignement est déterminée, entre autres, par une liste légale de certains intérêts fondamentaux du pays. En d'autres termes, la question de savoir si un service de renseignement est compétent dans un cas concret doit être résolue en examinant si, dans ce cas concret, un lien peut être trouvé avec au moins un de ces intérêts. L'utilisation de la notion de « sécurité nationale » dans le projet d'article 18/17/1, alinéa 1er L.R&S laisse la possibilité d'utiliser cette compétence pour protéger d'autres intérêts (de sécurité nationale) que ceux énumérés aux articles 7 et 11 L.R&S. Le Comité recommande donc que la notion de « sécurité nationale » dans le projet d'article 18/17/1, alinéa 1er L.R&S soit remplacé par les mots *« les intérêts*

21. Overeenkomstig de artikelen 7 en 11 W.I&V laat de bevoegdheid van de VSSE en de ADIV binnen de inlichtingenopdracht zich, onder meer, bepalen door een wettelijke oplijsting van bepaalde fundamentele belangen van het land. De vraag of een inlichtingendienst bevoegd is in een concreet geval moet m.a.w. beantwoord worden door na te gaan of in dit concreet geval een aanknopingspunt te vinden is met minstens één van deze belangen. Het gebruik van het begrip "nationale veiligheid" in het ontworpen artikel 18/17/1, eerste lid W.I&V laat ruimte open dat deze bevoegdheid wordt aangewend ter bescherming van andere (nationale veiligheids) belangen dan deze opgesomd in de artikelen 7 en 11 W.I&V. Het Comité beveelt daarom aan om het begrip *"nationale veiligheid"* in het ontworpen artikel 18/17/1,

---

13 Les mots *« une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible »* doivent – comme dans les arrêts de la Cour de Justice et de la Cour constitutionnelle – être traduits par *« een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid »*.

14 Grammaticalement, les mots *« die door hen wordt gegenereerd en verwerkt »* doivent être remplacés par *« die door hen worden gegenereerd en verwerkt ».*

15 De woorden *"une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible"* moeten – zoals in de arresten van het Hof van Justitie en het Grondwettelijk Hof – vertaald worden als *"een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid"*.

16 Grammaticaal gezien, dienen de woorden *"die door hen wordt gegenereerd en verwerkt"* te worden vervangen door *"die door hen worden gegenereerd en verwerkt"*.

fondamentaux du pays tels que visés aux articles 7 et 11 ».

Dans ce contexte, la question se pose de savoir s'il n'existe pas d'autres intérêts de sécurité nationale, dont la protection ne fait pas partie des missions des services de renseignement, qui pourraient également donner lieu à une conservation généralisée et indifférenciée.

22. Le Comité recommande de renforcer le lien entre l'actuel article 18/8 (qui règle l'accès) et le projet d'article 18/17/1 (qui règle la conservation généralisée). Actuellement, il est possible qu'une menace bien définie (par exemple, le terrorisme) puisse justifier l'imposition d'une conservation généralisée et indifférenciée aux opérateurs de télécommunications, sans aucune limitation ultérieure, et que l'accès à ces données puisse donc également être utilisé à d'autres fins (par exemple, dans le cadre de la lutte contre d'autres menaces).

Le Comité constate, en outre, qu'une telle limitation fait défaut non seulement dans la proposition de modification de la Loi relative aux services de renseignement, mais aussi dans la proposition de modification du Code d'instruction criminelle. Cela permet aux acteurs judiciaires de demander certaines données de trafic dans le cadre d'une enquête pénale portant, par exemple, sur des organisations criminelles (conformément à l'article 88*bis* CIC) lorsque ces données ont été conservées par les opérateurs de télécommunications à la demande d'un service de renseignement en raison de l'existence d'une menace terroriste grave.

23. L'alinéa 2 du projet d'article 18/17/1 prévoit que *« (l)a réquisition est effectuée par écrit par le dirigeant du service et mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné visée à l'article 18/10 § 3, alinéa 3, selon le cas ».* Le Comité rappelle au

eerste lid W.I&V te vervangen door de woorden *"de fundamentele belangen van het land zoals bedoeld in de artikelen 7 en 11"*.

In het licht hiervan rijst overigens de vraag of er geen andere nationale veiligheidsbelangen zijn, waarvan de bescherming niet behoord tot het takenpakket van de inlichtingendiensten, die eveneens de aanleiding kunnen vormen voor een algemene en ongedifferentieerde bewaring.

22. Het Comité beveelt aan om de band tussen het actuele artikel 18/8 (dat de toegang regelt) en het ontworpen artikel 18/17/1 (dat de algemene bewaring regelt) te verstevigen. Momenteel is het mogelijk dat een welbepaalde dreiging (bv. terrorisme) de rechtvaardiging kan vormen om een algemene en ongedifferentieerde bewaring op te leggen aan de telecomoperatoren, zonder dat vervolgens enige beperking van toepassing is en dat bijgevolg de toegang tot deze gegevens ook kan worden gebruikt voor andere doeleinden (bv. binnen de bestrijding van andere dreigingen).

Het Comité stelt daarnaast vast dat dergelijke beperking niet enkel ontbreekt in het voorstel tot wijziging van de Inlichtingenwet, maar eveneens in het voorstel tot wijziging van het Wetboek van Strafvordering. Hierdoor is het mogelijk dat de gerechtelijke actoren bepaalde verkeersgegevens opvragen binnen een strafonderzoek naar bv. criminele organisaties (o.g.v. artikel 88*bis* Sv) wanneer deze gegevens door de telecomoperatoren werden bewaard op vraag van een inlichtingendienst wegens het bestaan van een ernstige terreurdreiging.

23. Het tweede lid van het ontworpen artikel 18/17/1 stelt dat *"(d)e vordering (…) schriftelijk (wordt) gedaan door het diensthoofd en vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken*

gouvernement que, lorsqu'il est fait usage de méthodes exceptionnelles, le ministre de la Justice (en ce qui concerne la VSSE) ou le ministre de la Défense (en ce qui concerne le SGRS) peuvent également intervenir conformément à la procédure d'urgence visée à l'article 18/10, § 4, alinéa 9 L.R&S. Le Comité recommande donc de supprimer dans le projet d'article 18/17/1 L.R&S les mots *« visée à l'article 18/10 § 3, alinéa 3* ». Les mots *« selon le cas »* du projet de disposition, combinés aux conditions énoncées aux articles 18/10, §§ 3 et 4 L.R&S, sont suffisamment clairs à cet égard. L'alinéa 3 du projet d'article 18/17/1 est donc formulé de manière similaire à l'alinéa 5.

minister bedoeld in artikel 18/10, §3, derde lid.". Het Comité herinnert de regering eraan dat de minister van Justitie (t.a.v. de VSSE) of de minister van Defensie (t.a.v. de ADIV) bij de aanwending van uitzonderlijke methoden eveneens tussenbeide kunnen komen overeenkomstig de hoogdringendheidsprocedure bedoeld in artikel 18/10, §4, negende lid W.I&V. Het Comité beveelt daarom aan om in het ontworpen artikel 18/17/1 W.I&V de woorden *"bedoeld in artikel 18/10, §3, derde lid"* te schrappen. De woorden *"naargelang het geval"* in de ontworpen bepaling in combinatie met de voorwaarden bepaald in de artikelen 18/10, §§ 3 en 4 W.I&V zijn in deze afdoende duidelijk. Het derde lid van het ontworpen artikel 18/17/1 wordt daarmee overigens op eenzelfde wijze verwoord als zijn vijfde lid.

24. L'alinéa 3 du projet d'article 18/17/1 L.R&S proposé prévoit que : *« (l)'autorisation du dirigeant du service est transmise au ministre compétent.* Dans l'exposé des motifs, il est indiqué que : *« L'autorisation prise par le dirigeant du service concerné de mettre en œuvre cette méthode exceptionnelle est transmise au ministre compétent pour information. Il convient de préciser que le but est donc d'informer le ministre compétent qu'une conservation indifférenciée est déclenchée. Cela n'est pas à confondre avec l'autorisation qui pourrait éventuellement être prise par le ministre compétent, en application de l'article 18/10, §3, alinéa 3, si la commission ne rend pas son avis dans les quatre jours ou est dans l'impossibilité de délibérer dans ce délai. ».*

24. Het derde lid van het ontworpen artikel 18/17/1 W.I&V stelt dat *"(d)e machtiging van het diensthoofd wordt overgemaakt aan de bevoegde minister."*. De memorie van toelichting stelt hieromtrent: *"De machtiging van het betrokken diensthoofd om deze uitzonderlijke methode toe te passen, wordt ter informatie aan de bevoegde minister overgemaakt. Het doel is de bevoegde minister in kennis te stellen van het feit dat een ongedifferentieerde bewaring gestart is. Dit mag niet worden verward met de toelating die eventueel door de bevoegde minister zou kunnen worden verleend met toepassing van artikel 18/10, §3, derde lid, wanneer de commissie niet binnen de vier dagen advies uitbrengt of niet in staat is binnen deze termijn te beraadslagen."*.

Le Comité recommande que le ministre concerné soit informé non seulement de l' « autorisation » définitive du dirigeant du service, mais aussi du « projet d'autorisation ». Ni la notification du projet d'autorisation ni la notification de l'autorisation ne sont actuellement prévues dans la procédure MRD pour les méthodes exceptionnelles. Toutefois, le Comité estime qu'un si les services de renseignement ordonnent aux opérateurs de

Het Comité beveelt aan om de betrokken minister niet enkel in kennis te stellen van de uiteindelijke "machtiging" van het diensthoofd maar eerder ook al van het "ontwerp van machtiging". Zowel de notificatie van het ontwerp van machtiging als de notificatie van de machtiging worden actueel niet voorzien in de BIM-procedure bij uitzonderlijke methoden. Het Comité is echter van oordeel dat een bevel van de inlichtingendiensten aan de

télécommunications une conservation généralisée et indifférenciée[17] des données de trafic et de localisation, l'impact est si important en termes d'ingérence dans la vie privée des citoyens belges et des résidents sur le territoire belge que de telles exigences de forme divergentes se justifient certainement. Comme l'indique clairement l'exposé des motifs, la notification de l'autorisation sert à informer le gouvernement qu'une conservation généralisée et indifférenciée a été lancée. La notification du projet d'autorisation au ministre compétent n'a pas pour but de porter le pouvoir décisionnel au niveau ministériel, mais de rendre obligatoire l'information du gouvernement sur le fait que, selon le service de renseignement concerné, il existe un danger pour la sécurité nationale d'un niveau si élevé qu'une mesure aussi intrusive de conservation généralisée et indifférenciée des données de communication en question semble justifiée. Il appartiendra *in fine* à la Commission BIM d'évaluer la légalité, la subsidiarité et la proportionnalité de la méthode proposée.

25. La version néerlandaise de l'alinéa 6 du projet d'article 18/17/1 L.R&S stipule que *« (t)oute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à [dix][19] mille euros.».* Le Comité souhaite faire remarquer que la Loi relative aux services renseignement prévoit déjà diverses dispositions en matière de sanctions. Dans chaque cas, la sanction est soit *« une amende de vingt-six euros à dix mille euros »* (plus précisément à l'article 16/2, § 3 L.R&S pour refus de communication des données d'identification demandées), soit *« une amende de vingt-six euros à vingt mille euros »* (plus précisément aux articles 18/7, 18/8, 18/14, 18/15, 18/16 et 18/17L.R&S pour refus de communication des données d'identification demandées et d'assistance technique requise). Après avoir comparé le

telecomoperatoren tot het algemeen en ongedifferentieerd[18] bewaren van verkeers- en lokalisatiegegevens een dusdanige grote impact heeft op vlak van de inmenging in de persoonlijke levenssfeer van de burgers en inwoners van België dat dergelijke afwijkende vormvereisten zeker te rechtvaardigen zijn. Een kennisgeving van de machtiging dient hierbij, zoals de memorie van toelichting duidelijk verwoord, om de regering op de hoogte te brengen dat een algemene en ongedifferentieerde bewaring gestart is. Een kennisgeving van het ontwerp van machtiging aan de betrokken minister beoogt niet om de beslissingsbevoegdheid op ministerieel niveau te brengen, maar om de regering verplicht op de hoogte te brengen dat volgens de betrokken inlichtingendienst er een gevaar voor de nationale veiligheid aanwezig is van een dermate hoog niveau dat een dergelijke verregaande maatregel van algemene en ongedifferentieerde bewaring van betrokken communicatiegegevens gerechtvaardigd lijkt te zijn. Het zal uiteindelijk de BIM-Commissie zijn die de wettigheid, de subsidiariteit en de proportionaliteit van betrokken voorgestelde methode moet beoordelen.

25. De Nederlandstalige versie van het zesde lid van het ontworpen artikel 18/17/1 W.I&V stelt dat *"(e)enieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend[20] euro."*. Het Comité wenst op te merken dat de Inlichtingenwet reeds in diverse strafbepalingen voorziet. De strafmaat is hierbij telkenmale ofwel *"een geldboete van zesentwintig euro tot tienduizend euro"* (m.n. in artikel 16/2, §3 W.I&V voor wat betreft het niet overmaken van de gevorderde identificatiegegevens) ofwel *"een geldboete van zesentwintig euro tot twintigduizend euro"* (m.n. in de artikelen 18/7, 18/8, 18/14, 18/15, 18/16 en 18/17 W.I&V voor wat betreft het niet overmaken o.m. van de gevorderde verkeers- en lokalisatiegegevens of het niet verlenen van de gevorderde technische

17 Par opposition aux autres méthodes exceptionnelles qui sont ciblées (cf. art. 18/10, §2, 2° L.R&S).
18 In tegenstelling tot de andere uitzonderlijke methoden die doelgericht zijn (cf. art. 18/10, §2, 2° W.I&V).
19 La version française dit « vingt mille euros ».
20 In de Franstalige versie staat "twintigduizend euro".

projet d'article 18/17/1 L.R&S avec les dispositions légales susmentionnées et compte tenu des conditions d'introduction d'un tel nouveau comportement criminel (c'est-à-dire *« lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible »),* le Comité conclut que les sanctions prévues par le projet d'article 18/17/1 L.R&S ne sont pas suffisamment adaptées. Le Comité recommande de relever la limite de dix mille euros *au moins* jusqu'à la sanction de vingt mille euros.

Ensuite, il convient de noter que le projet d'article 39*quinquies*, § 3, alinéa 2 CIC (comparable) prévoit non seulement une amende de vingt-six à vingt mille euros mais aussi une peine d'emprisonnement de six mois à un an.

26. L'alinéa 7 du projet d'article 18/17/1 L.R&S prévoit que *« (l)a méthode est autorisée pour une durée ne pouvant excéder 6 mois sans préjudice de la procédure visée à l'article 18/10, § 5 ».* Le Comité n'a pu trouver dans l'exposé des motifs aucune raison justifiant que la durée de conservation soit de 6 mois, ni les raisons de s'écarter du délai d'utilisation dans le cadre des méthodes exceptionnelles, à savoir 2 mois (la période peut être prolongée). Le Comité recommande donc de supprimer l'alinéa 7.

27. L'alinéa 8 du projet d'article 18/17/1 L.R&S prévoit que *« (l)e service de renseignement et de sécurité concerné fait rapport à la commission tous les deux mois sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci »*. Le Comité constate que le gouvernement a opté pour un rapport bimensuel, ce qui s'écarte de la périodicité imposée pour les autres méthodes exceptionnelles. L'article 9, alinéa 1er de l'Arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du

medewerking). Een vergelijking met het ontworpen artikel 18/17/1 W.I&V met vernoemde wetsbepalingen en indachtig de voorwaarden opdat er sprake zou zijn van een dergelijk nieuw in te voeren strafbare gedraging (m.n. *"in geval van een reële, actuele of voorzienbare ernstig bedreiging van de nationale veiligheid"*), doet het Comité besluiten dat de strafmaat in het ontworpen artikel 18/17/1 W.I&V niet afdoende aangepast is. Het Comité beveelt vooreerst aan om het maximumbedrag van tienduizend euro op te trekken, *minstens* tot aan de strafmaat van twintigduizend euro.

Ten tweede kan vastgesteld te worden dat het (vergelijkbare) ontworpen artikel 39*quinquies*, §3, tweede lid Sv niet enkel voorziet in een geldboete van zesentwintig tot twintigduizend euro maar eveneens in een gevangenisstraf van zes maanden tot een jaar.

26. Het zevende lid van het ontworpen artikel 18/17/1 W.I&V stelt dat *"(d)e methode wordt toegestaan voor een periode die niet langer mag zijn dat 6 maanden onverminderd de procedure bedoeld in artikel 18/10, §5"*. Het Comité kon in de memorie van toelichting geen reden terugvinden waarom de bewaarperiode 6 maanden bedraagt noch welke de redenen zijn om af te wijken van de geldende aanwendingsduur bij uitzonderlijke methoden, zijnde 2 maanden (die eveneens verlengd kunnen worden). Het Comité beveelt aan om het zevende lid zodoende te schrappen.

27. Het achtste lid van het ontworpen artikel 18/17/1 W.I&V stelt dat *"(d)e betrokken inlichtingen- en veiligheidsdienst (…) om de twee maanden bij de Commissie verslag uit(brengt) over de evolutie van de dreiging. In dit verslag worden de elementen belicht die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen."*. Het Comité stelt vast dat de regering ter zake kiest voor een tweemaandelijkse periodiciteit van de verslaggeving. Hierbij wordt afgeweken van de periodiciteit die opgelegd is bij de andere uitzonderlijke methoden. Artikel 9, eerste lid

30 novembre 1998 organique des services de renseignement et de sécurité dispose que : « *Pour l'application de l'article 18/10, § 1er, alinéa 3*[21]*, de la loi du 30 novembre 1998, le dirigeant du service concerné informe la commission du déroulement de l'exécution de la méthode exceptionnelle toutes les deux semaines, à partir du jour où elle est mise en œuvre, sous réserve de l'article 18/13, alinéa 4, de la même loi, et lorsqu'elle prend fin ».* L'exposé des motifs, dans le cadre du projet d'article 18/17/1 L.R&S, se limite à la précision suivante: *« Tous les deux mois, le service de renseignement fournit à la Commission un état de la situation. ».* Le gouvernement ne fournit aucune explication quant à la nécessité de s'écarter du rapport bimensuel. Le Comité recommande donc de supprimer la disposition en question et de revenir ainsi à la règle générale. Une telle modification est également appropriée au regard de la recommandation du Comité de limiter la durée (qui peut être prolongée) de la méthode à deux mois.

van het Koninklijk besluit van 12 oktober 2010 'houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten' bepaalt namelijk: *"Voor de toepassing van artikel 18/10, § 1, derde lid,*[22] *van de wet van 30 november 1998 informeert het betrokken diensthoofd de commissie om de twee weken, vanaf de dag waarop de uitzonderlijke methode toegepast wordt, over het verloop ervan, onder voorbehoud van artikel 18/13, vierde lid, van dezelfde wet. Het diensthoofd informeert de commissie ook wanneer de methode beëindigd is."*. De memorie van toelichting bij het ontworpen artikel 18/17/1 W.I&V beperkt zich ter zake met volgende verduidelijking: "*Om de twee maanden geeft de inlichtingendienst een stand van zaken aan de commissie."*. De regering geeft geen verduidelijking waarom er nood is aan een afwijking van het tweewekelijkse verslag. Het Comité beveelt daarom aan om de betrokken bepaling te schrappen en zodoende terug te vallen op de gemene regeling. Ook in het licht van de aanbeveling van het Comité de (verlengbare) duur van de methode te beperkingen tot 2 maanden, is een dergelijke aanpassing aangewezen.

28. Le Comité recommande de clarifier le rapport entre le projet d'article 18/17/1 L.R&S et le régime de protection particulier pour les avocats, les médecins et les journalistes prévu par la Loi relative aux services de renseignement. En vertu de l'article 18/9, § 4 L.R&S, des méthodes exceptionnelles ne peuvent être utilisées contre l'une de ces professions protégées ou, entre autres, contre les moyens de communication utilisés à des fins professionnelles, que si le service de renseignement dispose au préalable d'indices sérieux révélant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance

28. Het Comité beveelt aan om te verduidelijken wat de verhouding is tussen het ontworpen artikel 18/17/1 W.I&V en de bijzondere beschermingsregeling voor advocaten, artsen en journalisten ingericht in de Inlichtingenwet. Krachtens artikel 18/9, §4 W.I&V kunnen uitzonderlijke methoden slechts aangewend worden tegen een van deze beschermde beroepen of, onder meer, van hun communicatiemiddelen die ze voor beroepsdoeleinden gebruikten op voorwaarde dat de inlichtingendienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan

[21] L'article 18/10, § 1er, alinéa 3 L.R&S dispose que : *« L'officier de renseignement désigné pour le suivi de la mise en œuvre de la méthode exceptionnelle de recueil de données informe régulièrement le dirigeant du service, qui, à son tour, informe la commission de l'exécution de cette méthode, selon les modalités et délais déterminés par le Roi. ».*

[22] Artikel 18/10, §1, derde lid W.I&V stelt: *"De inlichtingenofficier die is aangesteld om de aanwending van de uitzonderlijke methode voor het verzamelen van gegevens op te volgen, informeert op regelmatige wijze het diensthoofd, dat op zijn beurt, overeenkomstig de door de Koning bepaalde nadere regels en termijnen, de commissie inlicht over de uitvoering van de methode."*.

ou au développement d'une menace potentielle grave. Le cas échéant, il y a lieu de suivre une procédure particulière, allant d'une concertation préalable entre le président de la Commission BIM et le président de l'Ordre des avocats, du Conseil national de l'Ordre des médecins ou de l'Association des journalistes professionnels concernés, respectivement, jusqu'à la sélection, par le président de la Commission BIM, des données collectées qui pourront effectivement être utilisées par les services de renseignement par la suite. Le fonctionnement de la méthode visée par le projet d'article 18/17/1 s'applique de manière généralisée et indifférenciée, et donc également à l'égard des professions protégées. Toutefois, ni le projet de disposition ni l'exposé des motifs ne précisent si, et le cas échéant dans quelle mesure, ces procédures particulières s'appliquent lorsque la méthode visée au projet d'article 18/17/1 du L.R&S est utilisée.

29. En vertu de l'article 18/10, § 6, alinéa 2 L.R&S, la Commission BIM est compétente pour pénétrer dans les lieux *« où sont réceptionnées ou conservées les données recueillies par ces méthodes exceptionnelles »*. Le Comité se demande si cela signifie aussi que, dans le cadre de leur contrôle des MRD, la Commission BIM – et, en seconde ligne, le Comité permanent R – sont également compétents pour visiter et pénétrer dans les lieux appartenant aux opérateurs de télécommunications, c'est-à-dire les lieux où sont conservées les données réclamées par les services de renseignement.

Au moins en ce qui le concerne, le Comité permanent R apprend du projet d'article 127/2, § 3, dernier alinéa LCE que ses pouvoirs d'investigation sont étendus. Cette disposition prévoit que *« les autorités de protection des données compétentes peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal ».* Il s'agit du journal contenant les enregistrements de chaque opération d'accès, tenu par les Cellules de coordination des opérateurs de télécommunications. Le Comité recommande d'ajouter la Commission

het ontstaan of aan de ontwikkeling van een ernstige potentiële dreiging. Desgevallend dient een bijzondere procedure gevolgd te worden gaande van voorafgaand overleg tussen de voorzitter van de BIM-Commissie met de voorzitter van de betrokken Orde van Advocaten, van de Nationale Raad van de Orde van Geneesheren respectievelijk van de Vereniging van Beroepsjournalisten, tot een selectie door de voorzitter van de BIM-Commissie welke ingewonnen gegevens daadwerkelijk door de inlichtingendiensten nadien mogen gebruikt worden. De werking van de methode bedoeld in het ontworpen artikel 18/17/1 is algemeen en ongedifferentieerd van toepassing, en zodoende eveneens ten aanzien van de beschermde beroepen. Noch de ontworpen bepaling, noch de memorie van toelichting verduidelijken evenwel of, en zo ja, in welke mate deze bijzondere procedures toepassing kennen bij de inzet van de methode bedoeld in het ontworpen artikel 18/17/1 W.I&V.

29. Krachtens artikel 18/10, §6, tweede lid W.I&V is de BIM-Commissie bevoegd om de plaatsen te betreden *"waar de gegevens die met de uitzonderlijke methode verzameld werden, in ontvangst genomen of bewaar worden"*. Het Comité vraagt zich af of dit ook betekent dat de BIM-Commissie – en in tweede lijn, het Vast Comité I – bevoegd zijn om in het kader van hun BIM-toezicht eveneens de plaatsen te bezoeken en te betreden die toebehoren tot de telecomoperatoren, meer bepaald de plaatsen waar de bewaring van de door de inlichtingendiensten gevorderde gegevens plaatsvindt.

Althans wat het Vast Comité I betreft, leert het Comité uit het ontworpen artikel 127/2, §3, laatste lid WEC dat zijn onderzoeksbevoegdheden uitgebreid worden. In betrokken bepaling staat immers dat *"de bevoegde gegevensbeschermingsautoriteiten (…) dat logboek (mogen) raadplegen of een kopie van een deel of van het geheel van dat logboek eisen"*. Bedoeld wordt het logboek met de registratie van elke toegangsverrichting bijgehouden door de Coördinatiecellen van de telecomoperatoren.

BIM dans la disposition précitée de la LCE.

Het Comité beveelt aan dat de BIM-Commissie aan vernoemde WEC-bepaling wordt toegevoegd.

PORTÉE DE CERTAINS CONCEPTS L.R&S, NOTAMMENT COMPTE TENU DE LA LCE

30. Le Comité permanent R attire l'attention du gouvernement sur la portée des concepts qui sont utilisés dans le cadre de la Loi relative aux services de renseignement.

Via l'article 20, 2° du projet de loi, le concept d' « opérateur »" est inséré et défini dans la loi relative aux services de renseignement (un point 10°/1 est ajouté à l'article 3 L.R&S). L'exposé des motifs indique à cet égard : *« A l'article 3 le terme « opérateur est défini comme terme fourre-tout englobant ce qui est actuellement décrit comme "opérateur d'un réseau de communications électroniques" ou "fournisseur d'un service de communications électroniques". Cette modification vise à simplifier le texte »*. Le Comité reconnaît qu'une telle modification peut améliorer la lisibilité de la Loi relative aux services de renseignement.

Premièrement, il convient de noter qu'il est préférable d'utiliser le concept d' « opérateur de télécommunications ». Les articles 18/6 et 18/14 L.R&S actuels emploient également les concepts d'« opérateur » et « opérateur postal ».

Deuxièmement, le Comité constate que les termes *« fournisseur d'un service de communications électroniques »* sont absents du projet d'article 3, 10°/1 L.R&S. Or, ils sont nécessaires puisque ce dernier concept est défini plus précisément à l'article 3, 11°/1 L.R&S. La précision donnée dans l'exposé des motifs selon laquelle il convient de lire la disposition en question en tant que telle est, selon le Comité, insuffisante. Le concept s'ajoute en effet au cadre conceptuel juridique de la Loi relatives aux services de renseignement (qui précise à son tour le champ d'application des activités du service

REIKWIJDTE VAN BEPAALDE BEGRIPPEN IN DE INLICHTINGENWET, REKENING HOUDENDE MET DE TELECOMWET

30. Het Vast Comité I vestigt de aandacht van de regering op de reikwijdte van bepaalde in de Inlichtingenwet gehanteerde begrippen.

Via artikel 20, 2° van het wetsontwerp wordt het begrip "operator" in de Inlichtingenwet ingevoegd en omschreven (een punt 10°/1 wordt aan artikel 3 W.I&V toegevoegd). De memorie van toelichting stelt hieromtrent: *"In artikel 3 wordt ook het begrip "operator" gedefinieerd als zijnde het containerbegrip voor hetgeen actueel als "operator van een elektronisch communicatienetwerk" of de "verstrekker van een elektronische communicatiedienst" omschreven wordt."*. Het Comité erkent dat een dergelijke wijziging de leesbaarheid van de Inlichtingenwet ten goede kan komen.

Er dient hierbij vooreerst opgemerkt te worden dat er beter geopteerd wordt voor het begrip "telecomoperator". De actuele artikelen 18/6 en 18/14 W.I&V maken namelijk eveneens gebruik van de begrippen "operator" en "postoperator".

Ten tweede stelt het Comité vast dat de woorden *"verstrekker van een elektronische communicatiedienst"* ontbreken in het ontworpen artikel 3, 10°/1 W.I&V. Nochtans is dit noodzakelijk gezien laatstgenoemde begrip nader gedefinieerd wordt in artikel 3, 11°/1 W.I&V. De verduidelijking in de memorie van toelichting als zou betrokken bepaling als dusdanig dienen gelezen te worden, is in deze volgens het Comité niet afdoende gezien het begrip toegevoegd wordt in het wettelijke begrippenkader van de Inlichtingenwet (wat op zijn beurt het toepassingsgebied van de

de renseignement).

31. En effet, il doit se dégager clairement du projet de loi et de son exposé des motifs de quels « opérateurs » et de quelles « données » il est question.

Force est de constater que la terminologie utilisée est inspirée de la terminologie de la Loi Télécom, s'agissant de prévoir des possibilités de collectes de données auprès des « fournisseurs de services et réseaux de communications électroniques ». Cela étant, la Loi relative aux services de renseignement ne fait pas non plus nécessairement explicitement référence aux définitions de la Loi Télécom. Ce qui en soi, n'est pas nécessairement problématique dès lors que la Loi relative aux services de renseignement poursuit une finalité distincte de celle poursuivie par la Loi Télécom : alors que la seconde régule le marché des communications électroniques d'une manière harmonisée par le droit européen, la première a pour finalité de sauvegarder la sécurité nationale belge. Il est donc défendable de recourir à des concepts différents (en tout ou en partie, selon les nécessités au regard de l'objectif poursuivi par le législateur). Il n'est donc en théorie pas exclu que des services non soumis à la « *data retention* » puisse faire l'objet de réquisitions des services de renseignement et de sécurité sur la base de leur loi organique.

Cela étant précisé, le projet de loi doit identifier clairement les concepts auxquels il se réfère et, gagnerait à préciser et expliciter les raisons pour lesquelles il s'aligne ou pas sur les concepts (européens) consacrés dans la Loi Télécom. Cela est d'autant plus vrai qu'il ne peut être pensé en vase clos, s'intégrant d'ailleurs clairement dans la réforme de la rétention des données imposée dans le cadre de la Loi Télécom. Il en va de même, *mutatis mutandis*, lorsque les solutions retenues dans le domaine du droit pénal divergent de celles retenues en l'espèce.

Concept d'opérateur

handelingen van de inlichtingendienst nader bepaalt).

31. Uit het wetsontwerp en de memorie van toelichting moet duidelijk blijken welke "operatoren" en "gegevens" wordt bedoeld.

Het is duidelijk dat de gebruikte terminologie is geïnspireerd op de terminologie van de Telecomwet, voor zover deze voorziet in de mogelijkheid gegevens te verzamelen van "aanbieders van elektronische communicatiediensten en -netwerken". De Inlichtingenwet verwijst echter ook niet noodzakelijkerwijs expliciet naar de definities in de Telecomwet. Dit is op zich niet noodzakelijk problematisch, aangezien het doel van de Inlichtingenwet verschilt van dat van de Telecomwet: terwijl de Telecomwet de elektronische-communicatiemarkt regelt op een wijze die geharmoniseerd is door de Europese wetgeving, heeft de Inlichtingenwet tot doel de Belgische nationale veiligheid te vrijwaren. Het is derhalve verdedigbaar verschillende begrippen te gebruiken (geheel of gedeeltelijk, naar gelang van de behoeften van het door de wetgever nagestreefde doel). Het is dus theoretisch niet uitgesloten dat diensten die niet onder de "*gegevensbewaring*" vallen, door de inlichtingen- en veiligheidsdiensten worden gevorderd op basis van hun organieke wet.

Het wetsontwerp moet duidelijk aangeven naar welke begrippen het verwijst en zou het nuttig zijn te preciseren en uit te leggen waarom het al dan niet is afgestemd op de (Europese) begrippen die in de Telecomwet zijn vervat. Dit geldt des te meer omdat het niet los van elkaar kan worden gezien en duidelijk is geïntegreerd in de hervorming van de gegevensbewaring die door de Telecomwet wordt opgelegd. Hetzelfde geldt, *mutatis mutandis*, wanneer de op strafrechtelijk gebied gekozen oplossingen afwijken van die welke in deze aangelegenheid zijn gekozen.

Begrip 'operatoren'

32. Le Comité permanent R observe que le concept d'opérateur (*cf*. article 20, 2° du projet de loi) est distinct des concepts utilisés par l'article 17 du projet de loi, qui introduit un nouvel article 39*quinquies* dans le CIC (*supra*). Il est également distinct des concepts actuellement utilisés dans la L.R&S.

Dans l'exposé des motifs, le gouvernement de loi se réfère explicitement[23] au Code des communications électroniques européen[24] [25] et notamment aux *« services de communications interpersonnelles »* que vise désormais ce code.[26]

Il convient de souligner que cette modification du Code, par l'ajout *« des services de communications interpersonnelles »*, apporte, en droit européen, une extension significative du concept de service de communications électroniques applicable au secteur des communications électroniques.
Ainsi, alors que tel n'était pas le cas sous l'empire de la directive n° 2006/24/CE[31], sur le plan du principe, certains opérateurs « *over the top* » (« OTT » ; en l'occurrence plus précisément, les fournisseurs de webmail tels que Gmail[32], Yahoo, etc., les fournisseurs de

32. Het Vast Comité I merkt op dat het begrip "operator" (*cf*. artikel 20, 2° van het wetsontwerp) verschilt van de begrippen die worden gebruikt in artikel 17 van het wetsontwerp, waarbij een nieuw artikel 39*quinquies* Sv wordt ingevoegd (*supra*). Het verschilt ook van de momenteel in de Inlichtingenwet gehanteerde begrippen.

In de memorie van toelichting verwijst de regering uitdrukkelijk[27] naar het Europese Wetboek voor elektronische communicatie[28] [29], en meer in het bijzonder naar de *"interpersoonlijke communicatiediensten"* die nu onder dit wetboek vallen. [30]

Er moet op gewezen worden dat deze wijziging van het Wetboek, m.n. door de toevoeging van de *"interpersoonlijke communicatiediensten"*, een aanzienlijke uitbreiding betekent van het begrip 'elektronische communicatiedienst' zoals gebruikt in het Europese recht m.b.t. de elektronische communicatiesector.
Terwijl dit niet het geval was onder Richtlijn 2006/24/EG[33], zouden bepaalde "over the top"-operatoren ("OTT's"; in dit geval meer bepaald webmailproviders zoals Gmail, Yahoo, enz., en dienstverleners zoals

---

23 Lorsqu'il est question de l'article 7 qui modifie *l'article 126 LCE*

24 Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte), qui, à la connaissance du Comité, n'est pas encore transposé en droit belge

25 p. 29, quant à l'article 7 du projet qui modifie l'article 126 de la LCE.

26 Voir le considérant n° 17 et l'article 2, 4) et 5) de la Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte).

27 Bij de verwijzing naar artikel 7, dat artikel 126 WEC wijzigt.

28 Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees Wetboek voor elektronische communicatie die, voor zover het Comité bekend, nog niet in Belgisch recht is omgezet

29 p. 29, wat betreft artikel 7 van het ontwerp dat artikel 126 WEC wijzigt.

30 Zie de overweging nr. 17 en artikel 2, 4) et 5) van de (EU) Richtlijn 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 houdende invoering van het wetboek établissant le code des communications électroniques européen (refonte).

31 Directive n° 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (annulée entre-temps, par la Cour de justice)

32 Voir par exemple CJUE, arrêt du 13 juin 2019 *Google LLC c/ Bundesrepublik Deutschland*, aff. C-193/18, qui confirme que Gmail *n'est pas* un service de communications électroniques.

33 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (inmiddels nietig verklaard door het Hof van Justitie)

services tels que WhatsApp) seraient soumis aux règles prévues par la proposition.

« Les services de communications interpersonnelles sont des services qui permettent l'échange interpersonnel et interactif d'informations, comprenant des services tels que les communications vocales traditionnelles entre deux personnes, mais aussi tous les types de courriers électroniques, services de messagerie ou discussions de groupe. Les services de communications interpersonnelles couvrent uniquement les communications entre un nombre fini, c'est-à-dire qui n'est pas potentiellement illimité, de personnes physiques, qui est déterminé par l'émetteur de la communication »
*(*Au sens du Code précité, selon le considérant n° 17 de la de la Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen).

Toutefois, ne sont pas considérés comme des services de communications interpersonnelles *« les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service »*[34].
Le considérant précité illustre encore ce que ne comprend pas le concept comme suit : *« les services qui ne répondent pas à ces exigences, tels que la radiodiffusion linéaire, la vidéo à la demande, les sites internet, les réseaux sociaux, les blogs ou l'échange d'informations entre machines, ne devraient pas être considérés comme des services de communications interpersonnelles »*.

Certes, il faut souligner que dans une certaine mesure, dans le domaine de la coopération avec les autorités dans le domaine pénal, le concept de service de communications électroniques avait déjà été adapté en droit belge, suite à un arrêt Yahoo! de la Cour de

WhatsApp) dus in principe onderworpen zijn aan de regels van het wetsontwerp.

"Interpersoonlijke communicatiediensten zijn diensten die een interactieve uitwisseling van informatie tussen personen mogelijk maken, zoals traditionele telefoongesprekken tussen twee personen, maar ook alle soorten e- mails, berichtendiensten of groepchats. Interpersoonlijke communicatiediensten omvatten alleen communicatie tussen een door de afzender van de communicatie bepaald aantal, d.w.z. een niet potentieel oneindig aantal, natuurlijke personen."
(In de zin van voornoemd Wetboek, volgens overweging nr. 17 van de Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees Wetboek voor elektronische communicatie).

Worden niet beschouwd als interpersoonlijke communicatiediensten, de *"diensten die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst "*.[35]
De bovenstaande overweging illustreert verder wat het begrip niet inhoudt, en wel als volgt: *"Diensten die niet aan deze eisen voldoen, zoals lineaire omroep, video-on-demand, websites, sociale netwerken, blogs of machine-to-machine informatie-uitwisseling, mogen niet worden beschouwd als interpersoonlijke communicatiediensten"*.

Er dient uiteraard op gewezen te worden dat, op het gebied van de samenwerking met de autoriteiten in strafzaken, het begrip "elektronische communicatiedienst" reeds in zekere mate in het Belgische recht was aangepast, naar aanleiding van het arrest

[34] Article 2, 5) de la Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte).
[35] Artikel 2, 5) van de 'EU) Richtlijn 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees Wetboek van elektronische communicatie (herschikking).

cassation[36]. Ainsi, le concept originellement repris du droit des communications électroniques[37] a reçu une interprétation autonome dans le domaine de la procédure pénale, distincte de l'acception du concept en droit européen des communications électroniques. De telle sorte qu'un webmail tel que Yahoo! s'est trouvé soumis à l'obligation consacrée dans l'article 46*bis* du CIC.

L'article 3, 11°/1 de la L.R&S a été inséré par la Loi d'actualisation MRD du 30 mars 2017, en reconnaissant explicitement cette réalité : (et en entérinant également un autre arrêt Yahoo!, concernant la compétence internationale[40]) :

- *« non seulement les fournisseurs classiques d'un service de communications électroniques, visés à l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques, tombent sous l'obligation de collaboration (Proximus, Mobistar, Base, Telenet, Scarlet, VOO, Mobile Viking, les fournisseurs d'hotspots Wifi gratuits)*
- *mais c'est également le cas de tous les fournisseurs de services de communication alternatifs comme Yahoo, Hotmail, Gmail, Skype, Whats App, Viber, les jeux avec possibilité de chat... ».*[42]

Le rapport explicatif, au sujet de l'article 20 du projet introduisant et définissant le concept d'opérateur dans l'article 3, 10°/1 de la L.R&S énonce ce qui suit :
« A l'article 3 le terme 'opérateur' est défini comme terme fourre-tout englobant ce qui est actuellement décrit comme 'opérateur d'un

Yahoo! van het Hof van Cassatie.[38] Aldus heeft het oorspronkelijk aan het elektronische communicatierecht[39] ontleende begrip een autonome interpretatie gekregen op het gebied van het strafprocesrecht, dat verschilt van de interpretatie van het begrip in het Europese elektronische communicatierecht. Een webmail als Yahoo! was dus onderworpen aan de in artikel 46*bis* Sv. voorziene verplichting.

Artikel 3, 11°/1 W.I&V werd ingevoegd door de BIM-actualisatiewet van 30 maart 2017, waarbij deze realiteit uitdrukkelijk werd erkend: (en waarbij ook een ander Yahoo! arrest, betreffende de internationale rechtsmacht, werd onderschreven).[41]

- *"niet alleen de traditionele verstrekkers van een elektronische communicatiedienst als bedoeld in artikel 2, 5° van de Wet van 13 juni 2005 betreffende de elektronische communicatie, zijn onderworpen aan de verplichting tot samenwerking (Proximus, Mobistar, Base, Telenet, Scarlet, VOO, Mobile Viking, de aanbieders van gratis wifi-hotspots)*
- *maar dit geldt ook voor alle alternatieve communicatiedienstverleners zoals Yahoo, Hotmail, Gmail, Skype, Whats App, Viber, spelletjes met chatfaciliteiten... ".*[43]

In de toelichting bij artikel 20 van het ontwerp tot invoering en definitie van het begrip "operator" in artikel 3, 10°/1 van de W.I&V staat het volgende:
"In artikel 3 wordt ook het begrip "operator" gedefinieerd als zijnde het containerbegrip voor hetgeen actueel als "operator van een

36 Cass., arrêt du 18 janvier 2011 (Belgique). RG P.10.1347.N.
37 Voir explicitement en ce sens, *Doc. Parl.* Sénat, session de 2006-2007, Doc. n° 3-1824/2, Amendement n° 1 du Gouvernement, dans le cadre du processus législatif ayant mené à l'adoption de la loi du 23 janvier 2007 modifiant l'article 46*bis* du Code d'instruction criminelle. Les concepts utilisés dans le cadre du Code d'instruction criminelle étaient alignés sur ceux de la LCE.
38 Cass., arrest van 18 januari 2011 (België). RG P.10.1347.N.
39 Zie uitdrukkelijk in die zin, *Parl. St. Senaat,* 2006-2007, Doc. n° 3-1824/2, Amendement nr°1 van de Regering, in het kader van het wetgevend proces dat leidde tot de aanname van de wet van 23 januari 2007 houdende wijziging van artikel 46*bis* van het Wetboek van Strafvordering. De concepten gehanteerd in het kader van het Wetboek van Strafvordering waren gealigneerd op deze van de WEC.
40 Voir Cass., arrêt du 1er décembre 2015, n° de rôle P.13.2082.N.
41 Zie Cass., arrest van 1 december 2015, rolnummer P.13.2082.N.
42 Pp. 26-27.
43 Pp. 26-27.

réseau de communications électroniques' ou 'fournisseur d'un service de communications électroniques'. Cette modification vise à simplifier le texte ».[44]

elektronisch communicatienetwerk" of de "verstrekker van een elektronische communicatiedienst" omschreven wordt.". Deze wijziging is bedoeld om de tekst te vereenvoudigen".[45]

Cependant à l'analyse, il s'avère que l'introduction du concept d'opérateur tel que suggéré par le gouvernement a un impact quant aux prestataires de services visés.

Uit analyse blijkt echter dat de invoering van het begrip "operator", zoals voorgesteld door de regering, gevolgen heeft voor de beoogde dienstverleners.

Premièrement, compte-tenu de l'historique du sujet en Belgique et juste rappelée, en vue d'assurer la sécurité juridique, le Comité permanent R invite le gouvernement à être clair quant à ce que recouvre le concept de « fournisseur d'un service de communications électroniques », notamment au regard des concepts utilisés en droit européen de manière telle qu'à l'avenir, la présente réforme et la transposition du Code des communications électroniques européen ne cause pas de difficulté d'interprétation.

In de eerste plaats verzoekt het Vast Comité I de regering, gelet op de voorgeschiedenis van het onderwerp in België en met het oog op de rechtszekerheid, duidelijk te zijn over wat wordt bedoeld met het begrip "aanbieder van een elektronische communicatiedienst", met name in het licht van de in het Europees recht gebruikte begrippen, zodat de huidige hervorming en de omzetting van het Europees Wetboek voor elektronische communicatie in de toekomst geen aanleiding zullen geven tot interpretatiemoeilijkheden.

Deuxièmement, dès lors que le nouveau concept d' « opérateur » n'a pour objectif que d'avoir une simple correction légistique, il incombe d'y biffer les termes « sur le territoire belge » *en ce qu'ils visent les fournisseurs de services de communications électroniques*. En effet, le 11°/1 de l'article 3 de la L.R&S comprend directement, une référence au champ d'application territorial du concept/des règles concernées.
Par contre, le 11° se bornant à se référer au concept de réseau de communication électronique de la LCE, il convient bien, au sujet du concept d'opérateur de réseau de communications électroniques, d'ajouter le critère territorial souhaité.

Ten tweede moeten, aangezien het de bedoeling is dat het nieuwe begrip "operator" een eenvoudige legistieke correctie heeft, de woorden "op het Belgische grondgebied" worden geschrapt, *voor zover zij betrekking hebben op aanbieders van elektronische communicatiediensten*. Artikel 3, 11°/1 W.I&V bevat immers rechtstreeks een verwijzing naar het territoriale toepassingsgebied van het betrokken begrip/de betrokken regels.
Anderzijds is het, aangezien in punt 11° alleen wordt verwezen naar het begrip elektronisch communicatienetwerk in de WEC, dienstig het gewenste territoriale criterium toe te voegen aan het begrip operator van een elektronisch communicatienetwerk.

Troisièmement enfin, et pour la même raison, ce concept d'opérateur doit viser les « réseaux de communications électroniques » ainsi que « le fournisseur d'un service de communications électroniques », dès lors qu'il s'agit des deux concepts qu'il entend englober et qui sont déjà définis dans la L.R&S.

Ten derde, en om dezelfde reden, moet dit begrip operator zowel verwijzen naar "elektronische communicatienetwerken" als naar "de aanbieder van een elektronische communicatiedienst", aangezien dit de twee concepten zijn die het beoogt te omvatten en die reeds in de W.I&V zijn gedefinieerd.

[44] P. 102.
[45] P. 102.

Cela étant précisé, alors que l'article 3, 11° se réfère simplement au concept de « réseaux de communications électroniques » de la LCE, le concept d'opérateur tel que proposé reprend lui le concept de « réseau *public* de communications électroniques » (italiques ajoutés par le Comité permanent R), sans toutefois renvoyer à la définition de ce concept dans l'article 2, 10° de la LCE. L'article 9, § 7 actuel de la LCE, repris dans l'article 13 du projet soumis pour avis qui crée un article 127/4 de la LCE se réfère quant à lui à des données conservées par des « réseaux *privés* de communications électroniques et de services de communications électroniques *qui ne sont pas accessibles au public* » (italiques ajoutés par le Comité permanent R).

Dans ce contexte, le Comité permanent R d'une part, n'est toutefois pas en mesure d'identifier ce que revêt le concept de réseau « privé » de communications électroniques (quels réseaux sont concrètement visés : des réseaux d'entreprises ?[46]), et ne perçoit pas non plus d'autre part, quels fournisseurs de réseaux de communications électroniques l'auteur du projet entend finalement viser dans la L.R&S.

Autrement dit, l'article 3, 10/1° tel qu'inséré par le projet et son exposé des motifs doivent être adaptés, de même que, le cas échéant, l'article 3, 11° de la L.R&S.

Dit gezegd zijnde, terwijl artikel 3, 11° simpelweg verwijst naar het begrip "elektronische communicatienetwerken" van de Telecomwet, neemt het begrip operator zoals voorgesteld het begrip "*openbaar elektronisch communicatienetwerk*" over (cursief toegevoegd door het Vast Comité I), zonder evenwel te verwijzen naar de definitie van dit begrip in artikel 2, 10° WEC. In het huidige artikel 9, §7, WEC, dat is overgenomen in artikel 13 van het voor advies voorgelegde ontwerp, waarbij een artikel 127/4 WEC wordt ingevoerd, wordt verwezen naar gegevens die zijn opgeslagen door "*niet voor het publiek toegankelijke private* elektronische-communicatienetwerken en elektronische-communicatiediensten" (cursivering toegevoegd door het Vast Comité I).

In dit verband kan het Vast Comité I echter niet vatten wat wordt bedoeld met het begrip "privaat" elektronisch communicatienetwerk (op welke netwerken is het specifiek gericht: bedrijfsnetwerken?[47]), en ziet het evenmin op welke aanbieders van elektronische communicatienetwerken de opsteller van het ontwerp zich in de W.I&V wil richten.

Met andere woorden, artikel 3, 10/1°, zoals ingevoegd bij het ontwerp en de memorie van toelichting daarbij, moet worden aangepast, evenals, in voorkomend geval, artikel 3, 11°, van de W.I&V.

---

[46] Il convient de souligner en passant, que la délégation au Roi prévue par ces dispositions (l'article 9, § 7 de la LCE et l'article 127/4 de la LCE en projet) n'apparaît pas conforme aux principes de transparence et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution. Parmi les réseaux qui ne sont pas accessibles au public, en droit des communications électroniques, pourraient être évoqués les réseaux internes d'entreprise et l'accès à internet offert par les cafés et restaurants, voir Body of Europeans Regulators for Electronic Communications, BEREC Guidelines on the Implementation of the Open Internet Regulation, BOR (20) 112, paragraphe 12, disponible sur https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation, dernièrement consulté le 20 mai 2021. Il va sans dire que le Comité permanent R comprend que l'objectif n'est pas de viser les réseaux domestiques des particuliers.

[47] Terloops zij erop gewezen dat de delegatie aan de Koning waarin deze bepalingen voorzien (artikel 9, lid 7, van het WEC en artikel 127/4 van het ontwerp-WEC), niet in overeenstemming lijkt te zijn met de beginselen van transparantie en wettigheid die zijn neergelegd in artikel 8 EVRM en artikel 22 van de Grondwet. Van de netwerken die krachtens de wetgeving inzake elektronische communicatie niet voor het publiek toegankelijk zijn, kunnen worden genoemd de interne bedrijfsnetwerken en de internettoegang die wordt aangeboden door cafés en restaurants, zie Body of European Regulators for Electronic Communications, BEREC Guidelines on the Implementation of the Open Internet Regulation, BOR (20) 112, paragraaf 12, beschikbaar op https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation, laatst geraadpleegd op 20 mei 2021. Het spreekt vanzelf dat het Vast Comité I begrijpt dat het niet de bedoeling is thuisnetwerken te viseren.

Concept de 'facture'

33. L'article 27, 3° du projet de loi instaure la compétence de réclamer aux opérateurs de télécommunications *« des factures afférentes aux abonnements identifiés ».* L'exposé des motifs indique à ce propos que *« (p)ar ailleurs, il est ajouté à l'article 18/7 que les services de renseignement peuvent également demander les factures relatives à un abonnement spécifique. Ces factures sont susceptibles de fournir des informations intéressantes, par exemple au sujet de la personne qui effectue le paiement, des moyens de communication qui y figurent, etc. »*
Et l'exposé des motifs de mentionner que :
« (c)ette possibilité existait avant la modification de l'article 18/7 par la loi du 5 février 2016 et avait disparu lors de cette modification. Elle est dès lors réinsérée. ».

Premièrement, le Comité note que le gouvernement ne donne aucune raison justifiant la réintroduction de cette possibilité. Le fait que les données de facturation *« fournissent des informations intéressantes »* ne constitue pas une raison de fond pour réintroduire la disposition en question cinq ans après sa suppression.

Deuxièmement, le Comité demande des précisions sur ce que le gouvernement entend par « données de facturation ».

Ce point doit être mis en perspective avec la question de la facturation dans le domaine des communications électroniques. Ainsi, il convient de souligner que les données de trafic – dont il n'est en principe pas question dans l'article 18/7 de la L.R&S – peuvent bien entendu être traitée à des fins de facturation. Or l'article 110 de la LCE prévoit que l'abonné a le droit à une facture « détaillée » dont le niveau de détail est fixé par le Ministre compétent.
Dans ce contexte, de deux choses l'une. Premièrement, vu la manière dont la facturation est régie dans le domaine des services de communications électroniques

Begrip 'factuur'

33. Artikel 27, 3° van het wetsontwerp creëert de bevoegdheid om *"de facturen met betrekking tot de geïdentificeerde abonnementen"* van de telecomoperatoren te vorderen. De memorie van toelichting stelt hierover: *"In artikel 18/7 wordt eveneens ingevoegd dat de inlichtingendiensten ook de facturen met betrekking tot een welbepaald abonnement kunnen opgevraagd worden. Deze facturen kunnen interessante informatie opleveren bijvoorbeeld over wie de betaling verricht, welke communicatiemiddelen op de factuur staan ed."*.
Eveneens vermeld de memorie: "*Deze mogelijkheid bestond voor de wijziging van artikel 18/7 door de wet van 5 februari 2016, maar werd geschrapt door voornoemde wijziging. Daarom is het opnieuw ingevoerd."*.

Vooreerst merkt het Comité op dat de regering geen reden geeft waarom deze mogelijkheid wordt heringevoerd. Dat facturatiegegevens *"interessante informatie opleveren"* vormt immers geen inhoudelijke reden waarom betrokken bepaling, nadat ze eerst werd geschrapt, vijf jaar later opnieuw wordt ingevoerd.

Ten tweede vraagt het Comité om nader te bepalen wat de regering bedoelt met betrokken facturatiegegevens.

Dit aspect moet worden bekeken vanuit de facturering op het gebied van elektronische communicatie. Zo moet worden benadrukt dat verkeersgegevens – die in beginsel niet onder artikel 18/7 W.I&V vallen – uiteraard voor factureringsdoeleinden kunnen worden verwerkt. Artikel 110 WEC bepaalt dat de abonnee recht heeft op een "gespecificeerde" factuur, waarvan de mate van gedetailleerdheid wordt bepaald door de bevoegde minister.
In dit verband zijn twee dingen duidelijk. In de eerste plaats is het, gelet op de wijze waarop de facturering is geregeld op het gebied van de onder de WEC vallende elektronische communicatiediensten, *in fine* de voor dit

relevant de la LCE, c'est *in fine* le Ministre compétent en ce domaine qui déterminera les données qui doivent être reprises sur la facture détaillée.
Deuxièmement, le Comité permanent R n'est pas en mesure d'identifier si et dans quelle mesure les "factures" sont susceptibles de reprendre le détail de données de trafic. Or les données de trafic sont en principe visées par l'article *18/8* de la L.R&S. L'exposé des motifs semble bien confirmer que les factures sont susceptibles de reprendre des données de trafic : *"Par exemple, en matière de facturation détaillée, l'IBPT doit être en mesure de demander à l'opérateur de lui fournir un échantillon de factures. Or, ces factures reprennent des données de trafic, telles que les destinataires, dates, heures et durées des communications passées."*.[48]

gebied bevoegde minister die bepaalt welke gegevens moeten worden opgenomen in de gespecificeerde factuur.
Ten tweede is het Comité niet in staat vast te stellen of en in welke mate de "facturen" mogelijkerwijze details over verkeersgegevens zullen bevatten. Verkeersgegevens vallen in beginsel onder artikel 18/8 W.I&V. De memorie van toelichting lijkt te bevestigen dat de facturen waarschijnlijk verkeersgegevens zullen bevatten: *"Wat bijvoorbeeld de gespecificeerde facturering betreft, moet het BIPT aan de operator kunnen vragen om hem een steekproef van facturen te bezorgen. Deze facturen bevatten echter verkeersgegevens, zoals de ontvangers, data, tijdstippen en duur van de gevoerde gesprekken."*.[49]

NOTIFICATION OBLIGATOIRE OPÉRATEURS

34. Le Comité recommande de créer une obligation pour les services de renseignement d'informer les opérateurs concernés lorsque le Comité permanent R a ordonné la cessation d'une conservation généralisée et indifférenciée ou d'une conservation ciblée. Étant donné qu'une telle procédure n'est pas spécifique à une catégorie de méthodes, un nouvel article 18/19 L.R&S serait inséré.

VERPLICHTE KENNISGEVING OPERATOREN

34. Het Comité beveelt aan om een verplichting in hoofde van de inlichtingendiensten te creëren om de betrokken operatoren op de hoogte te brengen wanneer het Vast Comité I de stopzetting van een algemene en ongedifferentieerde bewaring of van een gerichte bewaring heeft bevolen. Gezien een dergelijke procedure niet eigen is aan een categorie van methoden, zou hierbij een nieuw artikel 18/19 W.I&V ingevoegd worden.

AMÉLIORATIONS TEXTUELLES LOI RENSEIGNEMENT

35. À l'article 27, 1° du projet de loi, une amélioration textuelle est proposée à la phrase introductive de l'article 18/7 L.R&S. Plus précisément, les mots *« Dans l'intérêt de l'exercice des missions, le dirigeant du service peut, par une décision écrite »* sont remplacés par *« Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent (…) ».* Le Comité reconnaît qu'une telle modification textuelle ne change

TEKSTUELE VERBETERINGEN INLICHTINGENWET

35. In artikel 27, 1° van het wetsontwerp wordt een tekstuele verbetering voorgesteld aan de inleidende zin van artikel 18/7 W.I&V. Meer in het bijzonder worden de woorden *"In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing,"* vervangen door de woorden *"De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,"*. Het

[48] EdM, pag. 90.
[49] MvT, pag. 90.

pas le contenu et peut améliorer la lisibilité de la Loi relative aux services de renseignement. Le Comité recommande d'apporter également une telle amélioration à la version néerlandaise des articles 18/14 § 1er, 18/15 § 1er, et 18/17 § 1er L.R&S.

Comité erkent dat een dergelijke tekstuele wijziging geen inhoudelijke wijzigingen teweegbrengt en de leesbaarheid van de Inlichtingenwet ten goede kan komen. Het Comité beveelt aan om een dergelijke verbetering eveneens aan te brengen in de Nederlandstalige versie van de artikelen 18/14 §1, 18/15 §1 en 18/17 §1 W.I&V.

B. Modifications à la Loi Télécom

36. L'exposé des motifs du projet d'article 126/1, § 3, 2° LCE stipule que *« (u)ne conservation ciblée des données est prévue en cas de menace grave, réelle et actuelle pour la sécurité nationale. Cette menace est établie par l'OCAM en cas de niveau de la menace 3 ou 4. ».* Le projet de disposition lui-même introduit une conservation ciblée des données sur la base d'un critère géographique, c'est-à-dire pour : *« (t)outes les zones dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones ».*

Le Comité demande que soit précisée la notion de « zones » dans cette disposition. En effet, il n'est pas clair si – comme dans le projet d'article 126/1, § 3, 1° LCE – il s'agit des « arrondissements judiciaires » ou des « zones de police », ou si – comme dans le projet d'article 126/1, § 3, 3° – il s'agit de certaines « zones » (par exemple, les installations portuaires, les gares, les aéroports, les prisons, etc.), ou si la notion de « zone » a une définition spécifique. Dans ce dernier cas, le Comité recommande de clarifier davantage cette interprétation spécifique.

De manière plus générale, le Comité recommande que les mots *« en cas de menace grave, réelle et actuelle »* soit inscrit dans le dispositif même.

B. Wijzigingen aan de Telecomwet

36. De memorie van toelichting bij het ontworpen artikel 126/1, §3, 2° WEC bepaalt dat *"(e)r (…) in een gerichte bewaring (wordt) voorzien in geval van ernstige, reële en actuele bedreiging voor de nationale veiligheid."*. "*Deze bedreiging wordt vastgelegd door het OCAM in geval van dreigingsniveau 3 of 4."*. De ontworpen bepaling zelf voert een gerichte gegevensbewaring in op grond van een geografisch criterium, zijnde voor: *"(a)lle zones waar het algemeen dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2° van de wet van 10 juli 2006 betreffende de dreigingsanalyse, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de dreiging, en zolang niveau 3 blijft bestaan"*.

Het Comité vraagt om het begrip "zones" in deze bepaling nader te verduidelijken. Het is immers niet duidelijk of het hier – net zoals in het ontworpen artikel 126/1, §3, 1° WEC – gaat om "gerechtelijke arrondissementen" of "politiezones", of – zoals in het ontworpen artikel 126/1, §3, 3° WEC – om bepaalde "gebieden" (bv. havenfaciliteiten, spoorwegstations, luchthavens, gevangenissen, edm.), of als begrip "zone" een eigen, specifieke omschrijving heeft. In dit laatste geval beveelt het Comité aan om deze specifieke invulling nader te verduidelijken.

Meer algemeen beveelt het Comité aan om de woorden "*in geval van een ernstige, reëel en actuele dreiging"* in te schrijven in het dispositief zelf.

37. En vertu du projet d'article 126/1, § 3, 4°, b) LCE[50], les services de renseignement sont chargés d'établir une liste annuelle *« (d)es bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé »*, qui doit être approuvée par le Conseil national de sécurité sur proposition des ministres de la Justice et de la Défense. Cette liste est tenue à la disposition du Comité permanent R (*cf.* projet d'article 126/1, § 3, 5°, alinéa 5, LCE).

37. Krachtens het ontworpen artikel 126/1, §3, 4°, b) WEC[51] worden de inlichtingendiensten belast met het jaarlijks opstellen van een lijst van *"de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden"* en die op voorstel van de ministers van Justitie en Defensie dient goedgekeurd te worden door de Nationale Veiligheidsraad. Deze lijst wordt ter beschikking gehouden van het Vast Comité I (*cf*. ontworpen artikel 126/1, §3, 5°, vijfde lid WEC).

Le Comité rappelle au gouvernement l'existence du Plan d'action du gouvernement fédéral pour la sauvegarde du potentiel scientifique et économique, approuvé le 16 mars 2007 par le Comité ministériel du renseignement et de la sécurité (actuellement : le Conseil national de sécurité), en abrégé : Plan PES. Ce plan d'action contient également une liste d'entités. À ce jour, cette liste – établie en 2007 – n'a pas été actualisée. À la lumière de cette constatation, le Comité se demande si une mise à jour annuelle de la liste prévue par le projet de loi est réaliste. Il est également important de noter que, contrairement au plan d'action PES, la liste prévue par le projet de loi doit servir de base à une conservation étendue des données.

Het Comité brengt de regering in herinnering van het bestaan van het Actieplan van de federale regering tot vrijwaring van het wetenschappelijk en economisch potentieel, op 16 maart 2007 goedgekeurd door het Ministerieel Comité voor inlichting en veiligheid (heden: de Nationale Veiligheidsraad), afgekort: het Plan WEP. Ook dit actieplan bevat een lijst van entiteiten. Tot op heden kende deze lijst – gemaakt in 2007 – geen actualisering. In het licht van deze vaststelling stelt het Comité de vraag of een jaarlijkse actualisering van de lijst voorzien in het wetsontwerp realistisch is. Hierbij is het daarenboven van belang dat, in tegenstelling tot het Actieplan WEP, de in het wetsontwerp bedoelde lijst als grondslag dienst moet doen voor een verregaande gegevensbewaring.

38. Le Comité constate que le gouvernement introduit une notification obligatoire par la Police fédérale au C.O.C. des statistiques criminelles annuelles qui doit justifier la conservation ciblée sur une base géographique par le biais d'infractions criminelles.

38. Het Comité stelt vast dat de regering in een verplichte kennisgeving instelt in hoofde van de federale politie aan het COC wat betreft de jaarlijkse criminele statistieken die de gerichte bewaring op geografische basis via strafbare feiten moet rechtvaardigen.

Le Comité constate cependant que la même obligation de notification fait défaut dans le

Het Comité stelt echter vast dat eenzelfde verplichte kennisgeving ontbreekt in het

[50] Dans la disposition concernée, les mots « *la Sûreté de l'Etat et le Service général du Renseignement et de la sécurité* » doivent être remplacés par « *la Sûreté de l'Etat et le Service Général du Renseignement et de la Sécurité* ».

[51] In betrokken bepalen moeten de woorden *"de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst"* vervangen worden door *"de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid"*.

projet d'article 126/1, § 3, 2° LCE, selon lequel la conservation géographique ciblée est effectuée sur la base du niveau de menace général tel que déterminé par l'Organe de coordination de l'analyse de la menace (OCAM). Le Comité rappelle au gouvernement que le Comité permanent R et le Comité permanent P sont, conjointement, les autorités de protection des données compétentes vis-à-vis de l'OCAM. Le Comité recommande d'établir une obligation de notification similaire (au moins) pour le Comité permanent R. Le Comité recommande également d'interroger le Comité permanent P à cet égard.

ontworpen artikel 126/1, §3, 2° WEC waarbij de gerichte geografische bewaring gebeurt op grond het algemene dreigingsniveau zoals bepaald door het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Het Comité herinnert er de regering aan dat het Vast Comité I en het Vast Comité P, gezamenlijk, de bevoegde gegevensbeschermingsautoriteiten zijn tegenover het OCAD. Het Comité beveelt aan om eenzelfde kennisgevingsplicht in te richten (minstens) aan het Vast Comité I. Verder beveelt het Comité aan om hieromtrent eveneens het Vast Comité P te bevragen.

39. Le Comité apprend que, conformément au projet d'article 126/1 § 6 LCE, il est chargé, en sa qualité d'autorité de protection des données compétente, d'émettre un avis dans le cadre de l'évaluation annuelle que les ministres compétents doivent transmettre à la Chambre des représentants. Le Comité souhaite obtenir des précisions sur la portée exacte de cette nouvelle mission.

39. Het Comité leert dat ze, krachtens het ontworpen artikel 126/1, §6 WEC, vanuit haar hoedanigheid van bevoegde gegevensbeschermingsautoriteit, belast wordt om een advies te verstrekken in het kader van de jaarlijkse evaluatie dat de bevoegde ministers moeten overmaken aan de Kamer van volksvertegenwoordigers. Het Comité behoeft nadere verduidelijking over de precieze draagwijdte van deze nieuwe opdracht.

40. L'actuelle Loi Télécom stipule que les membres de la Cellule de coordination des opérateurs doivent être titulaires d'un avis de sécurité positif (*cf.* l'actuel article 126/1, § 1er, alinéa 3, 1° LCE). En vertu du projet d'article 127/3, § 3, 2° et 3°, une telle obligation ne sera plus établie par la loi, mais la possibilité d'imposer un tel screening de sécurité sera créée par arrêté royal.

40. De huidige Telecomwet voorziet dat de leden van de Coördinatiecel van de operatoren houder moeten zijn van een positief veiligheidsadvies (*cf*. huidig art. 126/1, §1, derde lid, 1° WEC). Krachtens het ontworpen artikel 127/3, §3, 2° en 3° wordt een dergelijke verplichting niet langer op wettelijk niveau vastgelegd maar wordt de mogelijkheid gecreëerd om een dergelijke veiligheidsscreening op te leggen per koninklijk besluit.

Le Comité souhaite tout d'abord souligner qu'il existe une contradiction entre le projet de loi et l'exposé des motifs. Ce dernier indique en effet que : *« les membres de cette cellule sont « screenés (vérification de sécurité[52]) avant de rejoindre cette cellule ».[53]*

Vooreerst wens het Comité onder de aandacht te brengen dat er een tegenstrijdigheid bestaat tussen het wetsontwerp en de memorie van toelichting. Laatstgenoemde stelt immers: *"de leden van deze eenheid worden gescreend (veiligheidscontrole[54])*

[52] Conformément à la Loi du 11 décembre 1198, la notion de *« vérification de sécurité »* doit d'ailleurs être traduite par *« veiligheidsverificatie »*. Cette dernière notion revêt une signification spécifique avec des conséquences juridiques adéquates.

[53] Exposé des motifs, p. 9.

[54] Het begrip *"vérification de sécurité"* dient, overeenkomstig de wet van 11 december 1998, overigens vertaald te worden als *"veiligheidsverificatie"*. Laatstgenoemde begrip heeft een specifieke betekenis met geëigende juridische gevolgen.

Il en ressort clairement que la loi impose l'obligation, et non que le Roi peut imposer un screening de sécurité.

Deuxièmement, le Comité recommande de maintenir la situation actuelle, c'est-à-dire l'obligation imposée par la loi aux collaborateurs des Cellules de coordination de se soumettre à des avis et vérifications de sécurité. Le Comité estime que, compte tenu de l'accès à des données (très) sensibles, il y a lieu de décrire l'appartenance à une telle entité comme une fonction sensible qui justifie donc un screening de sécurité.

Enfin, le Comité recommande que le projet d'article 127/3 § 3 LCE non seulement rende obligatoires les avis et vérification de sécurité, mais stipule également que la validité d'un tel avis de sécurité n'est que de cinq ans, et que cet avis peut être modifié à tout moment en raison d'antécédents problématiques. De telles modifications garantissent le respect de la réglementation générale relative aux avis et vérifications de sécurité, telle qu'elle figure à l'article 22*quinquies* de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

41. Enfin, le Comité recommande que les mots *« des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité »* dans le projet d'article 127/4, alinéa 1er LCE, soient remplacés par *« des missions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité »*. La disposition précitée charge le Roi d'établir des modalités relatives à la conservation des données d'identification. Le Comité rappelle que la formulation actuelle peut être synonyme d'une limitation pour la compétence des services de renseignement de requérir la conservation de ces données, telle que visée à l'article 16/2 L.R&S, une compétence qui n'est pas limitée aux activités de renseignement. Le projet d'article 127/4,

voordat zij tot de eenheid toetreden".[55] Hieruit blijkt duidelijk dat de wet de verplichting oplegt, niet dat de Koning een veiligheidsscreening kan opleggen.

Ten tweede beveelt het Comité aan om de actuele situatie te behouden, zijnde een in de wet opgelegde verplichting voor medewerkers van de Coördinatiecellen om onderworpen te worden aan een veiligheidsadvies en -verificatie. Het Comité is de mening toebedeeld dat het lidmaatschap van een dergelijke entiteit, gelet op de toegang tot (zeer) gevoelige gegevens, omschreven dient te worden als een gevoelige functie die derhalve een veiligheidsscreening rechtvaardigt.

Tot slot beveelt het Comité aan om – in het ontworpen artikel 127/3, §3 WEC – niet enkel een veiligheidsadvies en -verificatie op te leggen, maar tevens te stellen dat een dergelijk veiligheidsadvies slechts vijf jaar geldig is alsook te allen tijde gewijzigd kan worden wegens problematische antecedenten. Dergelijke wijzingen zorgen ervoor dat de algemene regeling m.b.t. veiligheidsadviezen en -verificatie bedoeld in artikel 22*quinquies* van de Classificatiewet van 11 december 1998 wordt nageleefd.

41. Tot slot adviseert het Comité om de woorden *"de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houden regeling van de inlichtingen- en veiligheidsdiensten"* in het ontworpen artikel 127/4, eerste lid WEC te vervangen *door "de opdrachten bepaald in de wet van 30 november 1998 houden regeling van de inlichtingen- en veiligheidsdiensten"*. Vernoemde bepaling geeft de Koning de opdracht om nadere regels uit te werken rond de bewaring van identificatiegegevens. Het Comité brengt in herinnering dat de actuele bewoording een beperking kan betekenen voor de vorderingsbevoegdheid van de inlichtingendiensten van dergelijke gegevens bedoeld in artikel 16/2 W.I&V, een bevoegdheid die zich niet beperkt tot inlichtingenopdrachten. Het ontworpen

[55] Memorie van toelichting, pag. 9.

alinéa 1er LCE est d'ailleurs la seule disposition qui limite le traitement de ces données à un certain type de missions des services de renseignement. Le Comité estime que de telles limitations – si elles sont déjà souhaitables ici – doivent être prévues dans la Loi relative aux services de renseignement.

artikel 127/4, eerste lid WEC is overigens de enige bepaling waarin de verwerking van deze gegevens beperkt wordt tot een bepaald type van opdrachten van de inlichtingendiensten. Het Comité is van oordeel dat dergelijke beperkingen – indien ze al in deze gewenst mogen zijn – moeten bepaald worden in de Inlichtingenwet.

Bruxelles, le 15 juin 2021

POUR LE COMITÉ PERMANENT R
Président
Greffier f.f.

Brussel, 15 juni 2021

VOOR HET VAST COMITÉ I
Voorzitter
Griffier d.d.

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 108/2021 du 28 juin 2021

Objet : Demande d'avis concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (CO-A-2021-099)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Madame Alexandra Jaspar et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Frank Robben ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA ») ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis du Ministre de la Justice, Monsieur Vincent Van Quickenborne, reçue le 7 mai 2021 ;

Vu les informations complémentaires transmises les 1er et 8 juin 2021 ;

Vu le rapport d'Alexandra Jaspar ;

Émet, le 28 juin 2021, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Ministre de la Justice, Monsieur Vincent Van Quickenborne (ci-après « le demandeur ») a sollicité, le 7 mai 2021, l'avis de l'Autorité concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités (ci-après « l'avant-projet de loi ») et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après « le projet d'arrêté »).

2. L'avant-projet de loi vise, comme le souligne son Exposé des Motifs, *« à répondre à l'annulation par la Cour constitutionnelle dans son arrêt n° 57/2021 du 22 avril 2021 des articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques'* » (ci-après « la loi du 29 mai 2016 »).

3. Cette loi du 29 mai 2016 prévoyait, comme le rappelle l'Exposé des motifs de l'avant-projet, « *l'obligation pour les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet et de courrier électronique par Internet (qu'ils soient opérateurs notifiés à l'IBPT ou non) de conserver certaines catégories de données de localisation et de trafic pendant une durée de 12 mois essentiellement afin que ces données soient disponibles pour des finalités répressives et en particulier pour les enquêtes pénales* ». Cette loi imposait ainsi une obligation de conservation généralisée et indifférenciée de certaines données de trafic et de localisation. Elle a été annulée par la Cour constitutionnelle en raison de sa contrariété avec l'article 15 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après « la Directive ePrivacy »), lu à la lumière des articles 7 et 8, ainsi que de l'article 52 § 1 de la Charte des droits fondamentaux de l'Union européenne, en combinaison avec les articles 10 et 11 de la Constitution. L'annulation de la Cour constitutionnelle est très largement motivée par un renvoi à l'arrêt que la Cour de justice de l'Union européenne (ci-après « la CJUE ») a rendu à la suite des questions préjudicielles posées, notamment, par la Cour constitutionnelle concernant l'interprétation à donner à l'article 15 de la Directive ePrivacy[1].

4. L'avant-projet entend mettre en place un système de conservation des données de communication qui respecte les exigences imposées par la CJUE. Pour ce faire, il entend modifier la loi du 13 juin 2005 relative aux communications électroniques (ci-après « la loi télécom »), le Code d'instruction criminelle (ci-après « le CIC »), la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (ci-après « la loi statut IBPT »), la loi du 5 août 1992 sur la fonction

[1] CJUE, arrêt du 6 octobre 2020, aff. Jointes C-511/18, C-512/18 et C-520/18 (affaire dite de « La Quadrature du Net »). Cet arrêt de la CJUE a été rendu à la suite notamment des questions préjudicielles posées par la Cour constitutionnelle dans son arrêt n° 96/2018 du 19 juillet 2018.

de police (ci-après « la loi sur la fonction de police »), la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après « la loi sur les services de renseignement »), la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers (ci-après « la loi FSMA »), la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits (ci-après « la loi relative à la protection de la santé des consommateurs ») et la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après « la loi NIS »).

5. Le projet d'arrêté, pour sa part, exécute certaines habilitations législatives contenues dans l'avant-projet.

II. EXAMEN DE LA DEMANDE D'AVIS

6. Dans son avis, l'Autorité commence par identifier les dispositions de la Directive ePrivacy qui sont transposées par l'avant-projet de loi (A). Elle poursuit en présentant le « système » que l'avant-projet de loi entend mettre en place concernant la conservation des données de trafic et de localisation par les opérateurs et leur accès par différentes autorités (B). L'Autorité rappelle, ensuite, les exigences auxquelles doivent répondre les normes qui prévoient une conservation des données de trafic et/ou de localisation (et leur communication éventuelle aux autorités) (C). Enfin, l'Autorité examine la conformité de l'avant-projet de loi et du projet d'arrêté avec ces exigences (D).

7. À toutes fins utiles, l'Autorité souligne qu'elle se prononce uniquement sur les dispositions pour lesquelles elle est compétente, à l'exclusion des dispositions qui relèvent de la compétence exclusive d'une autre autorité de contrôle. Pour rappel, c'est l'Organe de contrôle de l'information policière (ci-après « le COC ») qui est compétent pour l'examen des dispositions prévoyant des traitements de données à caractère personnel effectués par la police intégrée et c'est le Comité permanent de contrôle des services de renseignement et de sécurité (ci-après « le Comité R ») qui est compétent pour l'examen des dispositions qui prévoient des traitements de données effectués par les services de renseignement et de sécurité.

A. LES DISPOSITIONS PERTINENTES DE LA DIRECTIVE ePRIVACY

8. La directive ePrivacy, qui précise et complète le RGPD en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, entend protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies.

9. L'avant-projet de loi transpose certaines dispositions de cette directive, et en particulier ses articles 5, 6, 9 et 15. À des fins de lisibilité et de clarté, l'Autorité reprend ces dispositions ci-dessous.

10. **L'article 5.1 de la Directive ePrivacy** impose aux Etats de garantir « *la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité* »[2].

11. **L'article 6.1 de la Directive ePrivacy rappelle et précise la portée du principe de la confidentialité des données relatives au trafic** : « *Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1* »[3].

12. **L'article 6.2 de la Directive ePrivacy** autorise le traitement des données relatives au trafic « *qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement* »[4].

13. **L'article 6.3 de la Directive ePrivacy** autorise le fournisseur d'un service de communications électronique accessible au public à traiter les données relatives au trafic « *dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de [de services de communications électroniques ou de fournir des services à valeur ajouté], pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic* »[5].

14. **L'article 6.5 de la Directive ePrivacy** dispose que *« Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes*

[2] C'est l'Autorité qui souligne
[3] C'est l'Autorité qui souligne.
[4] C'est l'Autorité qui souligne.
[5] C'est l'Autorité qui souligne.

agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités » alors que **l'article 6.6 de cette même Directive** indique que « *Les paragraphes 1, 2, 3 et 5 s'appliquent sans préjudice de la possibilité qu'ont les organes compétents de se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation* ».

15. **L'article 9.1 de la Directive ePrivacy** dispose que « *Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou, moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. […]* »[6].

16. Aux termes de **l'article 9.3 de la Directive ePrivacy**, « *Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée* ».

17. **L'article 15.1 de la Directive ePrivacy** se lit comme suit : « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, […] et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent*

[6] C'est l'Autorité qui souligne.

paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne »[7].

B. PRESENTATION DU « SYSTEME » PROPOSE PAR L'AVANT-PROJET DE LOI CONCERNANT LA CONSERVATION DES DONNEES DE COMMUNICATION PAR LES OPERATEURS TELECOM ET LEURS COMMUNICATIONS EVENTUELLES AUX AUTORITES[8]

❖ *Quant aux données qui peuvent ou doivent être conservées par les opérateurs*

18. Plusieurs dispositions de la loi télécom, que l'avant-projet de loi prévoit de modifier, permettent ou imposent la conservation, par les opérateurs, des données de trafic et/ou de localisation (y compris des données de localisation autres que des données de trafic), et ce pour différentes finalités :

1) Les opérateurs **peuvent** conserver et traiter **les données de trafic nécessaires à l'établissement des factures des abonnés** ou **celles qui sont nécessaires aux paiements d'interconnexion** (**nouvel article 122 § 2** de la loi télécom[9])[10].

Ces données peuvent être conservées *« **jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement** »* (nouvel article 122 § 2, dernier alinéa, de la loi télécom).

La loi télécom donne uniquement une **définition fonctionnelle des données qui peuvent être conservées** : les données de trafic nécessaires à l'établissement de la facture de l'abonné ou au paiement d'interconnexion. Au contraire de ce qui est prévu dans la version actuelle de l'article 122 § 2 de la loi télécom, la nouvelle version de cette

[7] C'est l'Autorité qui souligne. L'article 6 §§ 1 et 2 du traité sur l'Union européenne se lit comme suit : « *1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités […].*
2. L'Union adhère à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales […] ».
[8] L'Autorité a synthétisé ce système dans un tableau repris dans l'Annexe II.
[9] L'article 122 § 2 de la loi télécom transpose l'article 6 § 2 de la Directive ePrivacy.
[10] La version actuelle de l'article 122 § 2 de la loi télécom impose – au lieu d'autoriser – aux opérateurs de conserver des données de trafic dans le but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion. Cet article prévoira à l'avenir uniquement une possibilité pour les opérateurs. Le passage d'une obligation de conservation vers une possibilité est justifiée comme suit dans l'Exposé des motifs : *« D'une part, une obligation n'est pas nécessaire, étant donné que les opérateurs ont tout intérêt à conserver ces données pour ces finalités et qu'il découle de l'article 110 de la [loi télécom], à tout le moins indirectement, que ces données doivent être disponibles [l'article 110 de la loi télécom impose aux opérateurs de fournir une facture détaillée de base aux abonnés et permet aux abonnés d'obtenir gratuitement, sur simple demande, une version plus détaillée de la facture de base qu'ils ont reçue]. D'autre part, cette modification permet de se rapprocher de l'article 6, § 2, de la directive [ePrivacy] que l'article 122, § 2 transpose. Cet article 6, § 2, prévoit que, par dérogation au principe de suppression ou d'anonymisation, les données de trafic peuvent être traitées à des fins de facturation »*

disposition ne détermine plus les catégories de données de trafic précises qui peuvent être conservées à cette fin[11].

2) Les opérateurs **peuvent traiter des données de trafic nécessaires** afin (i) d'assurer le **marketing des services de communications électroniques propres** et (ii) **d'établir le profil d'utilisation de l'abonné** ou de l'utilisateur final[12]**, à condition d'avoir obtenu le consentement** de l'abonné ou, le cas échéant, de l'utilisateur final (**nouvel article 122 § 3** de la loi télécom)[13]

3) Les opérateurs **doivent conserver** des **données de localisation et d'autres des données de trafic nécessaires** afin de **détecter et d'analyser une fraude présumée[14]** ou **une utilisation malveillante présumée[15]** du réseau de communications électroniques (**nouvel article 122 § 4** de la loi télécom).

Cette disposition prévoit que **les données de localisation et les autres données de trafic nécessaires** afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communications électroniques **doivent être conservées pour minimum 4 mois,** mais qu'elles **peuvent être conservées pour une durée plus longue** si cela est nécessaire (sans autre précision).

Les **données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles**[16] doivent, pour leur part, être **conservées pendant 12 mois.**

---

[11] Dans l'Exposé des motifs, cette suppression de la liste des données de trafic qui devaient être conservées en application de l'article 122 § 2 de la loi télécom est justifiée comme suit : « *La liste des données de trafic que les opérateurs devaient traiter selon l'article 122, § 2, est supprimée, étant donné que cette liste n'est plus adaptée aux différents services de communications électroniques offerts par les opérateurs. Cette liste était surtout pertinente pour le service de téléphonie fixe […]* ».

[12] Plusieurs dispositions de la loi télécom prévoient la possibilité pour les opérateurs d'établir des profils d'utilisation des abonnés et/ou des consommateurs ou utilisateurs finaux afin de leur permettre de déterminer le plan tarifaire le plus avantageux pour eux : article 110, § 4, alinéa premier, article 110/1 et article 111, § 3, alinéa 2 de la loi télécom.

[13] L'article 122 § 3 de la loi télécom transpose l'article 6 § 3 de la Directive ePrivacy.

[14] La notion de fraude est définie par le nouvel article 122 § 4, alinéa 1er, de la loi télécom comme suit : *« un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite, commis par le biais de l'utilisation d'un service de communications électroniques* »

[15] La notion d'utilisation malveillante du réseau est définie par le nouvel article 122 § 4, alinéa 2, de la loi télécom comme suit : « *une utilisation du réseau afin d'importuner son correspondant ou de provoquer des dommages* ».

[16] La notion de « service de communications interpersonnelles » est issue du nouveau Code des communications électroniques européen (établi par la Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018). Cette notion y est définie comme suit : « *un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service* » (article 2.5) de la Directive établissant le Code des communications électroniques européen).

Aux termes du nouvel article 122 § 4 de la loi télécom**, le Roi peut – mais ne doit pas – déterminer les données de trafic qui doivent être conservées** sur pied de cette disposition.

4) Les opérateurs **doivent conserver**, pour **minimum 12 mois**[17], les **données de trafic** nécessaires **pour assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques**, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte (**nouvel article 122 § 4/1** de la loi télécom).

   Cette disposition donne une **définition fonctionnelle des données qui doivent être conservées** : les données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement du réseau et des services de communication électroniques. Elle ne comprend **aucune définition des catégories précises de données** qui doivent être conservées et **n'habilite pas, non plus, le Roi à procéder à cette détermination**.

5) Les opérateurs **doivent conserver les données de trafic nécessaires** pour répondre à une **obligation légale** dans leur chef, pour la durée requise à cette fin (**nouvel article 122 § 4/2** de la LCE)[18].

6) Les **opérateurs de réseaux mobiles peuvent** conserver **des données de localisation autres que des données de trafic** dans les cas suivants (**nouvel article 123** de la loi télécom)[19] :

   - Lorsque cela **est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service**, les données étant conservées le temps nécessaire à cette fin ;
   - Lorsque cela est **nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau**, les données étant conservées le temps nécessaire à cette fin ;

[17] Le nouvel article 122 § 4/1 de la loi télécom indique que les données peuvent être conservées « *pour une durée plus longue, qui est limitée au strict nécessaire* ».
[18] Dans l'Exposé des Motifs, il est indiqué à ce sujet ce qui suit : « *Un opérateur doit pouvoir conserver des données de trafic pour répondre à ses obligations légales, comme par exemple la législation comptable ou fiscale ou pour répondre à une injonction d'une autorité de geler les données (également connu comme le « quick freeze »), qui se trouve par exemple dans le Code d'instruction criminelle. Ces obligations légales ne ressortent pas du présent paragraphe mais bien des législations spécifiques qui les prévoient. Cette disposition permet également de tenir compte des évolutions futures (nouvelles obligations*) ». L'Exposé des Motifs précise ensuite que « *Conformément à l'article 15, §1er de la directive « vie privée et communications électroniques » (directive 2002/58/CE), toute obligation légale de conservation de données de trafic doit être nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour atteindre la finalité poursuivie, et adoptée dans le respect des principes généraux du droit européen, en ce compris ceux visés par la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'homme* ».
[19] Cette disposition transpose partiellement l'article 9 de la Directive ePrivacy.

- Lorsque **les données ont été rendues anonymes** ;
- Lorsque **le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation** et que l'abonné ou, le cas échéant, l'utilisateur final, **y a donné son consentement** ;
- Lorsque **le traitement est nécessaire pour répondre à une obligation légale** dans le chef de l'opérateur.

7) Les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, **doivent conserver les données de souscription de l'abonné** ainsi que **les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé**, à l'exception des données qui sont liées à une seule communication électronique (**nouvel article 126** de la loi télécom).

Ces données – à l'exception des adresses IP dynamiques, autres que celle qui a été utilisée pour souscrire au service – **sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé** (nouvel article 126 de la loi télécom).

Les **adresses IP dynamiques**, autres que celle qui a été utilisée pour souscrire au service sont, pour leur part, **conservées pendant douze mois après la fin de la session** (nouvel article 126 de la loi télécom).

Le nouvel article 126 § 2 de la loi télécom **délègue au Roi** le soin de **fixer les données à conserver** ainsi que les exigences auxquelles ces données doivent répondre. **Les articles 3 § 1, 4 § 1, 5 § 1 et 6 § 1 de l'arrêté royal du 19 septembre 2013** portant exécution des articles 126 et 126/1 de la loi du 13 juin 2005 relative aux communications électroniques et des articles 16/2/1 et 18/17/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après « l'arrêté du 19 septembre 2013 »), tel que modifié par le projet d'arrêté, **exécute cette habilitation législative**.

8) Les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, **doivent conserver certaines données de trafic et de localisation des communications émises à partir de, ou vers, certaines zones géographiques déterminées, et ce, en principe, pour une durée de 12 mois**, à

moins qu'une autre durée soit précisée dans l'avant-projet de loi (**nouvel article 126/1** de la loi télécom).

Le nouvel article 126/1 § 1, alinéa 3, de la loi télécom précise que « *ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique* ».
Le nouvel article 126/1 § 2 de la loi télécom **détermine les catégories de données qui doivent être conservées** :

- Les **données relatives à l'accès et la connexion de l'équipement terminal** au réseau **et au service et à la localisation de cet équipement**, y compris le point de terminaison du réseau ;
- Les **données de communication**, à l'exclusion du contenu, en ce compris leur origine et leur destination ;
- Les **données des appels infructueux**, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés, générées ou traitées par les opérateurs (en ce qui concerne les données de la téléphonie) ou journalisées par les opérateurs (en ce qui concerne les données de l'internet).

Le **Roi doit fixer les données à conserver** et les exigences auxquelles ces données doivent répondre. **Les articles 3 § 2, 4 § 2, 5 § 2 et 6 § 2 de l'arrêté du 19 septembre 2013**, tel que modifié par le projet d'arrêté, **pourvoient à l'exécution** de cette habilitation.

Le nouvel article 126/1 § 3 de la loi télécom **détermine les zones géographiques** dans lesquelles les opérateurs doivent conserver les données visées au nouvel article 126/1 § 2 de la loi télécom. Il s'agit des zones géographiques suivantes :

1° **La zone géographique composée** :

- Des arrondissements judiciaires dans lesquels **au moins 3 infractions visées à l'article 90ter du CIC par 1000 habitants par an ont été constatées** durant l'année sur une moyenne des trois années calendrier précédant celle en cours
- **Des zones de police dans lesquelles, au moins 3 infractions visées à l'article 90ter du CIC par 1000 habitants par an ont été constatées** sur une moyenne des trois années calendrier précédant celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier précédant celle en cours, moins de 3 infractions visées à l'article

90ter du CIC par 1000 habitants par an sur une moyenne de trois années précédant celle en cours ont été constatées.

La **durée de conservation des données varie selon le nombre d'infractions visées à l'article 90ter du CIC par an par 1000 habitants constatées** sur une moyenne des trois dernières années calendriers précédant celle en cours. Au plus ce nombre est élevé, au plus la durée de conservation est longue (la loi télécom établit trois seuils : 6 mois s'il y a 3 ou 4 infractions visées à l'article 90ter du CIC par an par 1000 habitants, 9 mois s'il y a 5 ou 6 infractions visées à l'article 90ter du CIC par an par 1000 habitants ou 12 mois s'il y a 7 ou plus de 7 infractions visées à l'article 90ter du CIC par an par 1000 habitants).

2° **Toutes les zones dont le niveau de la menace terroriste ou extrémiste**, qui est déterminé par l'Organe de coordination pour l'analyse de la menace (ci-après « l'OCAM ») **est au moins de niveau 3**. Les données doivent **être conservées aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones**.

Dans l'Exposé des motifs, il est précisé que « *Dès lors qu'un niveau de la menace atteint le niveau 3 (menace possible et vraisemblable) et, a fortiori, 4 (menace sérieuse et imminente), une conservation des données visées au § 2 [de l'article 126/1] sur les zones géographiques visées est réalisée. Il peut dans certains cas (évaluation générale de la menace de niveau 3 ou 4) s'agir de l'ensemble du territoire* »[20].

3° **Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave**. L'avant-projet de loi liste 17 catégories de lieux.

4° **Les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population**. L'avant-projet liste 8 catégories de lieux (dont certaines avec des « sous-catégories » de lieux).

5° **Les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national**. L'avant-projet liste 6 catégories de lieux.

[20] Exposé des motifs, p. 52.

9) Les opérateurs **doivent conserver les données nécessaires pour que les autorités qui sont habilitées à obtenir l'identité des abonnés des opérateurs puissent les identifier** (**nouvel article 127** de la loi télécom).

Ces données « *sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé* » (nouvel article 127 de la loi télécom).

Cette disposition habilite (mais n'oblige pas) le Roi à déterminer les « *modalités d'identification* » de l'utilisateur final/abonné.

19. Par ailleurs, à côté des obligations de conservation préventive qui sont imposées aux opérateurs par la loi télécom, l'avant-projet de loi prévoit **d'insérer un article 39quinquies dans le CIC** afin de permettre **au procureur du Roi d'ordonner**, lors de la recherche de crimes et délits et s'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, **la conservation, pour une durée qu'il détermine, de certaines données de trafic et de localisation** pour les besoins de l'enquête (parmi les données visées à l'article 88bis, §1, alinéa 1er du CIC[21]). La conservation doit être limitée aux seules données qui sont susceptibles de contribuer à l'élucidation de l'infraction.

❖ Quant aux possibilités pour les autorités d'accéder aux données conservées par les opérateurs

20. Le **nouvel article 127/1 de la loi télécom** comprend, comme le souligne l'Exposé des Motifs, « *la liste des catégories d'autorités qui peuvent demander l'accès aux données d'identification, aux données de trafic et aux données de localisation conservées auprès des opérateurs en vertu des [articles 122, 123, 126, 126/1 et 127] au bénéfice des autorités, des utilisateurs finaux ou pour leurs propres besoin* ».

21. Cette disposition prévoit ainsi que :

> « *Seules les autorités suivantes peuvent obtenir […] des opérateurs des données conservées en vertu des articles 122, 123, 126, 126/1 et 127, pour les finalités ci-dessous et dans les conditions prévues par les dispositions qui les y habilitent :*
> *1° les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal,*

[21] Il s'agit des données suivantes : des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées et des données relatives à la localisation de l'origine ou de la destination de communications électroniques.

ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne ;
2° les services de renseignement et de sécurité afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;
3° les autorités chargées d'apporter de l'aide aux personnes, en ce compris le service de médiation pour les télécommunications pour ce qui concerne l'utilisation malveillante du réseau, les services d'urgence et la Cellule des personnes disparues de la Police Fédérale ;
4° l'Institut dans le cadre de la mise en œuvre et le contrôle de la présente loi ;
5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service ».

22. Pour déterminer à quelles données quelles autorités peuvent avoir accès et pourquoi (« **qui peut avoir accès à quoi et pourquoi ?** »), il faut, notamment, **lire le nouvel article 127/1** de la loi télécom **à la lumière des (nouvelles versions des) articles 122, 123, 126, 126/1 et 127 de la loi télécom** :

- Les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom[22] **peuvent avoir accès aux données conservées en vertu des** (nouvelles versions des) **articles 122, 123, 126 et 127 pour chacune des finalités énoncées par cet article 127/1** de la loi télécom. Les autorités compétentes pour poursuivre l'une des finalités énoncées par le nouvel article 127/1 de la loi télécom **peuvent donc avoir accès à toutes les données qui sont conservées en application des articles 122 et 123, 126 et 127 de la loi télécom**, même si leur conservation a initialement été autorisée ou imposée pour une autre finalité que celle qui est poursuivie par l'autorité qui veut obtenir l'accès auxdites données[23].

- Les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom **peuvent avoir accès aux données conservées en vertu du nouvel**

[22] Contrairement aux versions antérieures de la loi télécom, le nouvel article 127/1 reprend une liste des finalités pour lesquelles les autorités peuvent obtenir un accès aux données conservées, et non plus une liste d'autorités pouvant avoir accès aux données. L'Exposé des Motifs justifie ce changement de perspective comme suit : « *Cela permet d'assurer que la législation couvre les différents cas de figure et les évolutions futures. A cet égard, il convient de noter qu'il est rapidement apparu que la liste fermée des autorités visées à l'article 126, § 2 était incomplète. L'adaptation de cette liste fermée s'est révélée être un exercice difficile (par exemple car la loi est attaquée devant la Cour constitutionnelle et peut difficilement être modifiée) et très lent, alors que le fait pour une autorité de ne pas figurer sur la liste, alors que c'est nécessaire, provoque immédiatement des difficultés opérationnelles pour cette dernière. Les données d'identification et de souscription visées par les articles 126 et 127 sont des données basiques dont ont besoin un nombre non négligeable d'autorités. On peut s'attendre à ce que ce nombre augmente à l'avenir, étant donné la croissance du nombre d'infractions en ligne. Il est également très difficile de faire une liste exhaustive de toutes les dispositions légales qui permettent aux différentes autorités d'obtenir des opérateurs des données d'identification, de trafic ou de localisation* ».

[23] En effet, les nouveaux articles 122 § 7 et 123 § 6 de la loi télécom prévoient, chacun, que « *cet article [à savoir, respectivement, l'article 122 et l'article 123] ne porte pas préjudice à l'article 127/1* ». Le nouvel article 126 § 1, alinéa 3, prévoit que « Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1 » et le nouvel article 127 § 1, alinéa 2, prévoit que « *Ces données et documents sont conservés pour les autorités et les finalités visées à l'article 127/1* ».

article 126/1 de la loi télécom **uniquement pour les finalités pour lesquelles elles sont conservées**, à savoir aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique.

23. Il faut préciser, en outre, que pour qu'une autorité puisse obtenir des données de l'opérateur, il est nécessaire **qu'elle poursuive l'une des finalités visées à l'article 127/1** de la loi télécom **et** que **sa loi organique ou sectorielle lui donne le pouvoir d'obtenir ces données de l'opérateur**[24].

24. L'avant-projet de loi entend d'ailleurs **modifier plusieurs dispositions déterminant dans quelles conditions certaines autorités peuvent avoir accès aux données** de trafic et/ou de localisation conservées par les opérateurs :

- L'avant-projet prévoit d'intégrer un **§ 2, 2°/1 à l'article 14 de la loi statut IBPT** afin de permettre à l'IBPT de « *demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions* ».

- **L'article 88bis du CIC** permet au juge d'instruction, « *s'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées [et] à la localisation de l'origine ou de la destination de communications électroniques* ». L'avant-projet **y réintroduit un paragraphe 3**, qui a été annulé par la Cour constitutionnelle dans son arrêt n° 57/2021. Ce paragraphe établit **des règles particulières concernant le repérage des données relatives aux moyens de communications électroniques des avocats et des médecins**, étant donné que ces personnes sont tenues au secret professionnel.

- Le nouvel **article 42 § 2 de la loi sur la fonction de police** prévoit que *« Un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale*

[24] L'article 127/1 prévoit, en effet, que « Seules les autorités suivantes peuvent obtenir […] des opérateurs des données conservées en vertu des articles 122, 123, 126, 126/1 et 127, pour les finalités ci-dessous et dans les conditions prévues par les dispositions qui les y habilitent » (c'est l'Autorité qui souligne).

peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue […] ».

- La **loi sur les services de renseignement** qui détermine les conditions auxquelles ces services peuvent avoir accès aux données conservées par les opérateurs

- **L'article 84 § 1 de la loi FSMA** prévoit que « *moyennant l'autorisation préalable d'un juge d'instruction, l'auditeur ou, en son absence l'auditeur adjoint, peut, lorsqu'il estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, faire procéder : 1° au repérage des données de trafic de moyens de communications électroniques à partir desquels ou vers lesquels des communications électroniques ont été faites ; 2° à la localisation de l'origine ou de la destination de communications électroniques, y compris les numéros de téléphone et les adresses réseau ; 3° à la demande des détails de paiement des services de communications électroniques […]. L'auditeur ou, en son absence l'auditeur adjoint, indique dans sa décision les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver sa décision, des principes de proportionnalité et de subsidiarité. […]* ». L'avant-projet prévoit **d'ajouter un nouveau § 1er bis/1** à l'article 84 de la loi FSMA **qui permet à l'auditeur d'ordonner aux opérateurs de conserver certaines données au cas où ces données risquent d'être supprimées ou rendues anonymes,** jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.

- L'avant-projet entend permettre aux « *membres du personnel statutaire ou contractuel du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement désignés à cette fin par le Roi* », qui sont chargés de surveiller l'exécution de la loi relative à la protection de la santé et de ses arrêtés d'exécution ainsi que des règlements de l'Union européenne et qui relèvent des compétences du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement, « *identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique* ». **Le nouvel article 11 § 1 de la loi relative à la protection de la santé** prévoira désormais que ces membres du personnel statutaire ou contractuel

du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement pourront « *sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification […]* ».

- L'avant-projet entend ajouter **un § 2 à l'article 62 de la loi NIS** afin de permettre au Centre pour la Cybersécurité Belgique (ci-après « le CCB ») « [l*]orsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, [d'] obtenir des opérateurs […] des données d'identification, de trafic ou de localisation conservées par ceux-ci […]* »[25].

C. RAPPEL DES CONDITIONS AUXQUELLES DOIVENT REPONDRE LES NORMES QUI PREVOIENT UNE CONSERVATION DES DONNEES DE TRAFIC ET/OU LOCALISATION ET LEUR COMMUNICATION EVENTUELLE AUX AUTORITES

25. La **conservation des données** relatives au trafic et des données de localisation **constitue une ingérence importante dans les droits au respect de la vie privée et à la protection des données à caractère personnel.** En effet, comme la CJUE l'a souligné, à plusieurs reprises, « *les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications* »[26].

26. **La communication** éventuelle de ces données aux autorités **constitue une ingérence distincte** de celle qui est causée par leur conservation**,** mais qui est, elle aussi, **importante**.

---

[25] Les tâches énumérées à l'article 60 a) à e) de la loi NIS sont les suivantes :
« *a) le suivi des incidents au niveau national et international, en ce compris le traitement de données à caractère personnel lié au suivi de ces incidents ;*
b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et incidents auprès des parties intéressées ;
c) l'intervention en cas d'incident ;
d) l'analyse dynamique des risques et incidents et conscience situationnelle ;
e) la détection, l'observation et l'analyse des problèmes de sécurité informatique »

[26] Voyez, par exemple, CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 « Digital Rights Irland* et *al »*, § 27 ; CJUE, 21 décembre 2016, *affaires jointes C-203/15 et C-698/15 « Tele2 Sverige et al »*, § 99 ; CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »*, § 117.

27. L'Autorité rappelle que toute ingérence dans le droit au respect de la protection des données à caractère personnel, en particulier lorsque l'ingérence s'avère importante comme c'est le cas en l'espèce, n'est admissible que **si elle encadrée par une norme suffisamment claire et précise et dont l'application est prévisible pour les personnes concernées.** Ainsi, toute norme encadrant des traitements de données à caractère personnel, en particulier lorsque ceux-ci constituent une ingérence importante dans les droits et libertés des personnes concernées, doit répondre **aux exigences de prévisibilité et de précision** de sorte qu'à sa lecture, **les personnes concernées, puissent entrevoir clairement les traitements qui sont faits de leurs données et les circonstances dans lesquelles un traitement de données est autorisé**. En exécution de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, les **éléments essentiels du traitement** doivent y être **décrits avec précision**. Il s'agit, en particulier, de la ou des **finalité(s)** précise(s) du traitement ; de **l'identité du (ou des) responsable(s) du traitement** ; des **catégories de données traitées**, étant entendu que celles-ci doivent s'avérer – conformément à l'article 5.1. du RGPD, « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » ; des **catégories de personnes concernées** (personnes à propos desquelles des données seront traitées) ; de la **durée de conservation des données** ; des destinataires ou **catégories de destinataires** auxquels leurs données sont communiquées et les **circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées** ainsi que **toutes mesures visant à assurer un traitement licite et loyal de ces données à caractère personnel**.

28. Outre l'exigence de légalité, une ingérence dans le droit au respect de la protection des données n'est admissible que si elle est **nécessaire** et **proportionnée** à l'(aux) objectif(s) qu'elle poursuit. À travers plusieurs arrêts se prononçant sur la conformité de la conservation des données de trafic et de localisation et leur communication ultérieure éventuelle aux autorités avec les droits au respect de la vie privée et à la protection des données à caractère personnel[27], la **CJUE a clarifié la portée de ces exigences de nécessité et de proportionnalité**. Ce faisant, la Cour de Luxembourg **a clarifié les conditions** que doivent rencontrer les mesures législatives qui imposent **une conservation des données de trafic et de localisation** et **leur communication éventuelle aux autorités**, en particulier à des fins répressives.

29. Les règlementations qui prévoient une conservation des données doivent opérer une **pondération équilibrée** entre, d'une part, **l'objectif d'intérêt général** poursuivi par l'ingérence et, d'autre part, **les droits au respect de la vie privée et à la protection des données à caractère personnel**.

[27] Voyez, en particulier, CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 « Digital Rights Irland et al »*; CJUE, 21 décembre 2016, *affaires jointes C-203/15 et C-698/15 « Tele2 Sverige et al »* ; CJUE, 2 octobre 2018, *affaire C-207/16 Ministerio Fiscal* ; CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »* ; CJUE, 2 mars 2021, *affaire C-746/18 « Prokuratuur »*.

Il convient ainsi de **vérifier que la gravité de l'ingérence est en relation avec l'importance de l'objectif d'intérêt général poursuivi**[28]. En d'autres termes, **au plus l'objectif d'intérêt général poursuivi est important, au plus la règlementation imposant une conservation des données peut être intrusive** dans les droits et libertés des personnes concernées. Mais quoi qu'il en soit, **la conservation des données de trafic et de localisation doit**, dans une société démocratique, **rester l'exception**[29]. Ces données ne peuvent donc pas faire l'objet d'une conservation systématique et continue, quand bien même une telle conservation permettrait de lutter contre la criminalité grave et prévenir des menaces graves contre la sécurité publique. La Cour de justice estime, en effet, qu'une **mesure de conservation généralisée et indifférenciée des données** constitue une **ingérence tellement importante** dans les droits fondamentaux des personnes concernées qu'elle **n'est, en principe, pas admissible**[30] (sauf, nous y reviendrons, à des fins de sauvegarde de la sécurité nationale[31]).

30. De plus, la CJUE exige que les règlementations qui prévoient une conservation des données **répondent à des critères objectifs** et **établissent un rapport entre les données à conserver et l'objectif poursuivi**[32].

31. Appliquant le principe de proportionnalité lors de l'examen de différentes catégories de mesures imposant une conservation des données de trafic et/ou de localisation, **la Cour a identifié les conditions dans lesquelles de telles mesures étaient – ou non – admissibles**.

- ***Mesures imposant une conservation généralisée et indifférenciée des données à des fins de sauvegarde de la sécurité nationale***

32. L'objectif de **sauvegarde de la sécurité nationale** est d'une telle importance que la CJUE admet **qu'il puisse justifier une conservation généralisée et indifférenciée** des données de localisation et de trafic, **à condition** qu'il existe une **menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible** (et **uniquement** pour la p**ériode pendant laquelle cette menace existe**)[33].

33. La Cour ajoute qu'il est essentiel que la **décision qui enjoint** aux fournisseurs de services de communications électroniques **de procéder à une telle conservation** des données puisse faire l'objet d'un **contrôle effectif** soit par une juridiction, soit par une entité administrative indépendante,

[28] CJUE, arrêt du 2 octobre 2018, § 55 ; CJUE, arrêt du 6 octobre 2020, § 131 ; CJUE, arrêt du 2 mars 2021, § 32.
[29] CJUE, arrêt du 6 octobre 2020, § 142.
[30] CJUE, arrêt du 6 octobre 2020, § 141.
[31] CJUE, arrêt du 6 octobre 2020, § 136-137.
[32] CJUE, arrêt du 6 octobre 2020, § 133.
[33] CJUE, arrêt du 6 octobre 2020, § 137.

dont la décision est dotée d'un effet contraignant, visant à **vérifier l'existence d'une de ces situations** ainsi que **le respect des conditions et des garanties devant être prévues**[34].

- ***Mesures imposant une conservation préventive ciblée des données de trafic et des données de localisation à des fins de lutte contre la criminalité grave et prévention contre des menaces graves à la sécurité publique***

34. Selon la CJUE, une **conservation généralisée et indifférenciée** des données relatives au trafic et à la localisation **en vue de lutter contre la criminalité, même grave, excède,** dans une société démocratique, **ce qui est nécessaire**[35]**.** Les Etats **ne** peuvent donc **pas imposer une conservation généralisée et indifférenciée de ces données pour lutter contre la criminalité grave**. *A fortiori,* une telle mesure ne peut être introduite pour prévenir, rechercher, détecter et poursuivre des infractions pénales en général[36]. En revanche, la Cour estime qu'une **conservation préventive ciblée** des données de trafic et de localisation afin **de lutter contre la criminalité grave**, prévenir **des atteintes graves à la sécurité publique** et, *a fortiori*, **sauvegarder la sécurité nationale** peut être justifiée[37]. La lutte contre la criminalité en général ne peut, en revanche, pas justifier une telle conservation préventive, même si elle est ciblée.

35. Selon la Cour, **plusieurs critères** peuvent être utilisés **pour cibler la conservation** préventive des données en vue de **lutter contre la criminalité grave** : la conservation peut être limitée à des **données afférentes à une période temporelle** et/ou **une zone géographique** et/ou **sur un cercle de personnes** susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer par la conservation de leurs données, à la lutte contre la criminalité grave[38].

36. Quant à la délimitation de la conservation des données sur base de **critères géographiques**, la CJUE considère qu'elle est admise lorsque les autorités nationales compétentes considèrent, **sur la base d'éléments objectifs et non discriminatoires**, qu'il existe, dans une ou plusieurs zones géographiques, une **situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave**. La Cour précise que « *[c]es zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages* »[39].

[34] CJUE, arrêt du 6 octobre 2020, § 139.
[35] CJUE, arrêt du 6 octobre 2020, § 141.
[36] CJUE, arrêt du 6 octobre 2020, § 140.
[37] CJUE, arrêt du 6 octobre 2020, § 146-151.
[38] CJUE, arrêt du 8 avril 2014, § 59 ; CJUE, arrêt 21 décembre 2016, § 106 ; CJUE, arrêt du 6 octobre 2020, § 144.
[39] CJUE, arrêt du 6 octobre 2020, § 150.

37. Dans tous les cas, **les mesures imposant une conservation ciblée** des données à des fins de lutte contre la criminalité grave **ne sauraient dépasser celle qui est strictement nécessaire** au regard de l'objectif poursuivi ainsi que **des circonstances** la justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.

- ***Mesures imposant une conservation préventive et généralisée des adresses IP à des fins de lutte contre la criminalité grave et la sauvegarde de la sécurité publique***

38. La CJUE relève que « *les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée* »[40]. Pour autant que seules les adresses IP de la source des communications soient conservées et non celles du destinataire de celles-ci, ces adresses IP ne révèlent pas, en tant que telles, des informations sur le(s) destinataire de la communication[41]. Les adresses IP attribuées à la source d'une connexion présentent ainsi, selon la CJUE, un degré de sensibilité moindre que les autres données relatives au trafic, mais la CJUE souligne que ces adresses IP peuvent néanmoins être utilisées – si elles sont combinées aux adresses IP du destinataire de la communication – pour effectuer le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier[42]. **La conservation et l'analyse de ces données constituent dès lors des ingérences graves dans les droits fondamentaux de l'internaute[43]**.

39. Elle estime toutefois qu'il **est admissible d'imposer une conservation de ces données généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion**[44], **pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données[45]**. Eu égard à la gravité de l'ingérence causée par la conservation généralisée et indifférenciée des adresses IP, la CJUE estime que **seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature,** à l'instar de la sauvegarde de la sécurité nationale, **à justifier cette ingérence[46]**. La Cour ajoute que la **durée de conservation** doit être **limitée à ce qui est**

[40] CJUE, arrêt du 6 octobre 2020, § 152.
[41] CJUE, arrêt du 6 octobre 2020, § 152.
[42] CJUE, arrêt du 6 octobre 2020, § 152-153.
[43] CJUE, arrêt du 6 octobre 2020, § 153.
[44] En effet, la Cour note que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. Or, la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, s'avérer impossible sans avoir recours à une mesure législative imposant la conservation de ces données.
[45] CJUE, arrêt du 6 octobre 2020, § 155.
[46] CJUE, arrêt du 6 octobre 2020, § 156.

strictement nécessaire au regard de l'objectif poursuivi[47]. Enfin, il est nécessaire de prévoir **des conditions et des garanties strictes** quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées[48].

- ***Mesures imposant une conservation généralisée et indifférenciée des données relatives à l'identité civile***

40. La CJUE souligne que les **données relatives à l'identité civile** des utilisateurs des moyens de communications ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée[49]. Il s'ensuit que **l'ingérence causée par la conservation de ces données ne doit pas être qualifiée de grave[50]**. La Cour estime dès lors qu'une mesure législative peut imposer, sans délai particulier, **la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs** des moyens de communications électroniques **aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales** ainsi que de la **sauvegarde de la sécurité publique**, sans qu'il soit nécessaire que les infraction pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves[51].

- ***Mesures imposant une conservation « rapide » des données de trafic et de localisation à des fins de lutte contre la criminalité grave***

41. Les données de trafic et de localisation, qui sont conservées et traitées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6, 9 ou 15 de la Directive ePrivacy, doivent, en principe, être effacées ou rendues anonymes au terme de délais légaux déterminés par les dispositions nationales transposant la Directive ePrivacy[52]. La CJUE reconnait toutefois **qu'il peut être nécessaire de conserver ces données au-delà de ces délais** « *aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée* »[53].

[47] CJUE, arrêt du 6 octobre 2020, § 156
[48] CJUE, arrêt du 6 octobre 2020, § 156.
[49] CJUE, arrêt du 6 octobre 2020, § 157 ; CJUE, arrêt du 2 mars 2021, § 34.
[50] CJUE, arrêt du 6 octobre 2020, § 157.
[51] CJUE, arrêt du 6 octobre 2020, § 158.
[52] CJUE, arrêt du 6 octobre 2020, § 160.
[53] CJUE, arrêt du 6 octobre 2020, § 161.

42. La Cour de Luxembourg admet ainsi que les Etats **peuvent prévoir**, dans leur législation, **la possibilité d'enjoindre** aux fournisseurs de services de communications électroniques **de procéder**, pour une durée déterminée, à **la « conservation rapide »** des données relatives au trafic et des données de localisation dont ils disposent en vertu de dispositions législatives transposant les articles 5, 6, 9 et 15 de la Directive ePrivacy[54]. Une mesure de « conservation rapide » peut ainsi être prise à l'égard de données dont la conservation initiale poursuivait une autre finalité que la lutte contre la criminalité grave ou la sauvegarde de la sécurité nationale.

43. Toutefois, **la décision** de faire procéder à une conservation rapide des données n'est admise qu'aux **conditions suivantes**[55] :

- Cette décision doit être **soumise à un contrôle juridictionnel effectif ;**

- Cette décision ne peut être prise **qu'en vue de lutter contre la criminalité grave** et, *a fortiori*, la **sauvegarde de la sécurité nationale ;**

- L'obligation de conservation **ne peut porter que sur les données** de trafic et données de localisation **susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée[56]** ;

- La **durée de conservation** de ces données doit être **limitée au strict nécessaire**, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

➢ ***Exigences relatives aux mesures techniques et organisationnelles concernant la conservation des données par les fournisseurs de services de communications électroniques.***

44. La CJUE souligne qu'aux termes de l'article 4 §§ 1 et 1bis de la Directive ePrivacy, les fournisseurs doivent prendre des **mesures d'ordre technique et organisationnel appropriées** pour assurer **une protection efficace des données** conservées **contre les risques d'abus** ainsi que **contre**

[54] CJUE, arrêt du 6 octobre 2020, § 163.
[55] CJUE, arrêt du 6 octobre 2020, § 164.
[56] À cet égard, la CJUE admet que la conservation rapide des données peut concerner les données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale, mais également les *« données […] afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause* » (CJUE, arrêt du 6 octobre 2020, § 165).

tout accès illicite à ces données[57]. La Cour insiste, en particulier, sur la nécessité pour la réglementation nationale de **prévoir la conservation sur le territoire de l'Union** ainsi que la **destruction irrémédiable des données** au terme de la durée de conservation de celles-ci[58]. Il faut, en outre, que les **Etats garantissent le contrôle, par une autorité indépendante, du respect du niveau de protection garanti** par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel.

- ***Sur l'accès aux données conservées par les fournisseurs de services de communications électroniques***

45. Conformément à l'exigence de prévisibilité, la communication des données conservées par les fournisseurs de services de communications électroniques aux autorités nationales **doit être encadrée par des règles claires et précises** indiquant les **circonstances** et **sous quelles conditions** cette communication a lieu. Cette règlementation doit prévoir **des conditions matérielles et procédurales** afin de garantir que l'accès aux données conservées soit limité au strict nécessaire[59] **:**

    - **La règlementation doit déterminer la finalité pour laquelle les autorités peuvent obtenir un accès aux données conservées par les fournisseurs de services de communication**. À cet égard, la Cour indique que **l'accès aux données ne peut, en principe, être justifiée que par l'objectif d'intérêt général pour lequel leur conservation a été imposée**[60]. Ainsi, un accès à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, *a fortiori*, de sauvegarde de la sécurité nationale. **En revanche**, conformément au principe de **proportionnalité**, un **accès à des données conservées en vue de la lutte contre la criminalité grave peut**, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès, **être justifié par l'objectif de sauvegarde de la sécurité nationale**. En outre, la Cour admet que les **Etats peuvent prévoir que des données conservées d'une manière conforme aux articles 5, 6, 9 ou 15 de la Directive ePrivacy** peuvent être communiquées aux autorités, dans le respect de conditions matérielles et procédurales, **à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale**[61].

[57] CJUE, arrêt du 21 décembre 2016, § 122.
[58] CJUE, arrêt du 21 décembre 2016, § 122.
[59] CJUE, arrêt du 21 décembre 2016, §§ 118-121.
[60] CJUE, arrêt du 2 mars 2021, § 31.
[61] CJUE, arrêt du 6 octobre 2020, § 164-165.

La règlementation régissant l'accès aux données doit donc déterminer la finalité poursuivie par les autorités pouvant avoir accès aux données, mais cette règlementation ne saurait se limiter à exiger que l'accès réponde à l'un des objectifs visés par l'article 15 § 1 de la Directive ePrivacy, fût-ce la lutte contre la criminalité grave[62]. Cette règlementation doit également prévoir des conditions matérielles et procédurales régissant cette utilisation[63].

- **La réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé[64]**. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités.

- **L'accès des autorités nationales** compétentes aux données conservées doit, en principe, sauf cas d'urgence dûment justifiés, **être subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante**. La décision de cette juridiction ou de cette entité **doit intervenir à la suite d'une demande motivée de ces autorités**[65]. Par ailleurs, la Cour a souligné que **l'autorité chargée d'exercer le contrôle préalable**, qu'il s'agisse d'une juridiction ou d'une entité administrative indépendante, doit avoir **la qualité de tiers** par rapport à celle qui demande l'accès aux données, afin que la première puisse exercer ce contrôle de manière impartiale, à l'abri de toute influence extérieure[66].

- Les autorités qui ont eu accès aux données **doivent en informer les personnes concernées dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes** menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre aux personnes concernées d'exercer,

[62] CJUE, arrêt du 21 décembre 2018, § 118.
[63] CJUE, arrêt du 2 mars 2021, § 49.
[64] CJUE, arrêt du 2 mars 2021, § 50.
[65] CJUE, arrêt du 21 décembre 2018, § 120 ; CJUE, arrêt du 2 mars 2021, § 51.
[66] CJUE, arrêt du 2 mars 2021, § 52.

notamment, le droit de recours, explicitement prévu à l'article 15 § de la directive ePrivacy, lu en combinaison avec le RGPD, en cas de violation de leurs droits[67].

D. EXAMEN DE LA CONFORMITE DE L'AVANT-PROJET DE LOI ET DU PROJET D'ARRETE AVEC LES EXIGENCES DU DROIT EUROPEEN ET DES PRINCIPES FONDAMENTAUX EN MATIERE DE PROTECTION DES DONNEES

46. L'Autorité examine ci-dessous les différentes dispositions de l'avant-projet de loi qui autorisent ou imposent la conservation de données de trafic et/ou de localisation en vue de leur communication éventuelle aux autorités, afin d'apprécier leur conformité avec les principes fondamentaux en matière de protection des données.

47. L'Autorité estime nécessaire, préalablement à cet examen, de rappeler, comme la Cour constitutionnelle l'a fait dans son arrêt du 21 avril 2021, que la jurisprudence de la CJUE « *impose un changement de perspective par rapport au choix que le législateur a effectué* » : **l'obligation de conservation des données de trafic et de localisation doit être l'exception, et non la règle**. Or force est de constater que **l'avant-projet de loi** – qui entend répondre à l'annulation de la loi de 2016 **– n'opère pas complètement ce changement de perspective** puisque, comme l'Autorité le développera ci-dessous, l'avant-projet de loi entend imposer de nouvelles mesures de conservation des données de trafic et de localisation (afin de lutter contre la fraude, l'utilisation malveillante du réseau et pour garantir la sécurité des réseaux) qui pourraient aboutir à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données. **L'Autorité insiste pour que le législateur adapte l'avant-projet de loi pour que la loi qui sera votée respecte toutes les exigences imposées par la CJUE et la Cour constitutionnelle**. Il s'agit d'une condition essentielle pour conserver la confiance des citoyennes et des citoyens.

48. L'Autorité est consciente que la conservation des données de trafic et de localisation peut être nécessaire pour garantir le droit à la sécurité et le droit à un recours effectif qui sont, comme le droit au respect de la vie privée et à la protection des données à caractère personnel, des droits fondamentaux consacrés par la Constitution belge, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne. La CJUE, dans son arrêt du 6 octobre 2020, reconnait d'ailleurs la nécessité de procéder à une conciliation entre ces différents droits fondamentaux[68]. Elle rappelle, dans ce contexte, qu' « *un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre d'une part, l'objectif d'intérêt général et, d'autre, part, les droits en cause* »[69]. Dans l'analyse de la proportionnalité des différentes mesures de

[67] CJUE, arrêt du 21 décembre 2018, § 121.
[68] CJUE, arrêt du 6 octobre 2020, § 127.
[69] CJUE, arrêt du 6 octobre 2020, § 130.

conservation des données de trafic et de localisation, la CJUE a ainsi cherché constamment à réaliser cette conciliation entre les différents droits fondamentaux en jeu. **L'Autorité invite le législateur à prendre le temps de la réflexion et de l'analyse rigoureuse pour concilier, dans le respect de la jurisprudence européenne, les droits fondamentaux à la sécurité et à un recours effectif, d'une part, et les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, d'autre part**.

1) Remarque préalable concernant l'interaction entre l'avant-projet de loi et le Code de communications électroniques européen

49. Certaines modifications apportées par l'avant-projet de loi aux articles 122 et suivants de la loi télécom et par le projet d'arrêté visent à aligner la terminologie qu'ils emploient avec celle du Code de communications électroniques européen (ci-après « CCEE »). Ainsi, l'avant-projet de loi ou le projet d'arrêté utilisent, sans les définir, plusieurs notions qui ne sont pas encore définies (en particulier les notions de « service de communications interpersonnelles » ou de « services nomades ») parce qu'il est prévu que la loi télécom définisse ces notions à la suite de sa modification par la loi qui transposera le CCCE en droit interne. Le délégué du Ministre a confirmé que ce texte était en cours de finalisation et qu'il devrait être déposé au Parlement avant les vacances parlementaires. L'Autorité en prend note et souligne que **si le texte, qui définit ces nouvelles notions, n'était pas adopté avant l'adoption de l'avant-projet de loi et du projet d'arrêté, il conviendra d'inclure les définitions des notions qu'ils utilisent dans l'avant-projet de lo**i.

50. Par ailleurs, l'Autorité souligne **que la transposition du CCEE va entrainer la redéfinition, notamment, des concepts d'« opérateurs » et de « services de communications électroniques »**. La notion de « service de communications électroniques » sera désormais définie comme « le *service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus et à l'exception des services de médias audiovisuels ou sonores, comprend les types de services suivants : a) un service d'accès à l'internet ; b) un service de communications interpersonnelles ; et c) des services consistant entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine* ». La notion de « service de communications électroniques » sera donc définie de manière beaucoup plus large qu'actuellement puisqu'elle va englober, en particulier, les « services de communications interpersonnelles » qui seront définis comme : « *un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend*

pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service ». La notion d'« opérateur » sera définie, après la transposition du CCEE dans la loi télécom, comme « *une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public* ».

51. Ces modifications de définitions des concepts aboutissent à ce que les entreprises qui fournissent un service de communications électroniques « over-the-top », à l'instar, par exemple, de WhatsApp, Skype, Signal, ou encore Telegram, seront considérées comme des opérateurs soumis aux obligations de conservation des données de trafic et de localisation imposées par la loi télécom, telle qu'elle sera modifiée par l'avant-projet. **L'Autorité souligne que cette redéfinition des notions de « service de communications électroniques » et d'« opérateur » aboutit à étendre le champ d'application des dispositions autorisant ou imposant la conservation de telles données**.

2) Conservation des données à des fins de facturation et de paiement d'interconnexion (nouvel article 122 § 2 de la loi télécom)

52. Le nouvel article 122 § 2 de la loi télécom, qui transpose l'article 6 § 2 de la Directive ePrivacy, **autorise les opérateurs à conserver et traiter les données de trafic nécessaires pour établir les factures des abonnés ou effectuer les paiements d'interconnexion**. L'opérateur doit informer, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent, des types de données traitées, des objectifs précis du traitement et de la durée du traitement. Ce traitement de données est autorisé uniquement jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.

53. Les **traitement de données** autorisés par la nouvelle version de l'article 122 § 2 de la loi télécom **reposent sur une base juridique au sens de l'article 6.1 du RGPD** : l'exécution d'un contrat auquel la personne concernée est partie pour les traitements nécessaires pour établir les factures des abonnés (article 6.1.b) du RGPD) et la poursuite des intérêts légitimes du responsable du traitement ou d'un tiers pour les traitements nécessaires pour effectuer les paiements d'interconnexion (article 6.1.f) du RGPD).

54. Les **finalités poursuivies** – établir les factures des abonnés ou effectuer les paiements d'interconnexion – sont, conformément à l'exigence de l'article 5.1.b) du RGPD, **« *déterminées, explicites et légitimes* ».**

55. La nouvelle version de l'article 122 § 2 de la loi télécom n'identifie plus – contrairement à la version antérieure de l'article 122 § 2 de la loi télécom – les données précises qui peuvent être traitées sur pied de cette disposition. Si cette suppression aboutit à diminuer la prévisibilité de la norme autorisant le traitement de données, l'Autorité considère néanmoins qu'elle est admissible. En effet, la disposition indique que seules les données de trafic nécessaires pour établir les factures des abonnés ou effectuer les paiements d'interconnexion peuvent être traitées. Cette précision circonscrit de manière relativement prévisible les données qui peuvent être traitées[70]. En outre, l'Autorité comprend que les données de trafic nécessaires à ces fins peuvent varier selon les circonstances et qu'il est nécessaire que les opérateurs aient une marge de manœuvre à cet égard. Par ailleurs, il ressort de l'article 122 § 2 de la loi télécom que les personnes concernées doivent être informées, avant le traitement, des données qui seront traitées sur pied de cette disposition. Dans ces circonstances, l'Autorité considère que l'article 122 § 2 de la loi télécom reste suffisamment prévisible en ce qui concerne les catégories de données qui peuvent être traitées.

56. L'article 122 § 2 de la loi télécom, qui détermine **les critères permettant de déterminer la durée maximale de conservation**[71], **répond à l'exigence de l'article 5.1.e) du RGPD**.

3) Conservation des données pour assurer le marketing des services de communications électroniques propres et établir le profil d'utilisation ou des services à données de trafic ou de localisation (nouvel article 122 § 3 de la loi télécom)

57. **L'article 122 § 3 de la loi télécom**, qui transpose l'article 6.3 de la Directive ePrivacy, autorise les opérateurs à traiter et à conserver les données de trafic (qui incluent les données de localisation liées à une communication) nécessaires afin (i) d'assurer le **marketing** des services de communications électroniques propres et (ii) d'établir **le profil d'utilisation** de l'abonné ou de l'utilisateur final, **à condition d'avoir obtenu le consentement** de l'abonné ou, le cas échéant, de l'utilisateur final.

58. **Les modifications apportées par l'avant-projet de loi concernent la définition du « consentement »**. Cette notion est, à présent, définie par un renvoi à l'article 4 du RGPD (nouvel article 122 § 3, 2°, alinéa 2 de la loi télécom). Il s'ensuit que l'avant-projet prévoit que les abonnés ou utilisateurs finaux doivent avoir la possibilité de retirer leur consentement facilement et à tout moment (nouvel article 122 § 3, 3°). **L'Autorité prend note de ces changements** qui font suite à l'entrée en vigueur du RGPD.

[70] L'Autorité rappelle que les opérateurs, qui sont les responsables du traitement, devront respecter le principe de minimisation des données (article 5.1.c) du RGPD). Ainsi, si un abonné a un abonnement avec appels illimités, il n'apparait – à première vue – pas nécessaire de conserver les données de trafic permettant de comptabiliser le nombre ou la durée des appels sortants ayant été réalisé.
[71] L'Autorité constate, en outre, que les critères retenus par le législateur belge sont directement issus de la Directive ePrivacy.

59. L'avant-projet **remplace également la référence la loi du 8 décembre 1992** relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel **par une référence au RGPD et à la LTD**. L'Autorité **en prend note**.

4) Conservation des données pour détecter et analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine (nouvel article 122 § 4 de la loi télécom)

60. Le nouvel article 122 § 4 de la loi télécom **impose** aux opérateurs **de conserver des données de localisation et autres données de trafic nécessaires** afin de détecter et d'analyser **une fraude présumée** ou **une utilisation malveillante présumée** du réseau de communication électroniques.

61. La notion de « fraude » est définie par le nouvel article 122 § 4, alinéa 1er, de la loi télécom comme suit : « *un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite, commis par le biais de l'utilisation d'un service de communications électroniques* ».

62. La notion d'« utilisation malveillante du réseau » est définie par le nouvel article 122 § 4, alinéa 2, de la loi télécom comme suit : *« une utilisation du réseau afin d'importuner son correspondant ou de provoquer des dommages* ».

63. L'Exposé des motifs donne des exemples concrets de ce qui constitue une fraude ou une utilisation malveillante du réseau. Constituent une fraude, par exemple, le fait pour l'utilisateur final de ne pas respecter les conditions générales qui le lient à l'opérateur, le fait qu'un tiers fasse usage d'un service de communications électroniques au nom de l'abonné à son insu, le harponnage par SMS (« smishing »), le harponnage par Internet (« phishing ») ou encore un appel entrant induisant l'utilisateur final en erreur sur l'origine de cet appel et lui causant un préjudice (« spoofing »)[72]. L'utilisation malveillante du réseau couvre, par exemple, le harcèlement par téléphone[73].

64. Le nouvel article 122 § 4 de la loi télécom crée **une nouvelle obligation juridique** à charge des opérateurs de conserver et, le cas échéant de traiter, les données de localisation et autres données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communications électroniques. **Les traitements de données qui seront réalisés par les opérateurs sur pied de cette disposition seront, dès lors, « *nécessaires au***

[72] Exposé des motifs, p. 16.
[73] Exposé des motifs, p. 16.

respect d'une obligation légale à laquelle le responsable du traitement est soumis » (article 6.1.c) du RGPD).

65. Afin que ces traitements de données soient licites, il faut, comme le soulignait le Groupe de travail « Article 29 », que la loi remplisse « *toutes les conditions requises pour rendre l'obligation valable et contraignante, et [qu'elle soit] conforme au droit applicable en matière de protection des données, notamment aux principes de nécessité, de proportionnalité et de limitation de la finalité* »[74]. En d'autres termes, « ***le responsable du traitement ne doit pas avoir le choix de se conformer ou non à l'obligation*** »[75]. L'obligation légale doit être **claire et précise**, de telle sorte **que le responsable du traitement ne doit pas avoir de marge d'appréciation** quant à la façon de réaliser le traitement de données à caractère personnel nécessaire au respect de son obligation légale[76].

66. Le nouvel article 122 § 4 de la loi télécom **définit les finalités poursuivies par les nouveaux traitements de données qu'il impose** : il s'agit de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine. L'Autorité constate que **ces finalités** sont, conformément à l'exigence de l'article 5.1.b) du RGPD, « ***déterminées, explicites et légitimes*** ». Par ailleurs, l'Autorité reconnait que ces finalités peuvent **répondre à l'un des objectifs listés par l'article 15 § 1 de la Directive ePrivacy**, en particulier la prévention, la recherche, la détection ou la poursuite d'infractions pénales et/ou la protection de la personne concernée ou des droits et libertés d'autrui[77]. **Il ne suffit toutefois pas que les objectifs** poursuivis par le nouvel article 122 § 4 de la loi télécom **soient légitimes pour que l'obligation de conservation des données qu'il impose soit admissible**. Il faut, en outre, **que cette obligation soit « rigoureusement »[78] nécessaire et proportionnée à ces objectifs**.

67. À ce propos, l'Autorité constate que le nouvel article 122 § 4 de la loi télécom **impose aux opérateurs de conserver de manière systématique des données** de localisation et d'autres données de trafic

[74] Groupe de travail « Article 29 », Avis *06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 21.
[75] Groupe de travail « Article 29 », Avis *06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 21.
[76] Groupe de travail « Article 29 », Avis *06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 22.
[77] L'article 15 § 1 de la Directive ePrivacy liste plusieurs objectifs d'intérêt général permettant de justifier une limitation aux droits et obligations consacrés par les articles 5, 6 et 9 de ladite directive et fait, à la fin de cette liste, un renvoi à l'article 13 § 1 de la directive 95/46. Cette dernière disposition détermine les objectifs que peut poursuivre une mesure législative qui vise à limiter la portée des obligations et des droits prévus par la directive 95/46. Cette directive a été abrogée par l'article 94 du RGPD, lequel indique, en outre, que « *Les références faites à la directive abrogée s'entendent comme faites au présent règlement* ». Il s'ensuit que la référence faite à l'article 13 de la directive 95/46 doit être comprise comme une référence à l'article 23 du RGPD. L'article 23 du RGPD prévoit qu'une mesure législative peut limiter la portée des obligations et des droits prévus par le RGPD à condition qu'une *« telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir […] la protection de la personne concernée ou des droits et libertés d'autrui* ».
[78] Voyez le considérant 11 de la Directive ePrivacy

de l'ensemble des utilisateurs des moyens de communications électroniques[79]. Cette disposition constitue ainsi une **ingérence particulièrement grave** dans les droits au respect de la vie privée et à la protection des données à caractère personnel. **Le principe de proportionnalité exige que l'objectif d'intérêt général poursuivi par la mesure de conservation obligatoire soit en relation avec la gravité de l'ingérence qu'elle cause.** Or, la CJUE considère qu'une « *réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* »[80]. **L'Autorité doute dès lors de la proportionnalité de l'obligation prévue par l'article 122 § 4 de la loi télécom au regard des objectifs qu'elle poursuit alors que ces objectifs, s'ils sont légitimes, ne semblent pas, à première vue, présenter le même degré d'importance que la lutte contre la criminalité grave**[81]. L'Autorité souligne, en outre, que l'avant-projet de loi prévoit que les différentes autorités identifiées par le nouvel article 127/1 de la loi télécom – dont « *les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions*

[79] À la suite d'une demande d'informations complémentaires, le délégué du Ministre conteste que l'article 122 § 4 de la loi télécom impose une conservation généralisée et indifférenciée des données de localisation et autres données de trafic en développant l'argumentation suivante (les notes de bas de pages ont été omises): *« Dans son arrêt 'La Quadrature du Net', la Cour de justice de l'Union européenne (CJUE) a précisé qu'une 'réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi'. Or, le projet de loi soumis à l'avis de l'Autorité de protection des données effectue une différenciation au regard de l'objectif poursuivi, dès lors qu'il prévoit la conservation des seules données nécessaires au regard de chacune des finalités visées aux paragraphes 2, 3 et 4 de l'article 122 […]* ». Le délégué du demandeur considère ainsi que l'obligation de conservation n'est pas généralisée et indifférenciée parce qu'elle est imposée pour un objectif déterminé et que les données qui doivent être conservées sont les données nécessaires pour atteindre cette finalité. L'Autorité ne peut suivre cette argumentation. Le passage cité par le demandeur ne peut pas être coupé de son contexte et, en particulier, de la phrase qui le suit, laquelle indique qu'« *une telle réglementation […] concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique* ». **Si on lit le § 143 de l'arrêt « Quadrature du Net » dans sa globalité, il ne peut être compris comme autorisant une conservation des données de trafic et de localisation de l'ensemble des utilisateurs d'un moyen de communication électronique dès lors que cette obligation poursuit un objectif déterminé et ne porte que sur des données de trafic nécessaires à cette fin.** Si tel avait été la position de la Cour, elle n'aurait pas exigé une conservation ciblée des données de trafic et de localisation aux fins de lutte contre la criminalité grave. **Le paragraphe 143 de l'arrêt du 6 octobre souligne qu'il doit exister un lien, même s'il peut être indirect ou lointain, entre les personnes dont les données seront conservées et l'objectif poursuivi par l'obligation de conservation**. L'obligation imposée par l'article 122 § 4 de la loi télécom porte sur les données de trafic et de localisation de tout utilisateur de moyens de communications électroniques sans qu'il soit requis qu'il existe un lien, même indirect et lointain, avec l'objectif de lutte contre la fraude ou l'utilisation malveillante du réseau. Certes, toute personne peut, potentiellement, commettre un « fraude » ou une « utilisation malveillante du réseau » ou, en être victime, mais cette potentialité – qui existe également pour les crimes graves dont la lutte constituait l'objectif de la règlementation sur laquelle portait l'arrêt de la CJUE – ne peut, au regard de la jurisprudence de la CJUE, être jugée suffisante pour justifier une conservation préventive systématique des données de trafic de l'ensemble des utilisateurs d'un moyen de communication électroniques nécessaires à la lutte contre la fraude et l'utilisation malveillante du réseau.

[80] CJUE, arrêt du 6 octobre 2020, § 141.

[81] À la suite d'une demande d'informations complémentaires, le délégué du Ministre semble reconnaitre, lui-même, que l'objectif de lutte contre la fraude et l'utilisation malveillante du réseau ne présente pas le même degré de gravité que la lutte contre la criminalité grave puisqu'il écrit « *L'article 127/1 s'inscrit pleinement dans cette jurisprudence européenne vu que le critère de proportionnalité est in concreto rencontré : en effet, si la conservation des données est justifiée originellement pour lutter, par exemple, contre les fraudes ou à des fins protection de la sécurité des réseaux, ces mêmes données peuvent a fortiori être traitées ultérieurement pour des finalités plus graves, à savoir, dans le cadre de la criminalité grave et de menace grave contre la sécurité publique* » (c'est l'Autorité qui souligne).

commises en ligne » – pourront avoir accès à ces données[82]. L'Autorité remarque qu'en imposant une nouvelle obligation de conservation généralisée des données de trafic et de localisation afin de lutter contre la fraude et l'utilisation malveillante du réseau tout en prévoyant, en parallèle, que les autorités répressives (entre autres) peuvent accéder à ces données, l'avant-projet de loi aboutit, *de facto*, à réintroduire une obligation de conservation généralisée et indifférenciée de ces données à des fins de lutte contre la criminalité. La CJUE a pourtant considéré qu'il n'était pas admissible d'imposer une telle obligation de conservation, et ce même pour lutter contre la criminalité grave, ce qui n'est pas le cas ici.

68. Par ailleurs, **l'Autorité s'interroge également sur la nécessité de l'obligation de conservation préventive et systématique des données qui est imposée par le nouvel article 122 § 4 de la loi télécom** à des fins de détection et d'analyse d'une fraude présumée ou d'une utilisation malveillante présumée du réseau de communication électroniques. **Ces objectifs ne pourraient-ils pas être atteints par des mesures moins intrusives dans les droits et libertés des personnes concernées ?** Ne serait-il pas possible, par exemple, de prévoir que l'obligation de conservation des données à des fins de lutte contre la fraude et l'utilisation malveillante du réseau peut être « activée » lorsqu'il existe des indices de fraude ou d'utilisation malveillante du réseau[83], auquel cas la conservation serait ciblée sur les personnes susceptibles d'être mêlées d'une manière ou d'une autre à la fraude ou à l'utilisation malveillante du réseau ou qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave ? Cette option rencontrerait l'exigence du « changement de perspective » mise en évidence par l'arrêt de la Cour constitutionnelle[84] : on passerait d'une conservation préventive et généralisée à une conservation réactive et ciblée. L'Autorité rappelle qu'il incombe au législateur de justifier que l'option qu'il choisit constitue la voie la moins attentatoire aux droits et libertés des personnes concernées pour atteindre l'objectif qu'il poursuit.

69. **L'Autorité invite dès lors le législateur à apprécier rigoureusement au regard de la jurisprudence de la CJUE, et à justifier, la mesure dans laquelle l'obligation de conserver les données de localisation et autres données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communication électroniques est effectivement nécessaire et proportionnée aux objectifs qu'elle poursuit**.

[82] Telle que cela ressort d'une lecture combinée des nouveaux articles 122 § 7 et 127/1 de la loi télécom
[83] L'indice d'une utilisation malveillante du réseau peut consister, par exemple, en une plainte faite par une personne qui s'estime victime de harcèlement. Le harcèlement étant, par définition, une infraction qui s'étale dans le temps, avec des occurrences répétitives, « activer » une obligation de conservation en cas de plainte permettrait probablement d'identifier la personne commettant le harcèlement. L'indice d'une fraude consistant à abuser des conditions générales de l'opérateur pourrait apparaitre en examinant les données conservées en vue de la facturation du service.
[84] C.C., arrêt du 21 avril 2021, § B.18.

70. Au-delà des interrogations fondamentales de l'Autorité concernant la nécessité et la proportionnalité de l'obligation imposée par le nouvel article 122 § 4 de la loi télécom, **l'Autorité a plusieurs remarques plus « ponctuelles » à formuler concernant la prévisibilité et la proportionnalité de certaines des modalités de cette obligation**.

71. Tout d'abord, **l'Autorité constate que cette disposition ne détermine pas avec précision les données qui doivent être conservées** en vue de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communication électroniques. Elle indique seulement que les opérateurs conservent « *les données de localisation et les autres données de trafic nécessaires à cette fin* » et qu'ils « *traitent les données de trafic nécessaires à cette fin, en ce compris lorsque c'est nécessaire, les données visées au paragraphe 2* [ndlr : les données de trafic nécessaires pour établir les factures des abonnés et les paiements d'interconnexion] ». L'article 122 § 4 de la loi télécom **contient une habilitation facultative au Roi** de déterminer les données de trafic qui doivent être conservées et traitées en application de cette disposition. Le Roi peut, mais ne doit pas, déterminer ces données[85].

72. L'Autorité rappelle, **qu'en vertu de l'exigence de prévisibilité**, **les données traitées doivent être déterminées par la règlementation qui encadre leur traitement**. Lorsque le traitement constitue une ingérence importante dans les droits et libertés des personnes concernées, comme c'est le cas en l'espèce, **le législateur doit déterminer, au moins, les catégories de données, étant donné que les données précises qui feront l'objet du traitement peuvent être définies dans une norme de rang règlementaire**. En l'espèce, il peut être admis **que le nouvel article 122 § 4 de la loi télécom définit suffisamment les catégories de données** qui doivent être conservées, à savoir « *les données de localisation et les autres données de trafic nécessaires [afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine]* ». **La définition plus précise de ces données peut être déléguée au Roi, mais il est alors requis que le Roi intervienne**. Son intervention ne peut être facultative. En effet, tant que la règlementation ne comprend pas une définition plus précise des données à conserver, **l'exigence de prévisibilité n'est pas rencontrée**. Il en est d'autant plus ainsi que les notions de « fraude » et d'« utilisation malveillante du réseau » sont définies de manière assez large. Il est difficile dans ces circonstances pour les personnes concernées de prévoir quelles seront les données précises qui seront conservées en application de cette disposition. En outre, **lorsque le traitement est nécessaire au respect d'une obligation légale**, comme c'est le cas en l'espèce, il faut – comme l'Autorité l'a rappelé ci-dessus – que **tous les**

[85] L'Exposé des motifs justifie le caractère facultatif de cette habilitation législative comme suit : « *L'adoption de cet arrêté royal n'est pas obligatoire, au vu des défis suivants. D'abord, les fraudes évoluent significativement avec le temps. Certains types de fraude peuvent disparaître ou diminuer en importance alors que de nouveaux types de fraude peuvent voir le jour. Ensuite, les données que les opérateurs conservent pour lutter contre les fraudes peuvent être différentes selon le type de service de communications électroniques fourni, la taille de l'opérateur et les outils « anti-fraude » dont il dispose ou le type d'utilisateurs du service* ».

éléments qui permettent de circonscrire la portée de cette obligation soient déterminés par la norme imposant cette obligation, sans quoi le caractère contraignant de cette obligation pourra être remis en cause. Par ailleurs, et en tout état de cause, l'Autorité souligne que la conservation des données de trafic ne doit pas contenir ou permettre de déduire l'url spécifique des pages web visitées par les personnes concernées.

73. Ensuite, l'Autorité constate que le nouvel article 122 § 4 de la loi télécom impose aux opérateurs de conserver « *les données de localisation et les autres données de trafic nécessaires à cette fin, le temps nécessaire à cette fin et au minimum quatre mois* »[86], à l'exception **des données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles qui doivent être conservées pendant 12 mois**. L'Autorité comprend que la possibilité de conserver les données de localisation et autres données de trafic au-delà du délai minimal de 4 mois vise la situation où une conservation plus longue est nécessaire pour gérer un contentieux relatif à une fraude ou à une utilisation malveillante du réseau. **Il convient d'ajouter cette précision dans l'avant-projet de loi.**

5) Conservation des données pour assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte (nouvel article 122 § 4/1 de la loi télécom)

74. Le **nouvel article 122 § 4/1** de la loi télécom **impose** aux opérateurs de **conserver** et de **traiter** les **données de trafic** nécessaires pour assurer **la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques**, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

[86] À la suite d'une demande d'informations complémentaires, le délégué du Ministre a justifié le choix de cette durée minimale de 4 mois comme suit : « *Comme indiqué par l'exposé des motifs, la durée minimale de 4 mois a été retenue pour la finalité de lutte contre la fraude et l'utilisation malveillante du réseau, étant donné que la fraude peut avoir un impact sur la facturation de l'opérateur envers l'abonné (ou d'une entreprise envers l'abonné). Tel est le cas, par exemple, lorsqu'un tiers fait usage d'un service de communications électroniques au nom de l'abonné à son insu. Dans ce cas, l'auteur de la fraude est un tiers et la victime l'utilisateur final qui se verra facturer par l'opérateur des communications non souhaitées. La durée minimale de 4 mois de conservation tient compte d'un cycle complet de facturation (premier mois suivant la consommation du service), d'une durée de contestation minimale (de 15 jours à 1 mois, le deuxième mois suivant la consommation du service), d'une période de traitement de la contestation permettant un échange entre l'abonné et l'opérateur (le troisième mois suivant la contestation du service) et d'une période de retard possible dans ce traitement (le quatrième mois suivant la consommation). Il s'agit par conséquent d'une estimation de la durée de conservation des données nécessaire, dans la majorité des cas, aux fins de lutte contre la fraude et l'utilisation malveillante du réseau. Néanmoins, cela ne constitue pas en soi une durée maximale de conservation afin de permettre à chaque opérateur de déterminer, pour ce qui le concerne, une durée de conservation plus longue et ce, en prenant en considération ses spécificités et nécessités particulières. La durée nécessaire peut en effet dépendre de multiples facteurs propres à chaque opérateur et sur lesquels ceux-ci doivent continuer à bénéficier d'une certaine liberté, par exemple quant au degré précis de protection contre la fraude qu'ils entendent fournir à leurs clients (et aux éventuels services additionnels à cet égard), à la méthodologie employée et aux ressources allouées à la détection des fraudes et utilisations malveillantes du réseau* ». L'Autorité souligne que les arguments avancés par le délégué du Ministre pour justifier une durée de conservation de 4 mois sont convaincants.

75. Le nouvel article 122 § 4/1 de la loi télécom crée ainsi **une nouvelle obligation juridique de conservation et de traitement de données de trafic** afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques. Ces traitements reposent sur une base juridique au sens de l'article 6 du RGPD puisqu'ils sont « *nécessaires au respect d'une obligation légale à laquelle le responsable du traitement est soumis* » (article 6.1.c) du RGPD). Comme l'Autorité l'a rappelé ci-dessus, la norme qui impose l'obligation légale doit être **suffisamment claire et précise** pour que le responsable du traitement n'ait pas de marge d'appréciation quant à la façon de s'y conformer[87].

76. Le nouvel article 122 § 4/1 de la loi télécom **définit la finalité poursuivie par les nouveaux traitements de données qu'il impose** : il s'agit d'« *assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte* ». L'Autorité constate que **cette finalité répond à l'exigence de l'article 5.1.b) du RGPD**. Par ailleurs, l'Autorité reconnait que cette finalité est comprise dans la liste des **objectifs** qui peuvent justifier, **aux termes de l'article 15 § 1 de la Directive ePrivacy**, une limitation de la portée de l'obligation de garantir la confidentialité des données de trafic. Il s'agit, en l'espèce, de « *la prévention, la recherche, la détection ou la poursuite d'utilisations non autorisées du système de communications électroniques* » [88] et/ou de la sauvegarde de la « sécurité publique »[89].

77. Comme l'Autorité l'a rappelé ci-dessus, **il ne suffit toutefois pas que l'obligation de conservation des données poursuivie un objectif légitime, mais il faut également que cette obligation soit « rigoureusement »[90] nécessaire et proportionnée à cet objectif**.

78. À ce propos, l'Autorité constate que le nouvel article 122 § 4/1 de la loi télécom – comme le nouvel article 122 § 4 de la loi télécom sur lequel l'Autorité s'est prononcée plus haut – **impose aux opérateurs de conserver de manière systématique des données de trafic de l'ensemble des utilisateurs des moyens de communications électroniques**. Cette nouvelle obligation de conservation préventive et généralisée constitue **une ingérence particulièrement grave** dans les droits et libertés des personnes concernées. L'Autorité rappelle, comme elle l'a déjà fait ci-dessus, qu'en vertu du principe de proportionnalité une ingérence grave dans les droits et libertés des

[87] Groupe de travail « Article 29 », Avis *06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, p. 22.
[88] Selon la CJUE, « l'exception visant les utilisations non autorisées du système de communications électroniques […] apparaît concerner les utilisations qui remettent en cause l'intégrité ou la sécurité même de ce système » (CJUE, arrêt di 29 janvier 2008, affaire C-275/06, « Promiscuae »)
[89] Selon l'Exposé des Motifs, « *la sécurité des réseaux, qui se rattache à la sécurité publique, est essentielle pour la société dans son ensemble. Un incident au niveau du réseau d'un opérateur peut avoir des conséquences très dommageables sur de nombreux plans (vol ou perte de données, impact sur tous les services qui sont offerts à l'aide du réseau). L'importance de la sécurité des réseaux va croître dans le futur avec le développement de la 5G, dont seront dépendants de nombreux services et applications* ».
[90] Voyez le considérant 11 de la Directive ePrivacy

personnes concernées ne peut être justifiée que par la poursuite d'un objectif d'intérêt général suffisamment important. Or, comme l'Autorité l'a déjà souligné plus haut, la CJUE considère qu'une « *réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* »[91]. **L'Autorité doute dès lors de la proportionnalité de l'obligation prévue par l'article 122 § 4/1 de la loi télécom alors que l'objectif poursuivi par cette nouvelle obligation de conservation de données, s'il est légitime, ne semble pas, à première vue, présenter le même degré d'importance que la lutte contre la criminalité grave**. L'Autorité souligne, en outre, que l'avant-projet de loi prévoit que les différentes autorités identifiées par le nouvel article 127/1 de la loi télécom – dont « *les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne* » – pourront avoir accès à ces données[92]. Cette possibilité de permettre, notamment, aux autorités répressives d'avoir accès à toutes les données conservées par les opérateurs télécom en exécution de l'obligation qui leur est imposée par l'article 122 § 4/1 de la loi télécom renforce le doute de l'Autorité quant à la proportionnalité de cette obligation de conservation.

79. Par ailleurs, **l'Autorité s'interroge également sur la nécessité d'imposer une obligation de conservation préventive et systématique des données telle qu'elle est imposée par le nouvel article 122 § 4/1 de la loi télécom** afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques. Certes, les opérateurs doivent être en mesure de pouvoir traiter et conserver des données de trafic lorsque cela est nécessaire pour qu'ils puissent garantir la sécurité du réseau et de leurs services. **Mais l'Autorité se demande s'il est nécessaire de leur imposer une obligation de conservation des données à cette fin**. Actuellement, les opérateurs sont tenus par une obligation de prendre « *les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée, le cas échéant conjointement en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants. Des mesures sont notamment prises pour réduire au maximum les conséquences des incidents de sécurité pour les utilisateurs et les réseaux interconnectés* » (article 114 § 1 de la loi télécom[93]). Ils ont également la possibilité, « *dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques* », d'identifier intentionnellement les personnes concernées par une transmission d'information et de prendre connaissance intentionnellement de données en matière de

[91] CJUE, arrêt du 6 octobre 2020, § 141.
[92] Telle que cela ressort d'une lecture combinée des nouveaux articles 122 § 7 et 127/1 de la loi télécom
[93] Cette disposition transpose l'article 4 de la Directive ePrivacy.

communications électroniques (articles 124 et 125 de la loi télécom). Si le bon fonctionnement du réseau et la bonne exécution d'un service de communications électroniques l'exigent, les opérateurs disposent déjà de la possibilité de traiter les données de trafic nécessaires à cette fin (et de les conserver le temps nécessaire à cette fin). **En transformant la possibilité de conserver et de traiter ces données en une obligation de les conserver, l'avant-projet crée une ingérence plus importante dans les droits et libertés des personnes concernées, concernées en particulier par rapport à des services qui, actuellement, ne collecte et ne conserve pas ces données pour des raisons de protection de la vie privée et de sécurité. L'aggravation de cette ingérence doit être justifiée de manière rigoureuse.** L'Exposé des motifs et les informations complémentaires fournies par le délégué du Ministre justifient pourquoi les opérateurs doivent pouvoir traiter des données de trafic pour assurer la sécurité du réseau et le bon fonctionnement de leurs services. **Mais la raison pour laquelle il est nécessaire de passer d'une possibilité à une obligation n'apparait pas suffisamment développée et étayée dans l'Exposé des motifs.**

80. **L'Autorité invite dès lors le législateur à apprécier rigoureusement au regard de la jurisprudence de la CJUE, et à justifier, la mesure dans laquelle l'obligation de conserver les données de trafic nécessaires afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques est effectivement nécessaire et proportionnée aux objectifs qu'elle poursuit**.

81. Au-delà des interrogations fondamentales de l'Autorité concernant la nécessité et la proportionnalité de l'obligation imposée par le nouvel article 122 § 4/1 de la loi télécom, **l'Autorité a plusieurs remarques plus « ponctuelles » à émettre concernant la prévisibilité et la proportionnalité de certaines des modalités de cette obligation**.

82. L'Autorité rappelle, **qu'en vertu de l'exigence de prévisibilité**, **les données traitées doivent être déterminées** par la règlementation qui encadre leur traitement, en particulier lorsque l'ingérence est particulièrement importante, comme c'est le cas en l'espèce. Or l'article 122 § 4/1 de la loi télécom **identifie la catégorie des données[94]** qui doivent être conservées, mais **il ne détermine pas les données précises** qui doivent être conservées. Il n'habilite pas, non plus, le Roi à procéder à cette détermination. **L'exigence de prévisibilité n'est dès lors pas rencontrée**. L'avant-projet doit **soit déterminer lui-même** les données précises qui doivent être conservées, **soit déléguer au Roi** le soin de procéder à cette détermination[95]. En tout état de cause, l'Autorité souligne que la conservation

[94] Il s'agit des « *données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris l'origine de cette atteinte* »

[95] Comme l'Autorité l'a déjà souligné, cette exigence de précision est également imposée par le fait que la conservation de ces données repose sur « une obligation légale **»** (au sens de l'article 6.1.c) du RGPD). Or, dans une telle situation, tous les éléments

des données de trafic ne doit pas contenir ou permettre de déduire l'url spécifique des pages web visitées par les personnes concernées.

83. Ensuite, l'Autorité constate que le nouvel article 122 § 4/1 de la loi télécom **impose une durée de conservation de 12 mois,** étant entendu que les opérateurs « *peuvent **les conserver pour une durée plus longue, qui est limitée au strict nécessaire*** ». L'Autorité a **deux remarques** à formuler à ce propos.

(i) **Premièrement**, l'Autorité **s'interroge sur la proportionnalité de la durée de conservation de 12 mois**. L'Autorité se demande, en particulier, s'il ne pourrait pas être suffisant de conserver les données pendant un laps de temps plus court, en donnant la possibilité de prolonger cette durée uniquement si l'opérateur constate une atteinte à la sécurité ou au bon fonctionnement du réseau ou des services de communications électroniques ? **L'Autorité invite le législateur à apprécier, et, le cas échéant, à justifier à l'aide d'éléments concrets, la raison pour laquelle les données doivent être conservées pendant une durée de 12 mois**. Lors de cet exercice, le législateur doit prendre en compte le fait qu'aux termes de la loi télécom les opérateurs doivent veiller à être en mesure de détecter rapidement une atteinte à la sécurité des réseaux ou des services qu'ils fournissent.

(ii) **Deuxièmement,** l'Autorité note que le législateur entend permettre de prolonger la durée de conservation de 12 mois si cela est strictement nécessaire. L'Autorité comprend que cette possibilité vise la situation où une conservation plus longue de certaines données de trafic ou de localisation est nécessaire pour gérer un contentieux relatif à une attaque ou des actes portant atteinte à la sécurité du réseau ou au bon fonctionnement du service, étant entendu que seules les données nécessaires à la gestion du contentieux peuvent être conservées pour une durée plus longue. **Cette précision sera ajoutée à l'avant-projet.**

6) Conservation des données pour répondre à une obligation légale (nouvel article 122 § 4/2 de la loi télécom)

84. Le **nouvel article 122 § 4/2** de la loi télécom **impose** aux opérateurs de **conserver** et de **traiter** les **données de trafic** nécessaires **pour répondre à une obligation légale dans leur chef**, pour la durée nécessaire à cette fin.

qui permettent de circonscrire la portée de cette obligation – y compris donc les données à conserver – doivent être déterminés par la norme imposant cette obligation, sans quoi le caractère contraignant de cette obligation pourra être remis en cause.

85. **L'avant-projet doit préciser que cette obligation légale ne peut être imposée que par une norme législative formelle**. En effet, au vu de la gravité de l'ingérence causée par la conservation de données de trafic, il est requis que toute obligation de conservation de données soit imposée par une norme législative formelle qui en détermine, d'une manière prévisible, tous les éléments essentiels. À toutes fins utiles, l'Autorité souligne encore que cette norme législative devra également respecter les principes de nécessité et de proportionnalité, tels qu'ils sont interprétés par la CJUE.

7) Conservation des données de localisation autres que les données de trafic (nouvel article 123 de la loi télécom)

86. Le nouvel article 123 § 1 de la loi télécom **autorise** les **opérateurs de réseaux mobiles** à traiter et à conserver **des données de localisation autres que des données de trafic** dans les cas suivants :

- Lorsque cela **est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service**, les données étant conservées le temps nécessaire à cette fin ;

- Lorsque cela est **nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau**, les données étant conservées le temps nécessaire à cette fin ;

- Lorsque **les données ont été rendues anonymes** ;

- Lorsque **le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation** et que l'abonné ou, le cas échéant, l'utilisateur final, **y a donné son consentement** ;

- Lorsque **le traitement est nécessaire pour répondre à une obligation légale** dans le chef de l'opérateur.

87. Bien que l'Exposé des motifs indique que l'article 123 de la loi télécom transpose l'article 9 de la Directive ePrivacy, **l'Autorité constate que les situations dans lesquelles cette disposition autorise une conservation des données de localisation autres que des données de trafic sont plus nombreuses que celles qui sont mentionnées par l'article 9 de la Directive ePrivacy**. En effet, l'article 9 de la Directive ePrivacy n'autorise un traitement des données de localisation autres que des données de trafic uniquement après qu'elles aient été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée

nécessaire à la fourniture d'un service à valeur ajoutée. L'article 9 de la Directive ePrivacy ne prévoit pas le traitement et la conservation des données de localisation autres que les données de trafic qui sont nécessaires pour le bon fonctionnement et la sécurité du réseau ou du service, pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau ou pour répondre à une obligation légale dans le chef de l'opérateur. Toutefois, l'article 15 § 1 de la Directive ePrivacy autorise « [*l]es États membres [à] adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus […] à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* ». **Le législateur belge peut donc prévoir le traitement et la conservation de données de localisation autres que des données de trafic dans d'autres situations que celles prévues par l'article 9 de la Directive ePrivacy**, **<u>à condition</u>** que ces traitements **soient « nécessaires » et « proportionnés »** au regard de(s) (l') objectif(s) qu'ils poursuivent **et que la disposition légale qui les prévoit soit suffisamment prévisible** pour les personnes concernées.

88. À ce propos, l'Autorité constate **que l'Exposé des motifs ne justifie ni la nécessité ni la proportionnalité** des traitements de données de localisation autres que des données de trafic afin d'assurer **le bon fonctionnement et la sécurité du réseau ou du service**, ou afin de détecter ou analyser **les fraudes ou l'utilisation malveillante du réseau**[96]. L'Autorité invite dès lors le **législateur à apprécier rigoureusement, et le cas échéant à justifier à l'aide d'éléments concrets, la nécessité et la proportionnalité de ces traitements**. Par ailleurs, **afin de rencontrer l'exigence de prévisibilité**, l'avant-projet devra être revu afin de **déterminer**, au moins, les **conditions dans lesquelles les opérateurs pourront conserver et traiter ces données** et **les durées maximales de conservation** de ces données.

89. Concernant les traitements des données de localisation autres que des données de trafic **nécessaires au respect d'une obligation légale dans le chef de l'opérateur**, l'Autorité souligne que l'**avant-projet doit préciser –** au vu de la gravité de l'ingérence causée par la conservation de données de localisation – **que cette obligation légale ne peut être imposée que par une norme législative formelle**. À toutes fins utiles, l'Autorité souligne encore que cette norme législative devra également respecter les principes de nécessité et de proportionnalité, tels qu'ils sont interprétés par la CJUE.

[96] Concernant les objectifs poursuivis par ces traitements de données, l'Autorité a déjà pu souligner que ceux-ci répondaient à l'exigence de l'article 5.1.b) du RGPD et qu'ils étaient compris dans la liste des objectifs de l'article 15 § 1 de la Directive ePrivacy

90. Enfin, l'Autorité souligne que les données de localisation ne peuvent être que très difficilement rendues réellement anonymes lorsqu'elles sont conservées à un niveau individuel[97]. En effet, les opérateurs qui ont accès à des données de localisation qui se rattachent à une personne physique identifiée (et qui n'ont donc pas encore été rendues anonymes) peuvent aisément utiliser ces informations afin d'identifier, à travers des « *profiling attacks* »[98], les personnes auxquelles se rattachent les données de localisation qui ont été « anonymisées ».

8) Conservation des données de souscription et des données techniques permettant d'identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé (nouvel article 126 de la loi télécom) et des données d'identification des abonnés (nouvel article 127 de la loi télécom)

91. Le nouvel article 126 de la loi télécom **impose** aux « *opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques* » ainsi qu'aux « *opérateurs fournissant les réseaux de communications électroniques sous-jacents* » de **conserver les données de souscription** de l'abonné ainsi que **les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communication électronique employé, pour autant que ces opérateurs traitent ou génèrent déjà ces données dans le cadre de la fourniture des réseaux ou services de communication concernés**. Ces données, à l'exception des adresses IP dynamiques autres que celle qui a été utilisée pour souscrire au service, doivent être conservées à partir de la date d'activation du service et jusqu'à 12 mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé. Les adresses IP dynamiques autres que celle qui a été utilisée pour souscrire au service sont, pour leur part, conservées pendant 12 mois après la fin de la session.

92. Le nouvel article 126 § 2 **délègue au Roi** le soin de **déterminer les données à conserver** ainsi que les exigences auxquelles ces données doivent répondre. **L'arrêté du 19 septembre 2013**, que le projet d'arrêté soumis pour avis à l'Autorité modifie**, détermine la liste des données qui doivent être conservées** en exécution de l'article 126 de la loi télécom :

- Les fournisseurs **de services de téléphonie fixe accessibles au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

[97] Des données sont conservées à un niveau individuel lorsque les informations enregistrées sont liées à une personne. Au contraire, les informations, qui sont enregistrées de manière agrégée, ne contiennent que des informations liées à plusieurs personnes, par exemple, un pourcentage.
[98] Voyez, par exemple, Naini, F.M., Unnikrishnan, J., Thiran, P. and Vetterli, M., 2015. "Where you are is who you are: User identification by matching statistics". *IEEE Transactions on Information Forensics and Security*, 11(2), pp.358-372.

1° le numéro attribué à l'utilisateur final ;
2° les données personnelles de l'utilisateur final (qui sont définies comme « *les nom et prénom ainsi que les adresses de facturation et de livraison de l'utilisateur final* ») ;
3° la date de début de l'abonnement ou de l'enregistrement au service ;
4° le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit ;
5° en cas de transfert du numéro de l'utilisateur final auprès d'un autre fournisseur, l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré ;
6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
7° le numéro d'identification du terminal de l'utilisateur final, le cas échéant l'adresse « MAC (Media Access Control) » ou le « PEI (Permanent Equipment Identifier) ».

- Les fournisseurs d'un **service de téléphonie mobile accessible au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final ainsi que l'identité internationale d'abonné mobile (« International Mobile Subscriber Identity », IMSI ») ou « Subscription Permanent Identifier (SUPI) ») ;
2° les données personnelles de l'utilisateur final et le « Subscription Concealed Identifier (SUCI) » correspondant ;
3° la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final ;
4° la date et l'heure de la première activation du service, ainsi que l'identifiant cellulaire à partir duquel le service a été activé ;
5° les services annexes auxquels l'utilisateur final a souscrit ;
6° en cas de transfert de numéro auprès d'un autre opérateur, l'identité de l'opérateur d'origine de l'utilisateur final ;
7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
8° le numéro d'identification du terminal de l'utilisateur final (« International Mobile Equipment Identity », « IMEI », l'adresse « MAC (Media Access Control) » ou « Permanent Equipment Identifier (PEI) »).

- Les fournisseurs de service **d'accès à l'internet** accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° l'identifiant de l'utilisateur final, en ce compris le cas échéant le « Subscription Permanent Identifier (SUPI) » ;
  2° a) l'adresse IP ;
  b) en cas d'utilisation partagée d'une adresse IP, les ports attribués de l'adresse IP ainsi que la date et l'heure de l'attribution ;
  3° les données personnelles de l'utilisateur final, en ce compris le cas échéant le « Subscription Concealed Identifier (SUCI) » correspondant ;
  4° la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final ;
  5° l'adresse IP et le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final ;
  6° l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu'utilisateur final ;
  7° les services annexes auxquels l'utilisateur final a souscrit auprès du prestataire d'accès Internet public concerné ;
  8° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
  9° le numéro d'identification du terminal de l'utilisateur final, le cas échéant l'adresse « MAC (Media Access Control) » ou le « PEI (Permanent Equipment Identifier) ».

- Les fournisseurs d'un **service de courrier électronique par internet accessible au public,** les fournisseurs d'un **service de téléphonie par internet accessible au public** et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° l'identifiant de l'utilisateur final, en ce compris le cas échéant le « Subscription Permanent Identifier (SUPI) »
  2° l'adresse IP et le port source utilisés par l'utilisateur final ;
  3° les données personnelles de l'utilisateur final, en ce compris le cas échéant le « Subscription Concealed Identifier (SUCI) » correspondant ;
  4° la date et l'heure de la création du compte de courrier électronique ou de téléphonie par internet ;
  5° l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet ;

6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
7° sauf pour le service de courrier électronique par internet accessible au public, le numéro d'identification du terminal de l'utilisateur final, le cas échéant l'adresse « MAC (Media Access Control) » ou le « PEI (Permanent Equipment Identifier) ».

93. Le nouvel **article 127** de la loi télécom **impose**, pour sa part, aux opérateurs **d'identifier leurs abonnés** ou de collecter et conserver les données nécessaires, y compris, le cas échéant le numéro de registre national, pour que les autorités qui sont habilitées à obtenir cette identité puissent les identifier. Ces données doivent être **conservées pendant toute la durée d'activation** du service **et jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois** à l'aide du service utilisé. **Le Roi** est habilité – mais sans y être tenu – **à déterminer**, entre autres, **les données** et documents d'identification à collecter et à conserver par l'opérateur.

94. Les **données conservées en exécution des articles 126 et 127** de la loi télécom le sont **pour les autorités et les finalités suivantes** :

« *1° les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne ;*
2° les services de renseignement et de sécurité afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;
3° les autorités chargées d'apporter de l'aide aux personnes, en ce compris le service de médiation pour les télécommunications pour ce qui concerne l'utilisation malveillante du réseau, les services d'urgence et la Cellule des personnes disparues de la Police Fédérale ;
4° l'Institut dans le cadre de la mise en œuvre et le contrôle de la présente loi ;
5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service »[99].

95. Il ressort de la jurisprudence de la Cour de **justice qu'une mesure législative prise en application de l'article 15 de la Directive ePrivacy peut imposer aux opérateurs de conserver les données nécessaires à l'identification des utilisateurs d'un service de communications électroniques** si cette conservation s'avère nécessaire à la poursuite de l'un des objectifs énoncés par l'article 15.1 de la Directive ePrivacy.

[99] Nouvel article 127/1 de la loi télécom

96. Concernant **les données portant sur l'identité civile des abonnés**, la CJUE estime que leur conservation – sans délai particulier – et leur communication à la seule fin de l'identification de l'utilisateur concerné peut être justifiée par la poursuite de l'un des objectifs listés à l'article 15 § 1 de la Directive ePrivacy sans qu'il soit nécessaire que cet objectif revête une importance particulière (comme, par exemple, la lutte contre la criminalité grave). **La conservation des données relatives à l'identité civile des abonnés** afin de permettre leur identification **ne constitue pas**, aux yeux de la Cour, **une ingérence grave** dans les droits fondamentaux des personnes concernées.

97. En revanche, la Cour procède à une **appréciation plus stricte concernant la conservation de l'adresse IP des abonnés**. Cette donnée, qui est nécessaire à l'identification de la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée, permet également – si elle combinée aux adresses IP destinataires – d'effectuer un traçage exhaustif du parcours de navigation de l'internaute et ainsi d'établir son profil détaillé. La Cour estime dès lors **que la conservation généralisée des adresses IP attribuées à la source d'une connexion constitue une ingérence grave** dans les droits fondamentaux des internautes. Elle admet néanmoins qu'une telle conservation préventive généralisée puisse s'avérer nécessaire parce que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. Toutefois, eu égard à la gravité de l'ingérence, la Cour estime que **seul un objectif suffisamment important, à l'instar de la lutte contre la criminalité grave, peut justifier une telle mesure de conservation généralisée des adresses IP**[100].

98. L'Autorité prend note de la volonté du législateur d'imposer la conservation des données de souscription et d'identification des abonnés ainsi que des données techniques permettant leur identification, l'identification de l'équipement terminal utilisé et du service de communications électroniques utilisé. **Une telle conservation des données peut, en effet, s'avérer, à certaines conditions, nécessaire et proportionnée aux objectifs qu'elle poursuit**.

99. Toutefois, l'Autorité souligne que le niveau d'ingérence causé par la conservation de ces données varie selon le type de donnée sur laquelle elle porte. La conservation **des données qui permettent un traçage des activités des abonnés** constitue une **ingérence grave** dans les droits fondamentaux des personnes concernées alors que la conservation des données qui identifient les abonnés sans permettre le traçage de leur activité constitue une ingérence dans leur vie privée qui ne doit pas être qualifiée de grave. L'Autorité rappelle que le **principe de proportionnalité exige que la conservation des données qui permettent un traçage des activités des abonnés,** pour d'autres finalités que l'acheminement de la communication électronique **et leur utilisation**

[100] CJUE, arrêt du 6 octobre 2020, § 156

ultérieure éventuelle pour les motifs énoncés à l'articles 15 de la Directive ePrivacy **soient soumises à des conditions plus strictes afin que l'ingérence qu'elles créent reste strictement proportionnée aux objectifs poursuivis.**

100. Concernant **les adresses IP attribuées à la source d'une communication**, la CJUE estime que leur conservation ne peut avoir lieu qu'en vue de la poursuite d'objectifs suffisamment importants, que la durée de leur conservation doit être limitée au strict nécessaire au regard de ces objectifs et qu'il doit exister conditions et garanties strictes quant à l'exploitation de ces données[101]. **L'avant-projet devra dès lors être revu afin de prévoir que les adresses IP attribuées à la source d'une connexion ne pourront être conservées qu'afin de permettre la poursuite d'objectifs particulièrement importants qui devront y être précisés**.

101. L'Autorité constate, en outre, que **ni l'avant-projet de loi ni le projet d'arrêté ne précisent que seules les adresses IP attribuées à la source d'une communication doivent être conservées en exécution du nouvel article 126 de la loi télécom**, à l'exclusion des adresses IP du destinataire de cette communication. **L'avant-projet de loi et le projet d'arrêté seront revus afin d'ajouter cette précision**.

102. L'avant-projet de loi – et le projet d'arrêté qui l'exécute – **prévoient également la conservation des numéros d'identification des terminaux des utilisateurs finaux.** Sauf erreur, l'exigence de conservation de cette donnée est nouvelle. Les numéros d'identification des terminaux des utilisateurs finaux constituent un identifiant unique des équipements terminaux qui permettent de « tracer » un terminal à travers l'ensemble des services de communications électroniques qu'il utilise. **La conservation préventive et systématique de ces numéros constitue dès lors une ingérence importante dans les droits au respect de la vie privée et à la protection des données à caractère personnel**. Leur conservation doit dès lors être soumise **au strict respect des conditions de nécessité et de proportionnalité** au regard des objectifs poursuivis. À cet égard, la jurisprudence de la Cour de Luxembourg concernant la conservation généralisée des adresses IP peut être utilement mobilisée pour déterminer les conditions que doit rencontrer une mesure législative qui impose la conservation de telles données d'identification unique des équipements terminaux des abonnés. Le délégué du Ministre, dans une réponse à une demande d'informations complémentaires, souligne d'ailleurs, lui aussi, que le raisonnement suivi par la CJUE à propos des adresses IP « *peut être suivi quant aux autres données techniques nécessaires pour identifier l'utilisateur final, l'équipement terminal, le service de communication électroniques employé* ». **Ainsi, la conservation de ces données ne devrait être imposée qu'afin de poursuivre un objectif présentant une**

[101] CJUE, arrêt du 6 octobre 2020, § 156. Certes, ces exigences portent sur la conservation généralisée et indifférenciée des adresses IP et non de toutes données techniques permettant l'identification de l'abonné ou de son équipement terminal, mais comme le délégué du Ministre l'a indiqué lui-même, dans une réponse à une demande d'informations complémentaires, « *Le même raisonnement peut être suivi quant aux autres données techniques nécessaires pour identifier utilisateur final, l'équipement terminal, le services de communication électroniques employé* ».

importance particulière (comme la lutte contre la criminalité grave), **la durée de leur conservation devrait être strictement limitée** au regard de cet objectif et il faudrait prévoir des **conditions et des garanties strictes quant à l'exploitation de ces données**[102]. **L'avant-projet de loi et le projet d'arrêté**, qui ne rencontrent pas ces exigences, **devront donc être adaptés afin d'y répondre.**

103. Au-delà de ces remarques portant sur le principe des obligations de conservation des données de souscription et d'identification des abonnés ainsi que des données techniques permettant leur identification, l'identification de l'équipement terminal utilisé et du service de communications électroniques utilisé, l'Autorité a **deux remarques plus ponctuelles** à émettre relativement aux différentes dispositions qui encadrent ces obligations de conservation.

104. Premièrement, l'Autorité constate que le **nouvel article 127 § 2** de la loi télécom **entend permettre l'utilisation d'une technologie de reconnaissance faciale** à des fins d'identification de l'abonné**. Le recours à des techniques de reconnaissance faciale pour identifier les abonnés excède ce qui est nécessaire dans une société démocratique** alors qu'il existe, en Belgique, d'autres moyens plus surs et moins intrusifs (l'utilisation de l'eID ou d'Itsme) pour authentifier électroniquement des personnes. Cette possibilité **d'utiliser la reconnaissance faciale** comme moyen d'identification sera dès lors supprimée de l'avant-projet de loi. L'Autorité souligne, en outre**, que l'utilisation d'autres données biométriques, à l'instar des empreintes digitales, excèderait également ce qui est nécessaire et admissible dans une société démocratique**.

105. Ensuite, le **nouvel article 127 § 3** de la loi télécom habilite le Roi, **mais de manière facultative**, à déterminer les données et documents d'identification à collecter et à conserver par l'opérateur. L'exigence de prévisibilité requiert que ces données et documents soient déterminés. **Soit le législateur procède lui-même à cette détermination, soit il délègue au Roi le soin d'y procéder, mais** cette **habilitation** doit alors présenter un caractère **obligatoire**. **L'avant-projet de loi sera revu en ce sens.**

[102] CJUE, arrêt du 6 octobre 2020, § 156.

9) Conservation ciblée des données de trafic et de localisation aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique (nouvel article 126/1 de la loi télécom)

106. Le nouvel article 126/1 de la loi télécom **impose** aux opérateurs de conserver, en principe, **pendant 12 mois**[103], les **données de trafic et de localisation** de **toutes les communications** effectuées **à partir**, ou **vers**, une des **zones géographiques** qu'il liste. L'avant-projet de loi précise toutefois que les opérateurs ne doivent conserver ces données que s'ils les génèrent ou les traitent déjà dans le cadre de la fourniture des services de communications électroniques qu'ils offrent ou des réseaux de communications électroniques qu'ils mettent à disposition[104]. Cette conservation est imposée *« aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique* ». Ainsi, le nouvel article 126/1 de la loi télécom entend imposer, en vue de **poursuivre des objectifs présentant une importance particulière**, à l'instar de la lutte contre la criminalité grave, **une conservation préventive des données de trafic et de localisation qui soit ciblée en fonction de critères géographiques**. Une telle **obligation de conservation ciblée** est, **dans son principe**, **conforme aux exigences européennes** telle qu'interprétées par la CJUE.

107. L'Autorité constate toutefois que **le nouvel article 126/1 de la loi télécom appelle plusieurs commentaires** au regard des principes fondamentaux de la protection des données.

- ***Commentaires portant sur le nouvel article 126/1 § 2 de la loi télécom :***

108. Le nouvel article 126/1 § 2 de la loi télécom **détermine les catégories de données** qui doivent être conservées par les opérateurs. Il s'agit des données suivantes :

> « *1° les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau ;*

[103] A moins qu'une autre durée soit prévue par ce nouvel article 126/1 de la loi télécom. Cette disposition prévoit des durées de conservation plus courtes dans certaines circonstances. Voyez le nouvel article 126/1 § 3, 1° de la loi télécom.
[104] Il est précisé, dans l'Exposé des motifs, que « *les données ne sont conservées par les opérateurs concernés que dans la mesure où ces données ont été générées ou traitées par eux dans le cadre de la fourniture des services de communication concernés, et uniquement dans les zones géographiques prédéfinies. En d'autres termes, il n'y a aucune obligation de conserver les données lorsque celles-ci :*
1° ne sont pas générées ou traitées par les opérateurs concernés,
2° ne sont pas générées ou traitées dans les zones géographiques déterminées au paragraphe 3 ».

2° les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination ;
3° les données des appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :
i° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs ; ou
ii° en ce qui concerne les données de l'internet, journalisées par ces opérateurs.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre et du ministre de la Justice, du ministre de l'Intérieur, du ministre de la défense, et du ministre, après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver et peut fixer les exigences auxquelles ces données doivent répondre »

109. Tout d'abord, l'Autorité constate **que le nouvel article 126/1 § 2 de la loi télécom utilise le concept de « *données de communication* »** pour déterminer les catégories de données qui doivent être conservées alors que les autres dispositions de la loi télécom qui autorisent ou imposent une conservation des données utilisent, pour leur part, les concepts de « *données de trafic* », « *données de localisation* » ou « *données de localisation autres que les données de trafic* ». Ces trois dernières catégories de données sont définies, directement ou indirectement, par la loi télécom ; ce qui n'est pas le cas pour la notion de « données de communication ». **Cette absence de définition nuit à la prévisibilité de la loi**. Il en est d'autant plus ainsi que l'utilisation d'un concept différent pour identifier les données qui doivent être conservées en vertu du nouvel article 126/1 de la loi télécom laisse supposer que la notion de « données de communication » viserait d'autres types de données que les « données de trafic » et « les données de localisation ». À la suite d'une demande d'informations complémentaires, le délégué du Ministre a indiqué que « *La notion de données de communication est un sous-ensemble de la notion de trafic. Il s'agit de données qui donne des informations sur l'auteur ou le destinataire de la communication (qui a contacté qui/quoi)* ». **Afin de respecter l'exigence de prévisibilité**, **l'avant-projet de loi doit être revu afin d'y définir la notion de « données de communication »**.

110. Ensuite, **une même remarque doit être formulée à propos de la notion « données des appels infructueux »**. En effet, bien que la notion d'« appels infructueux » soit définie dans la loi télécom[105], la notion de « données des appels infructueux » ne l'est pas. À la suite d'une demande d'informations complémentaires, le délégué du Ministre a indiqué que « *Les 'données des appels infructueux' visent les données de trafic liées aux appels infructueux. Il peut s'agir,*

[105] Cette notion est définie par l'article 2 de l'avant-projet de loi qui insère un 74° à l'article 2 de la loi télécom : « toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau ».

par exemple, de la date et heure de cet appel et du numéro de l'appelant ». **Afin de répondre à l'exigence de prévisibilité de la loi, l'avant-projet de loi doit être revu afin d'y inscrire cette précision : la notion de « données des appels infructueux » sera remplacée par la notion de « données de trafic des appels infructueux ».**

111. Le nouvel article 126/1 § 2 **délègue au Roi** le soin de déterminer les données à conserver. Cette habilitation est « obligatoire » puisque le Roi est tenu de fixer les données à conserver. **L'Autorité estime qu'une telle délégation au Roi est admissible au regard du principe de légalité** : les catégories de données sont définies avec suffisamment de précision dans la loi (à condition toutefois que l'avant-projet de loi soit modifié pour répondre aux remarques émises par l'Autorité dans les paragraphes précédents) et la matière présente une technicité qui justifie de déléguer au Roi le soin de déterminer les données de trafic précises qui doivent être conservées.

112. **L'arrêté royal du 19 septembre 2013,** qui est modifié par le projet d'arrêté soumis pour avis à l'Autorité, **exécute le nouvel article 126/1 § 2 de la loi télécom** et fixe les données que les opérateurs doivent conserver en exécution de cette disposition :

- Les fournisseurs **de services de téléphonie fixe accessibles au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent, « **au minimum** », les données suivantes :

  1° l'identification du numéro de téléphone de l'appelant et de l'appelé ;
  2° la localisation du point de terminaison du réseau de l'appelant et de l'appelé
  3° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré ;
  4° la date et l'heure exacte du début et de la fin de l'appel ;
  5° la description du service de téléphonie utilisé.

- Les fournisseurs d'un **service de téléphonie mobile accessible au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent, « **au minimum** » les données suivantes :

  1° l'identification du numéro de téléphone de l'appelant et de l'appelé ;
  2° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré ;

3° l'identité internationale d'abonné mobile (« International Mobile Subscriber Identity », « IMSI ») ou « Subscription Permanent Identifier » (SUPI) de l'appelant et de l'appelé
4° l'identité internationale d'équipement mobile (« International Mobile Equipment Identity », « IMEI ») ou « Permanent Equipment Identifier (PEI) » du terminal mobile de l'appelant et de l'appelé ;
5° la date et l'heure exacte du début et de la fin de l'appel ;
6° la localisation du point de terminaison du réseau au début et à la fin de chaque connexion ;
7° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée
8° les caractéristiques techniques du service de téléphonie utilisé.

- Les fournisseurs de service **d'accès à l'internet** accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent, « **au minimum** » les données suivantes :

  1° l'identifiant de l'utilisateur final ;
  2° l'identification et la localisation des points de terminaison du réseau utilisés par l'utilisateur final du début à la fin d'une connexion ou d'une communication ;
  3° la date et l'heure de l'ouverture et de la fermeture d'une session du service d'accès à l'internet ;
  4° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée ;
  5° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée ;

- Les fournisseurs d'un **service de courrier électronique par internet accessible au public,** les fournisseurs d'un **service de téléphonie par internet accessible au public** et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° l'identifiant de l'utilisateur final du compte de courrier électronique ou de téléphonie par internet, ainsi que le numéro ou l'identifiant du destinataire prévu de la communication ;
  2° le numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public dans le cadre d'un service téléphonique par internet ;
  3° a) l'adresse IP et le port source utilisés par l'utilisateur final ;

b) l'adresse IP et le port source utilisés par le destinataire ;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service de courrier électronique ou de téléphonie par internet ;

5° la date et l'heure de la connexion établie à l'aide du compte de téléphonie par Internet ;

6° les caractéristiques techniques du service utilisé.

113. L'Autorité constate que **les listes de données établies par l'arrêté du 19 septembre 2013 ne sont pas exhaustives** puisque l'arrêté royal indique que les « *fournisseurs […] conservent au minimum les données suivantes […]* »[106]. **L'exigence de prévisibilité ne peut se satisfaire d'une détermination non-exhaustive des données à conserver**. Le **projet d'arrêté sera revu** afin de veiller à ce que l'arrêté royal du 19 septembre 2013 détermine de manière exhaustive les données qui doivent être conservées par les opérateurs.

114. Par ailleurs, l'Autorité souligne que la conservation des données de trafic ne doit pas contenir ou permettre de déduire l'url spécifique des pages web visitées par les personnes concernées

115. L'Autorité n'a **pas d'autre remarque** concernant les données déterminées par l'arrêté royal du 19 septembre 2013.

- ***Commentaires portant sur le nouvel article 126/1 § 3 de la loi télécom :***

116. Le nouvel article 126/1 § 3 de la loi télécom identifie **les différentes zones géographiques dans lesquelles les opérateurs doivent conserver, de manière préventive, les données de trafic se rapportant aux communications qui y sont effectuées** (parce que l'origine ou la destination de la communication s'y trouve).

117. Il ressort de la jurisprudence européenne qu'une mesure législative peut imposer une obligation de conservation préventive « ciblée » sur base de critères géographiques afin de sauvegarder la sécurité nationale, de lutter contre la criminalité grave, de prévenir des menaces graves contre la sécurité publique et de sauvegarder des intérêts vitaux d'une personne physique. La CJUE juge, en effet, qu'une telle mesure respecte, en principe, le principe de proportionnalité. **Il convient toutefois de veiller à ce que les critères retenus par l'avant-projet de loi pour déterminer les zones géographiques dans lesquelles une obligation de conservation des données de trafic est imposée de manière préventive n'aboutissent pas à réintroduire, *de facto*, une obligation de conservation généralisée et indifférenciée des données de trafic**

[106] C'est l'Autorité qui souligne.

118. Pour rappel, la CJUE considère que les Etats ne peuvent imposer une telle obligation de conservation généralisée et indifférenciée des données de trafic que lorsque qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. La CJUE précise que la sécurité nationale correspond à l'intérêt primordial de protéger les fonctions essentielles de l'Etat et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme[107].

119. Le **nouvel article 126/1 § 3, 1° de la loi télécom** prévoit qu'une obligation de conservation des données est imposée pour les « *arrondissements judiciaires dans lesquels au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an ont été constatées durant l'année sur une moyenne des trois années calendriers précédentes celle en cours* » ou pour les « *zones de police, dans lesquelles, au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an ont été constatées sur une moyenne des trois années calendriers précédentes celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier précédente celle en cours, moins de 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an sur une moyenne de trois années précédente celle en cours ont été constatées* ».

120. L'article 90ter § 2 du CIC comprend une longue liste d'infractions. Il s'agit des infractions pour lesquelles « *le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci* ». Comme l'indique le délégué du Ministre dans une réponse à des demandes d'informations complémentaires, cette liste « *wordt over het algemeen beschouwd als de lijst met de meest zware vormen van criminaliteit. De lijst wordt in het wetboek meerdere keren gebruikt als drempel voor de proportionaliteitsvereiste voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer. Dit is o.a. het geval voor:*

- *De proactieve recherche (artikel 28bis, § 2)*
- *Het blokkeren van banktegoeden (artikel 46quater, § 2, tweede lid)*
- *De inkijkoperatie (artikel 46quinquies/89ter)*
- *De infiltratie (artikel 47octies)*
- *De observatie met gebruik van technische middelen om zicht te krijgen in de woning van een advocaat of een arts (artikel 56bis)*

[107] CJUE, arrêt du 6 octobre 2020, § 135.

- *De volledige anonimiteit van getuigen (artikel 86bis)*
- *De onderschepping en kennisname van private elektronische communicatie en de geheime zoeking in een informaticasysteem (artikel 90ter)*
- *Het toekennen van bijzondere beschermingsmaatregelen aan bedreigde getuigen (artikel 104, § 2)*
- *Het toekennen van bijzondere beschermingsmaatregelen aan bedreigde personen die een openbaar ambt uitoefenen (artikel 111quater, § 1, tweede lid)* ».

121. **L'Autorité prend note du choix du demandeur d'utiliser cette liste pour définir ce qui relève de la « criminalité grave ».**

122. Elle **s'interroge, en revanche, sur le choix du seuil de « 3 infractions 90ter par 1000 habitants par an »** pour caractériser une zone comme étant particulièrement exposée à la commission d'actes de criminalité grave. L'Exposé des motifs indique le nombre d'infractions totales qui doivent être constatées dans un arrondissement judiciaire pour qu'une obligation de conservation des données y soit imposée, mais il ne donne pas les statistiques relatives aux nombres d'infractions « 90ter » ayant effectivement été constatées dans les différents arrondissements judiciaires. L'Autorité a demandé à pouvoir obtenir ces statistiques afin d'être en mesure d'évaluer si le seuil retenu aboutit à recréer, *de facto*, une obligation généralisée et indifférenciée des données de trafic de l'ensemble des utilisateurs d'un moyen de communications électroniques. Malgré sa demande, cette information ne lui a pas été communiquée. **L'Autorité n'est dès lors pas en mesure d'apprécier la pertinence et la proportionnalité du critère retenu**. **Le législateur devra justifier le seuil qu'il retient et démontrer que celui-ci n'aboutit pas à réintroduire, *de facto*, une obligation de conservation généralisée et indifférenciée des données sur la (quasi-)totalité du territoire national**. Certes, le critère retenu (une moyenne de 3 infractions 90ter par 1000 habitants par an) est un critère dynamique et il n'est dès lors pas possible de déterminer, une fois pour toutes, s'il aboutit à recréer, *de facto*, une obligation de conservation généralisée et indifférenciée des données sur la (quasi-)totalité du territoire national. Mais **le législateur doit veiller à ce que l'impact pratique de ce seuil soit proportionné au regard des statistiques actuelles** ; ce qui ne serait pas le cas s'il aboutissait à placer, lors de l'entrée en vigueur de l'avant-projet de loi, l'entièreté (ou presque) du territoire ou de la population « sous surveillance ». **Le législateur doit réaliser une analyse rigoureuse et quantitative de la proportionnalité du critère/seuil retenu dans l'avant-projet de loi.**

123. L'avant-projet de loi prévoit que « *les statistiques utilisées proviennent de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police* » (ci-après « la B.N.G »). **L'Autorité en prend note, mais elle souligne que le législateur doit toutefois être en mesure d'attester que la B.N.G est la base de données la plus adéquate à cette fin**. L'Autorité

s'interroge, en effet, sur la pertinence d'utiliser la B.N.G alors que cette base de données est tenue par la police qui aura naturellement, au vu de sa mission légale, une propension à y faire figurer toutes ses suspicions d'infractions 90ter et/ou, comme l'a souligné le C.O.C. dans son avis du 21 mai 2020, à qualifier trop facilement une suspicion d'infraction comme une suspicion de délit grave au sens de l'article 90ter du C.I.C**. Dans ce contexte, l'Autorité estime qu'il serait plus adéquat d'utiliser une base de données dont la qualité des données statistiques est encadrée par la loi, à l'instar de la loi du 4 juillet 1962 relative à la statistique publique**[108].

124. Afin d'éviter que les services de police puissent être tentés de qualifier « trop facilement » une suspicion d'infraction comme un suspicion d'une infraction grave au sens de l'article 90ter du C.I.C, l'Autorité considère, en outre, que **le seuil** retenu pour déterminer si la zone est particulièrement exposée à de la « criminalité grave » **doit être calculé en tenant compte du nombre d'infractions ayant abouti à une condamnation par les tribunaux**, et non du nombre d'infractions ayant été constatées par les services de police. Le recours au nombre de condamnations offre, en effet, une plus grande garantie que la conservation des données de trafic sera « activée », comme l'exige la CJUE, « *sur la base d'éléments objectifs et non discriminatoires* »[109].

125. Le nouvel article 126/1 § 3, 3° de la loi télécom liste 16 catégories de « *zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave* ». Le nouvel article 126/1 § 3, 4° de la loi télécom liste 14 catégories de « *zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population* ». Le nouvel

[108] L'article 1er bis de la loi du 4 juillet 1962 dispose que les « *statistiques sont régies par les principes suivants :*
1° Principe de licéité et de loyauté :
a) la collecte et le traitement des données se fondent soit sur une base légale ou réglementaire, soit sur le consentement du déclarant au sens de l'article 1er, § 8, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, sous réserve des dispositions particulières prévues dans la présente loi ;
b) la collecte loyale suppose la bonne information du déclarant au sujet de la collecte et du traitement des données. Le déclarant a le droit d'obtenir des informations concernant le fondement juridique, la finalité de la collecte et les mesures de protection adoptées ;
2° Principe de finalité :
a) les données individuelles sont utilisées exclusivement à des fins statistiques, à moins que le déclarant n'ait, sans équivoque, donné son consentement à ce que les données soient utilisées à d'autres fins ;
b) les données collectées à une fin statistique déterminée ne peuvent être utilisées à d'autres fins statistiques que si ces dernières sont compatibles avec la finalité statistique originaire ;
c) les données collectées et traitées à des fins statistiques ne peuvent pas être utilisées pour compléter ou corriger les fichiers de données à finalité non-statistique, notamment administratives ;
d) aucune décision ayant pour objet ou pour effet d'affecter la situation individuelle du déclarant, ne peut être prise sur base de données individuelles recueillies à l'occasion de la réalisation d'une statistique ;
3° Principe de proportionnalité :
a) lors du choix de la méthode de collecte, la priorité est accordée à la collecte secondaire par rapport à la collecte primaire. En toute hypothèse, la collecte s'opèrera par sondage de préférence à une collecte exhaustive et les enquêtes volontaires sont à privilégier par rapport aux enquêtes obligatoires ;
b) les données sont adéquates, pertinentes et non excessives au regard de la finalité statistique déterminée, c'est-à-dire que la collecte et le traitement des données sont limités aux seules données nécessaires aux fins statistiques poursuivies ;
4° Principe d'impartialité, d'objectivité et d'indépendance professionnelle :
a) les statistiques doivent être produites et diffusées dans le respect de l'indépendance scientifique et de manière objective, professionnelle et transparente plaçant tous les utilisateurs sur un pied d'égalité ;
b) la production et la diffusion des statistiques doivent être assurées par un organisme qui dispose d'une indépendance professionnelle à l'égard aussi bien des autres services et organismes politiques, réglementaires ou administratifs que des opérateurs du secteur privé ».
[109] CJUE, arrêt du 6 octobre 2020, § 150.

article 126/1 § 3, 5° de la loi télécom liste 5 catégories de « *zones où il y a une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national* ». À chaque fois, l'avant-projet de loi autorise le Roi à fixer d'autres zones par arrêté royal. L'Autorité a deux remarques à formuler à ce propos :

(i) Premièrement, l'Autorité constate que l'avant-projet de loi fait le choix de retenir de nombreux lieux pour y imposer une conservation préventive des données de trafic des communications qui y sont effectuées (soit que l'origine de la communication s'y trouve, soit que le destinataire de la communication s'y trouve). **L'Autorité souligne que le législateur doit bien veiller, au cours de la délibération précédant le vote, à apprécier la nécessité et la proportionnalité de la sélection des différents lieux retenus**[110]. Il importe, en tout état de cause, que cette sélection de lieux n'aboutisse pas à réintroduire, *de facto*, une obligation de conservation indifférenciée des données d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique.

(ii) Deuxièmement, et en tout état de cause, **le principe de légalité** consacré par l'article 22 de la Constitution **s'oppose à ce que le législateur puisse déléguer au Roi la possibilité d'étendre l'obligation de conservation à d'autres lieux** que ceux identifiés par l'avant-projet de loi. L'avant-projet de loi **sera modifié afin de supprimer cette possibilité**.

126. Enfin, l'Autorité estime nécessaire **qu'une transparence soit assurée** quant (1) **au pourcentage du territoire national soumis à l'obligation de conservation préventive** imposée en vertu du nouvel article 126/1 de la loi télécom et quant (2) au **pourcentage de la population concernée par cette obligation**. Une telle transparence permettrait de contrôler que les critères retenus par le législateur n'ont pas abouti à réintroduire, *de facto*, une obligation de conservation généralisée et indifférenciée des données de trafic et de localisation à des fins de lutte contre la criminalité grave alors qu'une telle obligation a été jugée disproportionnée par la CJUE. **Ces statistiques doivent être reprises dans le rapport que le Ministre des**

[110] L'Autorité se demande, par exemple, s'il est effectivement nécessaire et proportionné de prévoir une conservation des données de trafic de toutes les communications effectuées à partir de ou vers les autoroutes ou les parkings publics attenants aux autoroutes. Le délégué du Ministre indique, à la suite d'une demande d'informations complémentaires, que « *les autoroutes constituent le réseau de transport routier essentiel de notre pays. C'est grâce à celui-ci que l'approvisionnement en nourriture, énergie, etc., est assurée dans tout le pays. Il est également le réseau principal utilisé par les services qui délivrent une aide urgente à la population. Les parkings autoroutiers font partie intégrante du réseau autoroutier, ils constituent la zone de délestage de l'autoroute et sont, pour la plupart, la zone de ravitaillement en carburant des véhicules qui empruntent ces autoroutes. Vu les particularités des autoroutes (voies à grandes vitesses sans possibilité d'arrêt autre que la bande d'urgence), les parkings autoroutiers sont également des zones d'échange, de repos, etc. Le code de la route prévoit, en son article 21.4, que l'on ne peut mettre un véhicule à l'arrêt ou en stationnement que sur les aires de stationnement indiquées par le signal. La sécurité des parkings d'autoroute est importante non seulement pour les chauffeurs de camions, mais aussi pour tous les utilisateurs de ces autoroutes* ». Ces éléments ne démontrent toutefois pas la nécessité et la proportionnalité d'une obligation de conservation imposée pour les communications effectuées à partir de et vers les autoroutes.

télécommunications et le Ministre de la Justice doivent transmettre annuellement à la Chambre des représentants en vertu du nouvel article 127/2 § 1er de la loi télécom. Elles pourraient également être publiées sur le site Internet de l'IBPT, lequel doit déjà, aux termes du nouvel article 127/1 § 2 de la loi télécom, reprendre des informations générales concernant l'accès des autorités aux données conservées par les opérateurs.

127. Plus généralement, il est **essentiel que le rapport annuel transmis à la Chambre comprenne toutes les données nécessaires pour permettre une évaluation de l'efficacité et de la proportionnalité des différentes mesures de conservation** des données de trafic et de localisation. Dans cette perspective, **le rapport annuel devra, au moins, reprendre les données suivantes** :

- Les types et la quantité de données de trafic et de localisation collectées par les opérateurs en exécution des dispositions de la loi télécom et du C.I.C. (y compris le pourcentage du territoire et de la population concernée par une conservation des données en exécution du nouvel article 126/1 de la loi télécom) ;
- Le nombre de fois où une autorité a demandé à avoir accès aux données conservées par les opérateurs ;
- Les raisons pour lesquelles les autorités ont demandé (et obtenu) un accès aux données conservées par les opérateurs (sans, bien entendu, rentrer dans un exposé détaillé et concret) et des informations permettant d'établir l'utilité de cet accès.

L'avant-projet de loi sera revu afin de compléter les informations qui doivent être reprises dans le rapport annuel.

- ***Commentaires portant sur le nouvel article 126/1 § 4 de la loi télécom :***

128. Le nouvel article 126/1 § 4, alinéa 1er de la loi télécom prévoit que « *Les opérateurs conservent les données pour toutes les communications effectuées à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone* »[111]. **Afin d'assurer la clarté et la précision requise, l'avant-projet de loi précisera que « *les données* » sont les « *données visées au § 2* ».**

129. Le nouvel article 126/1 § 4, dernier alinéa prévoit que *« Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques* ». **Cette disposition est problématique au regard du principe de minimisation des données et, plus fondamentalement, du principe de la proportionnalité** qui doit régir

[111] C'est l'Autorité qui souligne.

toute mesure de conservation des données. Elle risque, en effet, d'aboutir à une conservation des données qui aille au-delà de ce qui est nécessaire et proportionné au regard des objectifs poursuivis par cette conservation. Le principe de proportionnalité, tel qu'il est interprété par la CJUE, s'oppose à ce que les opérateurs puissent conserver, en exécution de l'article 126/1 de la loi télécom, les données de trafic relatives à des communications qui sont effectuées en dehors des zones géographiques délimités par ladite disposition. Il en est d'autant plus ainsi que ces zones géographiques sont déjà déterminées de manière très large dans l'avant-projet de loi et que l'obligation de conservation des données s'impose, non seulement, aux communications « originaires » de ces zones, mais également aux communications vers ces zones. **L'avant-projet de loi sera revu afin supprimer la possibilité offerte aux opérateurs de pouvoir conserver des données au-delà des zones géographiques dans lesquelles l'avant-projet de loi impose une obligation de conservation s'ils ne leur pas techniquement pas possible de circonscrire la conservation des données à ces zones**.

130. L'Autorité insiste pour que le législateur vérifie qu'il est bien techniquement possible de mettre en place un système de conservation des données qui soit restreint à certaines zones géographiques avant d'imposer une obligation de conservation ciblée sur base de critères géographiques. **S'il n'était techniquement pas possible de circonscrire la conservation aux données de trafic relatives à des communications effectuées à certaines zones géographiques**, **le législateur ne pourra pas prévoir la mise en place d'un tel système**.

10) Détermination du responsable du traitement des traitements consistant en la conservation des données de trafic et de localisation imposées par les articles 122, 123, 126, 126/1 et 127 de la loi télécom (nouvel article 127/3 § 2 de la loi télécom)

131. Le nouvel article 127/3 § 2 de la loi télécom désigne « *chaque opérateur […] comme responsable du traitement au sens du RGPD pour les données traitées sur base des articles 122, 123, 126, 126/1 et 127* ».

132. L'Autorité **prend note de cette désignation**, **mais elle rappelle que le responsable du traitement est responsable d'un ou de plusieurs traitements, et non de données**. Ainsi, chaque opérateur est responsable du traitement des traitements visés aux articles 122, 123, 126, 126/1 et 127, et non pas des données traitées sur base de ces dispositions. **La formulation de l'article 127/3 § 2 doit être revue en ce sens.**

11) Mesures techniques et organisationnelles imposées aux opérateurs pour la conservation des données de trafic et de localisation (nouveaux articles 127/2 et 127/3 de la loi télécom)

133. Les nouveaux **articles 127/2 et 127/3** de la loi télécom entendent imposer aux opérateurs des mesures techniques et organisationnelles relatives à la conservation des données de trafic et de localisation.

134. La plupart de ces mesures sont imposées afin de garantir la sécurité des données conservées par les opérateurs. L'Autorité constate que c**es mesures visent, conformément à la jurisprudence de la CJUE, à assurer un niveau particulièrement élevé de protection et de sécurité**. Ces mesures rencontrent plusieurs exigences ayant été explicitement imposées par la CJUE, en particulier :
   - L'obligation de **conserver les données sur le territoire de l'Union européenne** (voir le nouvel article 127/2 § 3, alinéa 1, 2° de la loi télécom) ;
   - L'obligation **de détruire les données conservées de tout support lorsque le délai de conservation qui leur est applicable est expiré ou de les rendre anonymes** (voir le nouvel article 127/2 § 3, alinéa 2, 1° de la loi télécom) ;
   - L'adoption de mesures **afin de limiter le risque d'abus ou d'accès illicite aux données** (voir, notamment, le nouvel article 127 § 3, alinéa 1, 3° de la loi télécom qui impose de **rendre les données conservées pour les autorités illisibles et inutilisables**, **dès leur enregistrement, par toute personne qui n'est pas autorisée à y avoir accès** ou le nouvel article 127 § 3, alinéa 2, 4° de la loi télécom qui impose aux opérateurs **d'assurer une traçabilité de l'exploitation des données conservées à l'aide d'un journal**).

135. L'Autorité a néanmoins **plusieurs remarques** à émettre à propos de ces dispositions relatives à la sécurité des données.

136. Tout d'abord, l'Autorité constate **que l'obligation de conservation sur le territoire de l'Union européenne ne s'applique qu'aux données conservées par les opérateurs pour les autorités, et non pas aux données conservées pour leurs propres besoins** (voir le nouvel article 127/2 § 3, alinéa 1, 2° de la loi télécom). L'Autorité a **deux remarques** à ce propos :

(i) **Premièrement,** il y a un **manque de clarté sur la distinction entre données conservées pour les autorités et données conservées pour les propres besoins des opérateurs**. En effet, les nouveaux articles 122 et 123 de la loi télécom imposent des obligations de conservation à des fins de lutte contre la fraude (dont peuvent être victimes les opérateurs) et afin d'assurer la sécurité des réseaux (ce qui constitue une obligation à charge

des opérateurs). L'avant-projet prévoit, par ailleurs, que les autorités pourront, sous certaines conditions, obtenir un accès à ces données, y compris pour d'autres finalités que pour celles pour lesquelles elles ont initialement été conservées. Ces données sont-elles dès lors conservées pour les autorités ou pour les besoins propres des opérateurs ?[112]

(ii) **Deuxièmement**, l'Autorité souligne que la CJUE considère qu'en raison de la quantité de données conservées, du caractère sensible de ces données et du risque d'accès illicite à celles-ci, leur conservation sur le territoire de l'Union constitue une mesure nécessaire pour garantir un niveau particulièrement élevé de protection et de sécurité. **La CJUE ne fait pas de distinction selon la finalité pour laquelle les données sont conservées et l'Autorité n'aperçoit pas pourquoi une telle distinction serait pertinente**. **L'avant-projet sera donc modifié afin de prévoir que toutes les données conservées par les opérateurs le seront sur le territoire de l'Union**.

137. Ensuite, l'Autorité a **deux remarques principales concernant les informations qui doivent être reprises dans le journal** :

(i) L'avant-projet indique que « *le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte* ». L'Autorité souligne, au contraire, **qu'il est nécessaire que la finalité concrète pour laquelle l'accès aux données a été demandé soit ajoutée dans les informations que doit comprendre le journal** parce que cette information est nécessaire, pour permettre un contrôle effectif *a posteriori* de l'utilisation des données. Toutefois, au vu de la sensibilité de cette information, il **faut prévoir que cette information soit journalisée de manière « floutée ».**

(ii) L'avant-projet indique que « *L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal et, en particulier, pour empêcher toute manipulation non autorisée de ce dernier* ». L'Autorité souligne **qu'il faut prévoir, en tout état de cause, que toute manipulation dans le journal soit, elle-même journalisée**, voire spécifier la nécessité d'introduire une impossibilité d'effacement des données reprises dans le journal.

138. Par ailleurs, l'avant-projet de loi entend imposer certaines exigences techniques et/ou organisationnelles aux opérateurs afin, semble-t-il, de garantir la disponibilité et la qualité des données conservées.

[112] L'Autorité souligne que la remarque qu'elle formule à propos du manque de clarté de la distinction entre données conservées pour les autorités et données conservées par les opérateurs pour leurs propres besoins s'applique, bien évidemment, mutatis mutandis, aux autres obligations imposées par l'article 127/3 § 3, alinéa 1er de la loi télécom.

139. Le **nouvel article 127/2 § 2, alinéa 1er,** de la loi télécom prévoit que *« Les opérateurs font en sorte que les données qu'ils conservent pour leurs propres besoins et celles qu'ils conservent pour les autorités soient accessibles de manière illimitée à partir de la Belgique* ». L'objectif et la portée de cette disposition n'apparait pas de manière évidente à sa lecture. L'Exposé des Motifs n'apporte pas d'éclairage à cet égard. À la suite d'une demande d'informations complémentaires, le délégué du Ministre a indiqué que « *Le fait que les données doivent être accessibles 'à partir de la Belgique' ne signifie pas qu'elles doivent être conservées 'en Belgique'. […] L'objectif de la phrase 'accessibles de manière illimitée à partir de la Belgique' est qu'il revient à l'opérateur de fournir les données demandées par l'autorité en Belgique. De la sorte, le droit belge reste applicable* ». Il apparait ainsi que l'objectif de cette disposition est d'imposer aux opérateurs de garantir l'accessibilité des données qu'ils conservent en tout temps, quel que soit le lieu où ces données sont conservées. **La disposition sera revue afin d'en clarifier la portée**. Cette remarque vaut, *mutatis mutandis*, pour le nouvel article 127/4, dernier alinéa, qui comprend une disposition similaire.

140. Le **nouvel article 127/2 § 2, dernier alinéa** de la loi télécom prévoit que « *Les opérateurs sont en mesure d'établir des liens entre les données conservées pour les autorités* ». Dans l'Exposé des motifs, il est indiqué qu'« *[i]l revient aux opérateurs de décider comment ils s'organisent pour la conservation des données au bénéfice des autorités (en particulier les données conservées conformément aux articles 126, 126/1, 127). Dès lors, si une même donnée est visée dans plusieurs articles, ils peuvent conserver la donnée une seule fois. Par contre, les opérateurs doivent être mesure d'établir des liens entre les données conservées pour les autorités. Ceci est nécessaire vu que pour répondre à une demande d'une autorité, un opérateur pourrait être amené à consulter des données conservées sur base de différents article*s ». À la suite d'une demande d'informations complémentaires, le délégué du Ministre a précisé que « *L'objectif est d'éviter que des données conservées soient inexploitables en l'absence de lien entre les données. Par exemple, il est essentiel que les opérateurs puissent faire un lien entre les données d'accès, de connexion, ou de communication conservées en exécution du nouvel article 126/1 avec les données d'identification conservées sur la base du nouvel article 126. Les données d'identification n'ont pas été reprises à l'article 126/1, § 2, 3°, de manière à éviter de conserver deux fois les mêmes données* ». Si l'Autorité comprend la volonté du législateur, elle souligne que la portée de l'article 127/2 § 2 ne ressort pas suffisamment de son libellé. **La disposition sera revue afin d'en clarifier la portée**. L'Autorité souligne, à ce propos, que si le législateur entend permettre aux autorités de réaliser des recherches sur des personnes concernées à partir des différentes données conservées par les opérateurs, il lui reviendrait de déterminer, dans le respect du principe de proportionnalité, les critères de recherche qui pourraient être utilisés par les autorités compétentes pour faire leurs recherches et établir les liens.

12) Conservation des données permettant l'identification des personnes concernées, de l'équipement terminal ou du service de communications électroniques employé par les fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public (nouvel article 127/4 de la loi télécom)

141. Le **nouvel article 127/4 de la loi télécom** prévoit que le Roi doit fixer les conditions dans lesquelles les fournisseurs de **réseaux privés** de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public doivent **enregistrer et conserver les données permettant l'identification des personnes concernées, de l'équipement terminal ou du service de communications électroniques employé**. Cette obligation de conservation est imposée pour les **finalités suivante**s :

- La poursuite et la répression d'infractions pénales,
- La répression d'appels malveillants vers les services d'urgence,
- La recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques,
- L'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

142. Le nouvel article 127/4 de la loi télécom **délègue également au Roi** le soin de **déterminer les mesures techniques et administratives imposées aux fournisseurs de réseaux privés** de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public **en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées** aux conditions prévues par les articles 46bis, 88bis, et 90ter à 90decies, et 464/13, 464/25 et 464/26 du Code d'instruction criminelle, ainsi qu'aux conditions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

143. L'Autorité rappelle que le principe de légalité exige que les éléments essentiels d'un traitement de données, qui constitue une ingérence importante dans les droits fondamentaux des personnes concernées, soient déterminés par une norme législative formelle. Il convient, en outre, que cette norme soit suffisamment claire et précise pour que les personnes concernées puissent appréhender de manière prévisible les circonstances dans lesquelles le traitement de données est autorisé. Il s'ensuit que **les notions fondamentales utilisées pour circonscrire la portée de l'obligation de conservation de données doivent être définies par la législation**. Or, sauf erreur, **les notions de « fournisseurs de réseaux privés de communications électroniques » et de « fournisseurs de services de communications électroniques qui ne sont pas**

accessibles au public » ne sont pas définies par la loi télécom. Comme l'Autorité vient de le souligner, **il s'agit pourtant d'un élément essentiel** des traitements de données imposés par l'article 127/4 de la loi télécom **puisque la définition de ces notions impactera la portée des obligations** de conservation qu'il impose. En effet, la notion de « réseaux privés » a-t-elle vocation à viser uniquement les réseaux des entreprises ou n'importe quel réseau privé, y compris, ceux qui sont mis en place par une personne à son domicile ? Par ailleurs, la notion a-t-elle vocation à viser les réseaux crées par n'importe quelle entreprise ou le législateur entend-t-il imposer des obligations de conservation uniquement si l'entreprise a atteint une certaine taille ? **L'avant-projet sera revu afin d'apporter une définition à ces notions, étant entendu que la définition de ces notions** – et les obligations de conservation qui devront être mises en place en fonction de ces définitions – **devra respecter les principes de nécessité et de proportionnalité**.

144. L'Autorité souligne que l'avant-projet peut, en revanche, déléguer au Roi – comme il le fait – la détermination des modalités techniques relatives aux obligations de conservations imposées par le nouvel article 127/4 de la loi télécom.

13) Accès aux données

145. Le nouvel article 127/1 de la loi télécom identifie les catégories d'autorités qui peuvent avoir accès aux données conservées par les opérateurs en exécution des articles (nouveaux) 122, 123, 126, 126/1 et 127 de la loi télécom.

146. Il ressort d'une lecture de l'article 127/1 de la loi télécom à la lumière des articles 122, 123, 126, 126/1 et 127 de la loi télécom que les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom **peuvent avoir accès aux données conservées en vertu des** (nouvelles versions des) **articles 122, 123, 126 et 127 pour chacune des finalités énoncées par cet article 127/1** de la loi télécom.

147. Les nouveaux articles 126 et 127 de la loi télécom prévoient que les données qui doivent être conservées sur pied de ces dispositions sont « *conservées pour les autorités et les finalités visées à l'article 127/1* ».

148. Les articles 122 et 123 de la loi télécom autorisent ou imposent, en revanche, des obligations de conservation pour des finalités spécifiques (la facturation, le marketing des services à valeur ajouté, la lutte contre la fraude et utilisation malveillante du réseau ou encore la sécurité des réseaux et le bon fonctionnement des services de communication). Mais le nouvel article 127/1 prévoit que les autorités compétentes pour poursuivre l'une des finalités qui y est énoncée **peuvent avoir accès à toutes les données qui sont conservées en application de ces articles 122 et 123 de la loi télécom**,

même si leur conservation a initialement été autorisée ou imposée pour une autre finalité que celle qui est poursuivie par l'autorité qui veut obtenir l'accès auxdites données[113].

149. Enfin, concernant les **données conservées en vertu du nouvel article 126/1,** une lecture combinée des articles 126/1 et 127/1 de la loi télécom indique que les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom **peuvent avoir accès à ces données uniquement pour les finalités pour lesquelles elles sont conservées**, à savoir aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique.

150. Par ailleurs, l'article 127/1 de la loi télécom précise que les **autorités ne peuvent avoir accès aux données conservés par les opérateurs que dans le respect des conditions prévues par les dispositions qui les y habilitent**.

151. L'Autorité a **plusieurs remarques** à formuler à propos des dispositions encadrant la possibilité pour les autorités d'avoir accès aux données conservées par les opérateurs.

152. Tout d'abord, l'Autorité rappelle que la CJUE a jugé que **l'accès à des données de trafic et de localisation conservées par les opérateurs ne peut, en principe, être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée**. Il s'ensuit, en particulier, *« qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale.* ***En revanche, conformément au principe de proportionnalité*** *[…],* ***un accès à des données conservées en vue de la lutte contre la criminalité grave*** *peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès […],* ***être justifié par l'objectif de sauvegarde de la sécurité nationale*** »[114]. En outre, la CJUE estime qu'il *« est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58* »[115]. **Le législateur peut donc prévoir que les autorités peuvent accéder aux données conservées en application des**

[113] En effet, les nouveaux articles 122 § 7 et 123 § 6 de la loi télécom prévoient, chacun, que « *cet article [à savoir, respectivement, l'article 122 et l'article 123] ne porte pas préjudice à l'article 127/1* ». Le nouvel article 126 § 1, alinéa 3, prévoit que « Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1 » et le nouvel article 127 § 1, alinéa 2, prévoit que « *Ces données et documents sont conservés pour les autorités et les finalités visées à l'article 127/1* ».
[114] CJUE, arrêt du 6 octobre 2020, § 166 (c'est l'Autorité qui met en gras).
[115] CJUE, arrêt du 6 octobre 2020, § 166 (c'est l'Autorité qui met en gras).

articles 122 et 123 pour d'autres finalités que celles qui étaient poursuivies par leur conservation initiale, mais uniquement si ces finalités de traitement ultérieur relèvent de la sauvegarde de la sécurité nationale ou de la lutte contre la criminalité grave (ou d'un autre objectif listé à l'article 15 de la Directive ePrivacy qui présente un degré d'importance similaire). Dans sa version actuelle, l'avant-projet de loi permet une réutilisation des données conservées en application des articles 122 et 123 pour toutes les finalités reprises à l'article 127/1 de la loi télécom et pas seulement les finalités présentant une certaine gravité/importance, à l'instar de la lutte contre la criminalité grave. Cette possibilité n'est pas conforme aux exigences européennes. **L'avant-projet sera dès lors revu afin d'y inscrire cette limitation concernant les finalités pour lesquelles une utilisation ultérieure des données conservées en application des articles 122 et 123 est possible**.

153. Par ailleurs, **l'Autorité rappelle que l'accès aux données doit être subordonné au respect des conditions matérielles et procédurales identifiées par la CJUE**. L'avant-projet de loi précise, à cet égard, que les autorités ne peuvent avoir accès aux données que « *dans les conditions prévues par les dispositions qui les y habilitent* ». Ce sont donc ces dispositions qui doivent prévoir les conditions matérielles et procédurales nécessaires. **Pour rappel, ces conditions sont les suivantes** :

- La réglementation nationale concernée **doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé.**
- L'accès des autorités nationales compétentes aux données conservées doit, en principe, sauf cas d'urgence dûment justifiés, être subordonné **à un contrôle préalable** effectué soit par une juridiction soit par une entité administrative indépendante. La décision de cette juridiction ou de cette entité doit intervenir à la suite d'une demande motivée de ces autorités.
- Les autorités qui ont eu accès aux données doivent **en informer les personnes concernées** dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités.

154. **Il incombe au législateur de vérifier que toutes les dispositions qui habilitent les autorités à avoir accès aux données de trafic et de localisation conservées par les opérateurs prévoient les conditions matérielles et procédurales nécessaires afin de respecter les exigences européennes**. Les dispositions qui organisent l'accès des autorités aux données conservées par les opérateurs se retrouvent dans les lois organiques de ces autorités, lesquelles sont, pour la plupart, préexistantes à l'avant-projet de loi. Celui-ci apporte toutefois quelques modifications à des dispositions qui organisent l'accès de certaines autorités aux données conservées par les opérateurs. L'Autorité examine si ces modifications respectent les exigences issues de la jurisprudence

européenne (mais son examen se limite aux modifications apportées). C'est ainsi que l'Autorité a constaté que **l'avant-projet de loi prévoit de permettre à certaines autorités d'avoir accès aux données conservées par les opérateurs sans exiger que cet accès fasse l'objet d'une autorisation préalable par une juridiction ou par une entité administrative indépendante qui ait la qualité de tiers** par rapport à l'autorité qui cherche à avoir accès aux données. C'est le cas, notamment, pour les autorités suivantes :

- L'avant-projet prévoit que l'IBPT « *peut demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions* » (article 17 de l'avant-projet de loi)
- L'avant-projet de loi prévoit que le CCB peut, « *[l]orsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, […] obtenir des opérateurs, au sens de l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques, des données d'identification, de trafic ou de localisation conservées par ceux-ci* » (article 34 de l'avant-projet de loi)
- L'avant-projet de loi prévoit que les membres du personnel statutaire ou contractuel du SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement « *peuvent identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique. À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification* » aux opérateurs (article 33 de l'avant-projet de loi).
- L'avant-projet de loi prévoit qu' *« un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue* » (article 19 de l'avant-projet).

155. L'absence (systématique) de contrôle préalable à la communication des données n'est pas admissible[116]. **L'avant-projet sera revu afin de veiller à ce que l'accès aux données soit,**

[116] À la suite d'une demande d'informations complémentaires, le délégué du Ministre indique que la CJUE n'imposerait pas une exigence de contrôle préalable à l'accès des données lorsque cet accès a lieu dans un autre contexte que la recherche, la prévention, la détection ou la poursuite d'infractions pénales. L'Autorité ne peut souscrire à cette interprétation. Certes, la CJUE a identifié les différentes conditions matérielles et procédurales qui doivent subordonner l'accès des autorités aux données conservées par les opérateurs dans le cadre de décisions examinant la conformité de législations nationales organisant l'accès des autorités aux données de trafic dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Cependant, la Cour n'a pas limité ces exigences à ce seul contexte. En effet, la CJUE a jugé, dans un arrêt du 21 décembre 2016, qu' « *il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* » (C'est l'Autorité qui souligne). Dans un arrêt du 2 mars 2021, la CJUE a jugé que « *Ce contrôle préalable requiert entre autres, […],*

conformément aux exigences européennes, toujours subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante qui présente la qualité de tiers par rapport à l'autorité demandant l'accès aux données, **sauf dans les cas d'urgence dûment justifiés**[117]**.**

---

que la juridiction ou l'entité chargée d'effectuer ledit contrôle préalable dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès » (C'est l'Autorité qui souligne**). Les éléments soulignés laissent clairement sous-entendre que le contrôle préalable à l'accès aux données a, selon la CJUE, également un rôle à jouer en dehors des situations où l'accès aux données est demandé en vue de prévenir, détecter ou poursuivre des infractions pénales**. **L'objectif poursuivi par l'exigence de contrôle préalable par une juridiction ou une autorité administrative indépendante est de s'assurer que les autorités n'ont accès qu'aux données de trafic auxquelles elles peuvent effectivement avoir accès ; ces données devant être limitées à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi par la demande d'accès.** Ce contrôle préalable est particulièrement important parce que l'accès aux données de trafic constitue une ingérence qui peut être particulièrement grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel puisque ces données sont susceptibles de fournir des informations précises sur la vie privée d'un utilisateur d'un moyen de communications électroniques, même lorsque l'accès ne porte que sur une quantité limitée de données ou sur des données limitées à une courte période (voyez, les arrêts suivants de la CJUE : arrêt du 8 avril 2014, § 62 ; arrêt du 21 décembre 2021, § 118-120 ; arrêt du 2 mars 2021, § 40). **Les éléments qui justifient la nécessité d'un contrôle préalable existent tant lorsque l'accès des autorités a lieu dans le cadre d'une procédure pénale que lorsque cet accès intervient dans un autre contexte**. L'existence de voies de recours juridictionnels (*a posteriori*) ne peut suffire à rencontrer l'exigence d'un contrôle préalable.

[117] Le délégué du Ministre a justifié l'absence de contrôle préalable à l'accès aux données par un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale dans le cadre d'une recherche concernant des personnes disparues à l'aide de deux éléments : 1) le fait que la Cellule des Personnes Disparues n'œuvre pas dans le cadre d'une finalité « pénale » et 2) le fait qu'un recours à une procédure d'autorisation préalable pourrait avoir pour conséquence de faire perdre aux services de recherche des heures, voire des jours, qui s'avèrent souvent cruciaux dans le succès de la recherche de la personne concernée et dans la protection de ses intérêts vitaux. L'Autorité ne peut suivre le demandeur dans son premier argument. Cependant, l'existence d'une urgence particulière, qui est dûment justifiée, peut justifier de se passer de contrôle préalable. La législation pourrait dès lors prévoir une exception à l'obligation de contrôle préalable de la demande d'accès aux données d'un officier de police judiciaire de la Cellule des Personnes Disparues en cas d'urgence, étant entendue que celle-ci devrait être dûment justifiée (et évaluée au cas par cas). Le délégué du Ministre avance un argument similaire pour justifier l'absence de contrôle préalable à l'accès aux données de trafic par le CCB : « *En raison de l'augmentation, de la fréquence des incidents en matière de cybersécurité et de la rapidité de réaction nécessaire, le CCB ne pourrait prévenir et détecter en temps utile les infractions en matière de cybercriminalité, les menaces contre la sécurité publique liées à la cybersécurité et les défaillances de la sécurité des réseaux s'il devait obtenir systématiquement l'autorisation préalable d'une juridiction ou d'une autorité nationale indépendante pour accéder à ces données de communications électroniques* ». A nouveau, l'Autorité souligne que l'existence d'une urgence particulière, qui est dûment justifiée, peut justifier de se passer de contrôle préalable, mais cette appréciation doit se faire *in concreto* et ne peut être décrétée par principe.

Le délégué du Ministre a justifié l'absence de contrôle préalable à l'accès aux données par les membres du personnel statutaire ou contractuel du SPF Santé publique parce que les données sur lesquelles peuvent porter une demande d'accès sont limitées aux données strictement nécessaires afin de pouvoir identifier un utilisateur et que ces données sont considérées comme « moins sensibles ». À nouveau, l'Autorité ne peut souscrire à cette motivation. D'ailleurs, dans l'arrêt invoqué par le demandeur à l'appui de son raisonnement (arrêt du 2 octobre 2018, *Ministerio fiscal*), l'accès aux données d'identification était soumis à un contrôle judiciaire préalable. Ce contrôle est nécessaire pour s'assurer que l'accès de l'administration aux données d'identification répond bien aux exigences légales (y compris de nécessité et de proportionnalité). Par ailleurs, le délégué du Ministre indique que « *il est utile de préciser que ce pouvoir est prévu par l'article 14, c, du Règlement 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) no 765/2008 et (UE) no 305/2011* ». L'Autorité souligne, à cet égard, que ledit Règlement européen dispose que « *les autorités de surveillance du marché exercent les pouvoirs énoncés au présent article de manière effective et efficace, conformément au principe de proportionnalité, dans la mesure où cet exercice se rapporte à l'objet et à l'objectif des mesures, à la nature de la non-conformité et au dommage global, potentiel ou avéré, découlant d'un cas de non-conformités. Ces pouvoirs sont conférés et exercés conformément au droit de l'Union et au droit national, y compris aux principes de la Charte des droits fondamentaux de l'Union européenne, et aux principes du droit national relatifs à la liberté d'expression ainsi qu'à la liberté et au pluralisme des médias, aux garanties procédurales applicables et aux règles de l'Union concernant la protection des données, en particulier le règlement (UE) 2016/679* » (c'est l'Autorité qui souligne). Soumettre l'exercice du pouvoir de « *demander aux opérateurs économiques de fournir des informations pertinentes aux fins de l'identification du propriétaire d'un site internet, dès lors que cette information a trait à l'objet de l'enquête* » à un contrôle préalable est autorisé par le Règlement 2019/1020 parce que cela s'impose en vertu du droit au respect des données à caractère personnel tel qu'il a été interprété par la CJUE dans ses arrêts relatifs à la conservation des données de trafic.

156. L'Autorité rappelle également que la juridiction ou l'autorité administrative indépendante qui procède au contrôle préalable doit s'assurer que la communication de données poursuit une des finalités pour laquelle cette communication peut avoir lieu. À cet égard, l'Autorité rappelle que la communication de données ne peut, en principe, être justifiée que par l'objectif d'intérêt général pour lequel la conservation a été imposée, à moins que la loi permette, dans le respect du principe de proportionnalité, une communication pour d'autres finalités. Il convient, en outre, que la juridiction ou l'autorité administrative indépendante veille à la proportionnalité de la communication de données avant de l'autoriser.

157. Par ailleurs, concernant la possibilité pour l'IBPT d'avoir accès aux données de trafic nécessaires à l'exercice de ses missions, l'Exposé des Motifs indique que cet accès est nécessaire, par exemple, pour permettre à l'IBPT de contrôler le « *respect par les opérateurs de leurs obligations légales, telles que l'obligation d'adresser une facturation détaillée, prévue à l'article 110 de la loi du 13 juin 2005 relative aux communications électroniques, ou dans le cadre de la mise en œuvre de l'article 114 de cette même loi. Par exemple, en matière de facturation détaillée, l'IBPT doit être en mesure de demander à l'opérateur de lui fournir un échantillon de factures. Or, ces factures reprennent des données de trafic, telles que les destinataires, dates, heures et durées des communications passées* ». Afin d'assurer la prévisibilité de la loi et de veiller à la nécessité ainsi qu'à la proportionnalité de l'ingérence qui résulte de l'accès à des données de trafic, **l'avant-projet de loi doit identifier explicitement les missions pour lesquelles l'IBPT peut avoir accès aux données de trafic conservées par les opérateurs**.

14) Règles particulières insérées par l'avant-projet de loi concernant l'usage de la cryptographie dans le domaine des communications électroniques

158. Le nouvel article 127/5 § 1 de la loi télécom interdit « *de fournir ou d'utiliser un service ou un équipement qui empêche la réalisation des opérations suivantes :*
1° les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant ;
2° l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;
3° les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ».

159. Cette interdiction est déjà (partiellement) inscrite dans la version actuelle de la loi télécom (voir l'article 127 actuel de la loi télécom).

160. Le nouvel article 127/5 § 2 de la loi télécom apporte **des dérogations au principe selon lequel *« l'emploi de la cryptographie est libre »***[118] :

- Il est interdit de fournir ou d'utiliser un système d'encryptage qui empêche les communications d'urgence (nouvel article 127/5 § 2, alinéa 2 de la loi télécom).
- Les systèmes d'encryptage, qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements, ne peuvent pas empêcher la conservation par l'opérateur des données d'identification, de trafic ou de localisation pour les autorités (nouvel article 127/5 § 2, alinéa 3 de la loi télécom).Lorsqu'un opérateur met en place un système d'encryptage qui peut être utilisé pour garantir la confidentialité des communications et la sécurité des paiements, il doit rendre possible, dans les 24h à partir de la transmission de la requête, les mesures d'interception légale, en particulier l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public. L'opérateur rend possible la réalisation de ces opérations uniquement pour les communications visées dans la requête et qui sont postérieures à celles-ci (nouvel article 127/5 § 2, alinéas 4 et 5 de la loi télécom).

161. L'Autorité a **deux remarques fondamentales** à formuler à propos des interdictions imposées par cette disposition.

162. Premièrement, l'interdiction d'utiliser des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que la conservation des données d'identification, de trafic ou de localisation **constitue une ingérence disproportionnée** dans le droit au respect de la vie privée des personnes concernées et qui excède dès lors ce qui est nécessaire dans une société démocratique. **L'avant-projet de loi sera revu afin de supprimer cette interdiction**.

163. Deuxièmement, l'Autorité souligne qu'en imposant aux opérateurs qui mettent en place un système d'encryptage de rendre les mesures d'interception légale possibles, en particulier l'identification de l'utilisateur final, le repérage et la localisation des communications ainsi que les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public, le nouvel article 127/5 § 2 de la loi télécom impose *de facto* l'insertion de « portes dérobées » (« *backdoors* ») dans les systèmes de cryptographie afin de pouvoir déchiffrer les messages encryptés. Or l'Autorité relève qu'il existe, depuis les années 1990, un consensus fort

[118] Ce principe est actuellement consacré par l'article 48 de la loi télécom. Lorsque la loi transposant le CCEE aura été adoptée, ce principe sera consacré par le nouvel article 105/4 de la loi télécom (qui reproduit l'article 48 actuel de la loi télécom).

dans la communauté scientifique pour considérer que l'insertion de « portes dérobées » (« *backdoors* ») dans les systèmes de cryptographie présente plus de risques pour la vie privée des personnes concernées et les intérêts supérieurs des Etats que d'avantages en termes de lutte contre la criminalité grave[119]. **L'avant-projet de loi doit dès lors être revu afin de supprimer l'obligation pour les opérateurs qui mettent en place un système d'encryptage de rendre possible les mesures d'interception légale**. Certes, les systèmes de cryptographies ont rendu l'accès au contenu des communications plus difficile qu'auparavant. Mais l'Autorité souligne qu'il existe néanmoins déjà beaucoup d'informations « digitales » disponibles sur les équipements terminaux des utilisateurs (log, cookies, mémoire flash qui ne peut être effacée…), auprès des opérateurs (données collectées en vue de la facturation, par exemple) ainsi que dans l'espace public (caméras de surveillance, caméras ANPR,…). L'Autorité souligne, encore, que si cela s'avère nécessaire en vue de lutter contre la criminalité grave, les autorités peuvent « hacker » les appareils téléphoniques pendant leur utilisation (Encrochat, SKY ECC, Hacking team, NSO group...) ou encore faire appel à des techniques particulières de recherche (comme l'infiltration, l'observation à l'aide de moyens techniques, le recours aux indicateurs, …). L'Autorité constate que ces différents moyens, qui sont mis à la disposition des autorités répressives, rendent, sans doute, la lutte contre la criminalité grave plus facile qu'auparavant et qu'en tout cas, il n'existe aucune preuve du contraire. Dans ces conditions – et au regard des risques, notamment, de « mise sur écoute » de citoyen.ne.s, y compris d'hommes et de femmes politiques (comme l'a été Angela Merkel pendant 5 ans) ou encore de chef.fe.s d'entreprises, notamment, par des pays tiers – **l'Autorité insiste pour que le demandeur supprime les dérogations au principe selon lequel « l'emploi de la cryptographie est libre ».**

15) Remarque finale

164. L'article 1er de l'arrêté du 19 septembre 2013 dispose que « *Le présent arrêté transpose partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive « conservation de données ») (J.O. C.E. 13 avril 2006, L 105/54) et l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des*

[119] Voyez, par exemple, The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W (1997), Keys under doormats, https://www.lawfareblog.com/keys-under-doormats-mandating-insecurity (2015); US National Academies, Decrypting the Encryption Debate, https://www.nap.edu/read/25010/chapter/1 (2018); https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf; https://www.vice.com/en/article/8qxwda/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption; https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate; https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/; https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

communications électroniques (directive « vie privée et communications électroniques ») (J.O.C.E. 31 juillet 2002, L 201/37) ». Ainsi, l'Autorité constate que cette disposition fait encore référence à la directive 2006/24 alors que celle-ci a été invalidée par la CJUE en 2014. **L'arrêté du 19 septembre 2013 sera modifié pour supprimer cette référence à une directive invalide.**

PAR CES MOTIFS,

L'Autorité estime que les adaptations suivantes doivent être apportées à l'avant-projet de loi et au projet d'arrêté :

- Réaliser une analyse rigoureuse de la nécessité et de la proportionnalité de l'obligation de conserver les données de localisation et autres données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communication électroniques et adapter le projet en conséquence et/ou mentionner les justifications pertinentes dans l'exposé des motifs (cons. 67-69)

- Si, après analyse, le législateur estime qu'il est rigoureusement nécessaire et proportionné d'imposer une obligation de conservation des données de trafic à des fins de lutte contre la fraude et l'utilisation malveillante du réseau, les adaptations suivantes doivent être apportées :
  - Déterminer les données précises qui doivent être conservées en application de cette obligation ou imposer au Roi d'intervenir pour déterminer ces données (cons. 72)
  - Préciser que la possibilité de conserver les données au-delà du délai minimal de 4 mois concerne les situations où une conservation plus longue est nécessaire pour gérer un contentieux relatif à une fraude ou à une utilisation malveillante du réseau (cons. 73)

- Réaliser une analyse rigoureuse de la nécessité et de la proportionnalité de l'obligation de conserver les données de localisation et autres données de trafic nécessaires afin d'assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques et adapter le projet en conséquence et/ou mentionner les justifications pertinentes dans l'exposé des motifs (cons. 78-80)

- Si, après analyse, le législateur estime qu'il est rigoureusement nécessaire et proportionné d'imposer une obligation de conservation des données de trafic afin

d'assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques, les adaptations suivantes doivent être apportées :

- Déterminer les données précises qui doivent être conservées en application de cette obligation ou imposer au Roi d'intervenir pour déterminer ces données (cons. 82)
- Apprécier, et, le cas échéant, justifier à l'aide d'éléments concrets, la raison pour laquelle les données doivent être conservées pendant une durée de 12 mois (cons. 83)
- Préciser que la possibilité de conserver les données au-delà du délai de 12 mois concerne les situations où une conservation plus longue est nécessaire pour gérer un contentieux relatif à une attaque ou des actes portant atteinte à la sécurité du réseau ou au bon fonctionnement du service à une fraude ou à une utilisation malveillante du réseau (cons. 83)

- Préciser que l'obligation légale prévue par les articles 122 § 4/2 et 123 ne peut être imposée que par une norme législative formelle (cons. 85 et 89)

- Réaliser une analyse rigoureuse de la nécessité et de la proportionnalité de l'obligation de conserver les données de localisation autres que des données de trafic pour les différentes finalités identifiées par le nouvel article 123 de la loi télécom et adapter le projet en conséquence et/ou mentionner les justifications pertinentes dans l'exposé des motifs (cons. 87-88)

- Le cas échéant, déterminer, au moins, les conditions dans lesquelles les opérateurs pourront conserver et traiter les données de localisation autres que des données de trafic et les durées maximales de conservation de ces données (cons. 88)

- Prévoir que les adresses IP attribuées à la source d'une connexion ne pourront être conservées qu'afin de permettre la poursuite d'objectifs particulièrement importants à déterminer (cons. 97, 100)

- Préciser que seules les adresses IP attribuées à la source d'une connexion, à l'exclusion des adresses IP attribuées à la destination d'une communication, peuvent être conservées en exécution du nouvel article 126 de la loi télécom (cons. 101)

- Prévoir que la conservation préventive et systématique des numéros d'identification des terminaux des utilisateurs finaux est imposée uniquement afin de poursuivre des objectifs présentant une importance particulière qui doivent être déterminés (comme

la lutte contre la criminalité grave), que la durée de leur conservation est strictement limitée au regard de cet objectif et prévoir des conditions et des garanties strictes quant à l'exploitation de ces données (cons. 102)

- Supprimer la possibilité offerte aux opérateurs d'avoir recours à la technique de reconnaissance faciale (ou à toute autre technique reposant sur une utilisation des données biométriques) pour identifier leurs abonnés (cons. 104)

- Déterminer les données et documents d'identification à collecter et à conserver par l'opérateur ou imposer au Roi de procéder à cette détermination (cons. 105)

- Définir la notion de « données de communication » (cons. 109)

- Définir la notion de « données des appels infructueux » ou remplacer cette expression par celle de « données de trafic des appels infructueux » (cons. 110)

- Supprimer les mots « au minimum » dans l'arrêté du 19 septembre afin de veiller à ce que cet arrêté détermine de manière exhaustive les données à conserver en exécution du nouvel article 126/1 de la loi télécom (cons. 113)

- S'assurer que le seuil retenu pour déterminer si une zone est particulièrement exposée à la commission d'actes de criminalité grave n'aboutit pas à réintroduire, de facto, une obligation de conservation généralisée et indifférenciée des données sur la (quasi-) totalité du territoire national (cons. 117)

- Veiller à ces que les modalités utilisées pour déterminer si une zone est particulièrement exposée à la commission d'actes de criminalité grave sont adéquates (cons. 122-124)

- Veiller à ce que la sélection des lieux retenus pour y cibler une conservation préventive des données réponde aux exigences de nécessité et de proportionnalité (cons. 125)

- Supprimer la délégation au Roi l'autorisant à ajouter d'autres lieux à ceux listés par l'avant-projet de loi (cons. 125)

- Compléter les informations qui doivent être reprises dans le rapport annuel que le Ministre des Télécommunications et le Ministre de la Justice doivent transmettre annuellement à la Chambre (cons. 126-127).

- Préciser que les « données » sont les « données visées au § 2 » (cons. 128)

- Supprimer la possibilité offerte aux opérateurs de pouvoir conserver des données au-delà des zones géographiques dans lesquelles l'avant-projet de loi impose une obligation de conservation s'ils ne leur pas techniquement pas possible de circonscrire la conservation des données à ces zones (cons. 129-130)

- Revoir la formulation de la désignation du responsable du traitement (cons. 132)

- Prévoir que toutes les données conservées par les opérateurs le seront sur le territoire de l'Union (cons. 136)

- Prévoir que les informations suivantes doivent être reprises dans le journal :
  - ✓ La finalité concrète pour laquelle l'accès aux données a été demandé, étant entendu que cette finalité doit être « floutée » (cons. 137)
  - ✓ Toute manipulation dans le journal (cons. 137)

- Clarifier la portée du nouvel article 127/2 § 2, alinéa 1er **et** dernier alinéa (cons. 139-140)

- Définir les notions de « fournisseurs de réseaux privés de communications électroniques » et de « fournisseurs de services de communications électroniques qui ne sont pas accessibles au public » (cons. 143)

- Prévoir que les autorités peuvent accéder aux données conservées en application des articles 122 et 123 pour d'autres finalités que celles qui étaient poursuivies par leur conservation initiale uniquement si ces finalités de traitement ultérieur relèvent de la sauvegarde de la sécurité nationale ou de la lutte contre la criminalité grave (ou d'un autre objectif listé à l'article 15 de la Directive ePrivacy qui présente un degré d'importance similaire) (cons. 152)

- Revoir les dispositions pertinentes pour s'assurer que l'accès aux données soit, conformément aux exigences européennes, toujours subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante qui présente la qualité de tiers par rapport à l'autorité demandant l'accès aux données, sauf dans les cas d'urgence dûment justifiés (cons. 153-155)

- Identifier explicitement les missions pour lesquelles l'IBPT peut avoir accès aux données de trafic conservées par les opérateurs (cons. 157).

- Supprimer l'interdiction d'utiliser des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que la conservation des données d'identification, de trafic ou de localisation (cons. 162)

- Supprimer l'obligation faite aux opérateurs qui mettent en place un système d'encryptage de rendre possible les mesures d'interception légale (cons. 163).

- Supprimer, dans l'arrêté du 19 septembre 2013, la référence à la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE qui a été invalidée par la CJUE (cons. 164).

L'Autorité attire l'attention sur les éléments suivantes :

- Le législateur doit vérifier que toutes les dispositions qui habilitent les autorités à avoir accès aux données de trafic et de localisation conservées par les opérateurs prévoient les conditions matérielles et procédurales nécessaires afin de respecter les exigences européennes (cons. 154)

- La juridiction ou l'autorité administrative indépendante qui procède au contrôle préalable d'une communication des données de trafic aux autorités doit s'assurer que cette communication poursuit une des finalités pour laquelle elle peut avoir lieu et qu'elle respecte le principe de proportionnalité (cons. 156)

Pour le Centre de Connaissances,
(sé) Alexandra Jaspar, Directrice

ANNEXE I

Executive Summary

Le Ministre de la Justice, Monsieur Vincent Van Quickenborne a sollicité, le 7 mai 2021, l'avis de l'Autorité concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités (ci-après « l'avant-projet de loi ») et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après « le projet d'arrêté »).

Cet avant-projet de loi vise à répondre à l'annulation de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » par la Cour constitutionnelle. Le 21 avril 2021, la Cour constitutionnelle a, en effet, annulé cette loi du 29 mai 2016 qui reposait, dans son principe, sur une obligation de conservation généralisée et indifférenciée des données de trafic et de localisation des utilisateurs de moyens de communications électronique. Or la Cour constitutionnelle, dont la motivation renvoie largement à l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2020 (arrêt « Quadrature du Net »), juge que **l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle**. Dans son arrêt, la Cour constitutionnelle rappelle qu'*« il appartient au législateur d'élaborer une règlementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatible avec [la directive ePrivacy, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne]* ».

L'avant-projet de loi cherche à mettre en place un système de conservation des métadonnées de communication qui respecte les exigences imposées par le droit européen, tel qu'il est interprété par la CJUE (pour une synthèse de ce système, voyez le tableau repris dans l'Annexe II). **Force est toutefois de constater que l'avant-projet de loi n'opère pas réellement le changement de perspective exigé par la jurisprudence de la CJUE et la CC**. En effet, l'Autorité constate, dans son avis, que l'avant-projet de loi entend imposer de nouvelles mesures de conservation des données de trafic et de localisation qui pourraient aboutir à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données, tout en opérant une extension des possibilités d'accès à ces données. **Certes, la conservation de métadonnées peut être nécessaire pour garantir le droit à la sécurité de personnes qui est, comme le droit au respect de la vie privée et à la protection des données à caractère personnel, un droit fondamental consacré par la Constitution belge, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne**. Le droit à la sécurité génère, en effet, des obligations positives, dans le chef de l'Etat,

d'adopter des mesures matérielles et procédurales permettant de lutter efficacement contre les infractions pénales commises contre les personnes à travers une enquête et des poursuites effectives. La CJUE reconnait la nécessité de procéder à une conciliation entre ces différents droits fondamentaux**. L'Autorité invite le législateur à prendre le temps de la réflexion et de l'analyse rigoureuse pour concilier, dans le respect de la jurisprudence européenne, les droits fondamentaux à la sécurité et à un recours effectif en cas d'infractions pénales portant atteinte à cette sécurité, d'une part, et les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, d'autre part**. L'Autorité insiste pour que le législateur adapte son avant-projet de loi pour que la loi qui sera votée respecte toutes les exigences imposées par la CJUE et la Cour constitutionnelle. Une nouvelle annulation par la Cour constitutionnelle de la loi serait de nature à entacher la confiance des citoyennes et les citoyens dans les institutions démocratiques. **Il est, dans cette perspective, tout à fait crucial de s'assurer que l'avant-projet de loi ne réintroduise pas, *de jure* ou *de facto*, une obligation de conservation généralisée et indifférenciée des données de trafic ou de localisation de l'ensemble ou d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique.** L'Autorité a émis, dans son avis, de très nombreuses remarques à propos de l'avant-projet de loi qui pointent les adaptations qui doivent y être apportées afin d'assurer la conformité de la règlementation en projet avec les exigences découlant du droit à la protection des données à caractère personnel tel qu'il est interprété par la CJUE.

Par ailleurs, **l'Autorité est inquiète de constater que l'avant-projet de loi prévoit d'obliger les opérateurs qui mettent en place un système d'encryptage à rendre possible les mesures d'interception légale**, en particulier l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public. En effet, il existe, depuis les années 1990, un consensus dans la communauté scientifique pour considérer que l'insertion de « portes dérobées » (« backdoors ») dans les systèmes de cryptographie présente plus de risques pour la vie privée des personnes concernées et les intérêts supérieurs des Etats que d'avantages en termes de lutte contre la criminalité grave. **L'Autorité s'inquiète aussi de l'introduction d'obligations de collecte de données par des services, tels que des messageries encryptées, qui pour des raisons légitimes de sécurité et de protection de la vie privée ont jusqu'à présent évité de collecter ces données**.

78/81

ANNEXE II

Tableau récapitulatif des mesures de conservation préventive des données de trafic et de localisation

BASE LÉGALE	QUI DOIT CONSERVER ?	AUTORISATION OU OBLIGATION DE CONSERVATION DE DONNÉES	CATÉGORIES DE DONNÉES À CONSERVER	PRÉCISION CONCERNANT LES DONNÉES À CONSERVER	FINALITÉ INITIALE POURSUIVIE PAR LA CONSERVATION DE DONNÉES	AUTORITÉ(S) POUVANT ACCÉDER À CES DONNÉES & FINALITÉ(S) POUVANT JUSTIFIER CET ACCES
Art. 122§2 de la loi télécom (nouveau)	Tous les opérateurs	Autorisation	Données de trafic nécessaires à l'établissement des factures des abonnés ou celles qui sont nécessaires aux paiements d'interconnexion	Non – il n'y a pas de liste détaillée des données (ni dans la loi ni dans un AR) Mais l'opérateur doit informer les abonnées des données traitées	Établir les factures des abonnés et payer les interconnexions	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 122§3 de la loi télécom (nouveau)	Tous les opérateurs	Autorisation, mais nécessité d'obtenir le consentement (au sens RGPD) de l'abonné préalablement au traitement	Données de trafic, y compris les données de localisation	Non – il n'y a pas de liste détaillée des données (ni dans la loi ni dans un AR) Mais l'opérateur doit informer les abonnées des données traitées	Assurer le marketing des services de communications électroniques propres et établir le profil d'utilisation de l'abonné ou de l'utilisateur final	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 122§4 de la loi télécom	Tous les opérateurs	Obligation (nouveauté de l'avant-projet)	Données de localisation et d'autres des données de trafic nécessaires afin de	Pas de liste détaillée dans l'avant-projet, mais délégation facultative au Roi qui	Détecter et analyser une fraude présumée ou une utilisation	Les autorités et les finalités listées à l'article 127/1 de la loi télécom

(nouveau)			détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau	peut – mais ne doit pas – déterminer les données à conserver sur pied de cette disposition	malveillante présumée du réseau	
Art. 122 § 4/1 de la loi télécom (nouveau)	Tous les opérateurs	Obligation (nouveauté de l'avant-projet)	Données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques	Pas de liste détaillée dans l'avant-projet et pas de délégation au Roi pour déterminer les données à conserver	Assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques, et en particulier détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 123 de la loi télécom (nouveau)	Opérateurs de réseaux mobiles	Autorisation (nécessité d'obtenir le consentement de l'abonné dans certains cas)	Données de localisation autres que les données de trafic	Pas de liste détaillée dans l'avant-projet et pas de délégation au Roi pour déterminer les données à conserver	Bon fonctionnement et sécurité du réseau/service Détecter et analyser une fraude présumée ou une utilisation malveillante présumée du réseau Nécessaire pour fournir un service à valeur ajoutée (consentement nécessaire)	Les autorités et les finalités listées à l'article 127/1 de la loi télécom

Art. 126 de la loi télécom (nouveau)	Opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques & opérateurs fournissant les réseaux de communications électroniques sous-jacents	Obligation	Données de souscription de l'abonné & données techniques nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique	Délégation au Roi pour déterminer les données précises à conserver Cf. nouveaux articles 3§1, 4§1, 5§1 et 6§1 de l'AR du 19/09/2013	Conservation pour les autorités et les finalités identifiées à l'article 127/1 de la loi télécom (reprises dans la colonne de droite)	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 126/1 de la loi télécom (nouveau)	Opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques & opérateurs fournissant les réseaux de communications électroniques sous-jacents	Obligation ciblée sur base de critères géographique	Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination	Délégation au Roi pour déterminer les données précises à conserver Cf. nouveaux articles 3§2, 4§2, 5§2 et 6§2 de l'AR du 19/09/2013	Sauvegarde de la sécurité nationale Lutte contre la criminalité grave, Prévention de menaces graves contre la sécurité publique Sauvegarde des intérêts vitaux d'une personne physique	Les autorités et les finalités listées à l'article 127/1 de la loi télécom Mais l'accès à ces données n'est possible qu'à condition que cet accès poursuive l'une des finalités suivantes : la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et la sauvegarde des intérêts vitaux d'une personne physique.

			Les données des appels infructueux			
Art. 127 de la loi télécom (nouveau)	Tous les opérateurs	Obligation	Données nécessaires pour que les autorités qui sont habilitées à obtenir l'identité des abonnés des opérateurs puissent les identifier	Il n'y a pas de liste détaillée dans l'avant-projet, mais délégation facultative au Roi qui peut – mais ne doit pas – déterminer les données à conserver sur pied de cette disposition [L'AR du 19/9/2013 n'exécute pas cette disposition]	Conservation pour les autorités et les finalités identifiées à l'article 127/1 de la loi télécom (reprises dans la colonne de droite)	Les autorités et les finalités listées à l'article 127/1 de la loi télécom

Le nouvel article 127/1 de la loi télécom détermine les autorités qui peuvent accéder aux données conservées par les opérateurs télécom en exécution de la loi télécom et les finalités pouvant justifier cet accès. Il s'agit des autorités et des finalités suivantes :

1° les autorités répressives pour la prévention, la recherche, la détection et la poursuite d'infractions ;

2° les services de renseignement et de sécurité pour l'exercice de leurs missions légales ;

3° les autorités chargées d'apporter de l'aide aux personnes ;

4° l'IBPT pour l'exercice de ses missions légales ;

5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service

L'accès aux données se fait aux conditions prévues par les lois organiques des différentes autorités listées à l'article 127/1 de la loi télécom.

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 108/2021 van 28 juni 2021

Voorwerp: Adviesaanvraag over een voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten en over een ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (CO-A-2021-099)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "Autoriteit"), mevrouw Alexandra Jaspar en heren Yves-Alexandre de Montjoye, Bart Preneel en Frank Robben ;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid op artikelen 23 en 26 (hierna "WOG");

Gelet op Verordening (EU) 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van de gegevens, en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van de minister van Justitie, de heer Vincent Van Quickenborne, ontvangen op 7 mei 2021;

Gelet op de verdere inlichtingen die werden verzonden op 1 en 8 juni 2021;

Gelet op het verslag van Alexandra Jaspar;

Brengt op 28 juni 2021 het volgende advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De minister van Justitie, de heer Vincent Van Quickenborne (hierna "de aanvrager" genoemd), vroeg op 7 mei 2021 het advies van de Autoriteit over een voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten (hierna "het voorontwerp van wet") en over een ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna "het ontwerp van besluit").

2. Het voorontwerp van wet beoogt, zoals wordt benadrukt in de memorie van toelichting, *"tegemoet te komen aan arrest nr. 57/2021 van 22 april 2021 waarin het Grondwettelijk Hof heeft beslist om de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie te vernietigen"* (hierna "de wet van 29 mei 2016").

3. Deze wet van 29 mei 2016 voorzag, zoals is aangegeven in de memorie van toelichting van het voorontwerp, in "*de verplichting voor aanbieders van openbare telefoniediensten waaronder ook via het internet, van internettoegang, van e-mail via het internet (ongeacht of ze bij het BIPT een kennisgeving hadden gedaan of niet) om bepaalde categorieën locatie- en verkeersgegevens gedurende een periode van 12 maanden te bewaren, in hoofdzaak zodat deze gegevens beschikbaar zijn voor Law enforcement doeleinden en met name voor strafrechtelijk onderzoek".* Deze wet legde dus een verplichting op tot het algemeen en ongedifferentieerd bewaren van bepaalde verkeers- en locatiegegevens. Ze werd door het Grondwettelijk Hof vernietigd omdat ze indruist tegen artikel 15 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (hierna "de ePrivacyrichtlijn", gelezen in het licht van de artikelen 7 en 8, en van artikel 52 § 1 van het Handvest van de grondrechten van de Europese Unie, gecombineerd met de artikelen 10 en 11 van de Grondwet. De vernietiging door het Grondwettelijk Hof wordt ruimschoots gemotiveerd door een verwijzing naar het arrest van het Europees Hof van Justitie (hierna "het HvJ-EU"), uitgebracht naar aanleiding van de prejudiciële vragen die onder meer het Grondwettelijk Hof had gesteld over de interpretatie die moet worden gegeven aan artikel 15 van de ePrivacyrichtlijn[1].

4. Het voorontwerp beoogt de invoering van een systeem voor de bewaring van communicatiegegevens dat voldoet aan de eisen van het HvJ-EU. Het beoogt daartoe de wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna "de telecomwet"), van het Wetboek van

[1] HvJ-EU, arrest van 6 oktober 2020, Gevoegde zaken C-511/18, C-512/18 en C-520/18 (zaak "La Quadrature du Net"). Dit arrest van het HvJ-EU werd uitgebracht naar aanleiding van prejudiciële vragen, onder meer van het Grondwettelijk Hof in zijn arrest nr. 96/2018 van 19 juli 2018.

Strafvordering (hierna het "WSV"), van de wet van 17 januari 2003 betreffende het statuut van de regulator van de Belgische post- en telecommunicatiesector (hierna "de wet BIPT-statuut"), van de wet van 5 augustus 1992 op het politieambt (hierna "de wet op het politieambt"), van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna "de wet op de inlichtingendiensten"), van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten (hierna de wet FSMA"), van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en de andere producten (hierna de "wet betreffende de bescherming van de gezondheid van de gebruikers") en van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (hierna "de NIS-wet").

5. Het ontwerpbesluit van zijn kant voert bepaalde wetgevende machtigingen uit die zijn vervat in het voorontwerp.

II. ONDERZOEK VAN DE ADVIESAANVRAAG

6. In haar advies identificeert de Autoriteit eerst de bepalingen van de ePrivacyrichtlijn die worden omgezet door het voorontwerp van wet (A). Vervolgens stelt ze het 'systeem' voor dat het voorontwerp van wet wil invoeren voor de bewaring van de verkeers- en locatiegegevens door de operatoren en de toegang ertoe voor verschillende autoriteiten (B). De Autoriteit herhaalt ook de eisen waaraan de normen die voorzien in een bewaring van verkeers- en/of locatiegegevens (en hun eventuele communicatie aan de autoriteiten) moeten voldoen (C). Ten slotte onderzoekt de Autoriteit de conformiteit van het voorontwerp van wet en van het ontwerpbesluit met deze eisen (D).

7. Voor zover nodig benadrukt de Autoriteit dat ze zich enkel uitspreekt over de bepalingen waarvoor zij bevoegd is, met uitsluiting van de bepalingen die onder de exclusieve bevoegdheid vallen van een andere controleautoriteit. Ter herinnering: het Controleorgaan op de politionele informatie (hierna het "COC") is bevoegd voor het onderzoek van de bepalingen die voorzien in een verwerking van persoonsgegevens door de geïntegreerde politie, het Vast comité van toezicht op de inlichtingen- en de veiligheidsdiensten (hierna "het comité R") is bevoegd voor het onderzoek van de bepalingen die voorzien in een gegevensverwerking door de inlichtingen en de veiligheidsdiensten.

A. DE RELEVANTE BEPALINGEN VAN DE EPRIVACYRICHTLIJN

8. De ePrivacyrichtlijn vormt een specificatie van en een aanvulling op de AVG op het vlak van de verwerking van persoonsgegevens in de sector van de elektronische communicatie. Ze stelt zich tot doel om de gebruikers van de elektronische communicatiediensten te beschermen tegen de gevaren

voor hun persoonsgegevens en hun persoonlijke levenssfeer die voortvloeien uit de nieuwe technologieën.

9. Het voorontwerp van wet voorziet in de omzetting van enkele bepalingen van deze Richtlijn, in het bijzonder van de artikelen 5, 6, 9 en 15. Om de leesbaarheid en de duidelijkheid te bevorderen, zal de Autoriteit deze bepalingen hierna herhalen.

10. **Artikel 5.1 van de ePrivacyrichtlijn** legt de lidstaten de verplichting op om "*het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische-communicatiediensten*" te garanderen. *Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel*"[2].

11. **Artikel 6.1 van de ePrivacyrichtlijn herhaalt en preciseert de reikwijdte van het vertrouwelijkheidsbeginsel betreffende de verkeersgegevens**: "*Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische-communicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1*"[3].

12. **Artikel 6.2 van de ePrivacyrichtlijn** laat de verwerking toe van verkeersgegevens "*die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen* "[4].

13. **Artikel 6.3 van de ePrivacyrichtlijn** laat de aanbieder van een openbare elektronische communicatiedienst toe om de verkeersgegevens te verwerken "*voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing [voor elektronische communicatiediensten of voor de levering van diensten met toegevoegde waarde, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn voorafgaande toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.*"[5].

[2] Woorden onderlijnd door de Autoriteit.
[3] Woorden onderlijnd door de Autoriteit.
[4] Woorden onderlijnd door de Autoriteit.
[5] Woorden onderlijnd door de Autoriteit.

14. **Artikel 6.5 van de ePrivacyrichtlijn** bepaalt als volgt: "*De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor facturering of verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude en marketing van elektronische communicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde, en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren*", terwijl **artikel 6.6 van diezelfde Richtlijn** het volgende bepaalt: "*De leden 1, 2, 3 en 5 zijn van toepassing onverminderd de mogelijkheid voor de bevoegde organen om overeenkomstig de toepasselijke wetgeving in kennis te worden gesteld van verkeersgegevens met het oog op het beslechten van geschillen, in het bijzonder met betrekking tot interconnectie en facturering*".

15. **Artikel 9.1 van de ePrivacyrichtlijn** bepaalt: "*Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. […]*"[6].

16. **Artikel 9.3 van de ePrivacyrichtlijn** bepaalt: "*De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden*".

17. **Artikel 15.1 van de ePrivacyrichtlijn** luidt als volgt: "*De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene*

[6] Woorden onderlijnd door de Autoriteit.

beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie"[7].

B. PRESENTATIE VAN HET 'SYSTEEM' DAT WORDT VOORGESTELD DOOR HET VOORONTWERP VAN WET BETREFFENDE HET BEWAREN VAN COMMUNICATIEGEGEVENS DOOR DE TELECOMOPERATOREN EN DE EVENTUELE COMMUNICATIE ERVAN AAN DE AUTORITEITEN[8]

❖ *Aangaande de gegevens die kunnen of moeten worden bewaard door de operatoren*

18. Verschillende bepalingen van de telecomwet die het voorontwerp van wet wil wijzigen, bieden de operatoren de mogelijkheid, of leggen hen de verplichting op, om verkeers- en/of locatiegegevens (met inbegrip van andere locatiegegevens dan verkeersgegevens) te bewaren en dit voor verschillende doeleinden:

1) De operatoren **mogen de verkeersgegevens bewaren en verwerken die noodzakelijk zijn voor de facturering van abonnees** of **het doen van interconnectiebetalingen** (**nieuw artikel 122 § 2** van de telecomwet[9])[10].

Die gegevens mogen worden bewaard *"**tot het einde van de periode van de betwisting van de factuur of tot het einde van de periode waarin de betaling gerechtelijk kan worden afgedwongen***" (nieuw artikel 122 § 2, laatste lid, van de telecomwet).

De telecomwet geeft enkel een **functionele definitie van de gegevens die mogen worden bewaard**: de verkeersgegevens die noodzakelijk zijn voor de facturering van de

[7] Woorden onderlijnd door de Autoriteit. Artikel 6 §§ 1 en 2 van het Vedrag over de Europese Unie leest zich als volgt: "" 1. De Unie erkent de rechten, vrijheden en beginselen die zijn vastgelegd in het Handvest van de grondrechten van de Europese Unie van 7 december 2000, als aangepast op 12 december 2007 te Straatsburg, dat dezelfde rechtskracht als de Verdragen heeft [...].

[8] De Autoriteit heeft dit systeem samengevat in een tabel in bijlage II.

[9] Artikel 122 § 2 van de telecomwet voorziet in de omzetting van artikel 6 § 2 van de ePrivacyrichtlijn.

[10] De huidige versie van artikel 122 § 2 van de telecomwet verplicht de operatoren - in plaats van hen toe te laten - om verkeersgegevens te bewaren voor de facturering van abonnees of het doen van interconnectiebetalingen. Dit artikel voorziet in de toekomst enkel een mogelijkheid voor de operatoren. De overschakeling van een verplichting tot bewaring van gegevens naar een mogelijkheid, wordt in de memorie van toelichting als volgt gerechtvaardigd: *"Enerzijds is een verplichting niet nodig aangezien de operatoren er alle belang bij hebben om deze gegevens te bewaren voor die doeleinden en vloeit uit artikel 110 van de wet [telecomwet] al minstens onrechtstreeks voort dat deze gegevens beschikbaar moeten zijn [artikel 110 van de telecomwet verplicht de operatoren om de abonnees een gespecificeerde basisfactuur te verstrekken en biedt de abonnees de mogelijkheid om op eenvoudig verzoek gratis een meer gespecificeerde versie te ontvangen van de basisfactuur die zij gekregen hebben]. Anderzijds maakt deze wijziging het mogelijk om beter aan te sluiten bij artikel 6, § 2, van de [ePrivacy]richtlijn dat wordt omgezet door artikel 122, § 2. Dat artikel 6, § 2 bepaalt dat, in afwijking op het principe van verwijdering of anonimisering, de verkeersgegevens voor factureringsdoeleinden mogen worden gebruikt".*

abonnee of voor het doen van interconnectiebetalingen. In tegenstelling tot wat is voorzien in de huidige versie van artikel 122 § 2 van de telecomwet geeft de nieuwe versie van deze bepaling niet langer de precieze categorieën van verkeersgegevens aan die voor dat doeleinde mogen worden bewaard[11].

2) De operatoren **mogen de verkeersgegevens verwerken die noodzakelijk zijn** om (i) de **marketing te verzorgen van de eigen elektronische communicatiediensten** en (ii) **het gebruikspatroon op te stellen van de abonnee** of de eindgebruiker[12], **op voorwaarde dat de toestemming werd verkregen** van de abonnee of, in voorkomend geval, de eindgebruiker (**nieuw artikel 122 § 3** van de telecomwet)[13]

3) De operatoren **moeten de locatiegegevens en andere verkeersgegevens die daartoe nodig zijn bewaren** om **een vermoed geval van fraude op te sporen en te analyseren[14]** of **een vermoed kwaadwillig gebruik[15]** van het elektronische communicatienetwerk (**nieuw artikel 122 § 4** van de telecomwet).

Deze bepaling voorziet dat de **locatiegegevens en de andere verkeersgegevens die nodig zijn** om een vermoed geval van fraude of een vermoed kwaadwillig gebruik van het elektronisch communicatienetwerk op te sporen en te analyseren **moeten worden bewaard gedurende minstens 4 maanden,** maar **ook voor een langere periode mogen worden bewaard** indien dat noodzakelijk is (zonder verdere precisering).

De **verkeersgegevens in verband met de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten**[16] van hun kant moeten **gedurende 12 maanden worden bewaard.**

---

[11] In de memorie van toelichting wordt dit schrappen van de lijst van verkeersgegevens die moesten worden bewaard in toepassing van artikel 122 § 2 van de telecomwet als volgt gerechtvaardigd: *"De lijst met verkeersgegevens die de operatoren dienden te behandelen volgens artikel 122, § 2 wordt geschrapt aangezien die lijst niet langer is afgestemd op de verschillende elektronische communicatiediensten die worden aangeboden door de operatoren. Die lijst was vooral relevant voor de vaste telefoniedienst […]"*.

[12] Verschillende bepalingen van de telecomwet geven de operatoren de mogelijkheid om de gebruikspatronen op te stellen van de abonnees en/of de consumenten of eindgebruikers zodat ze het voor hen meest gunstige tariefplan kunnen bepalen: artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid van de telecomwet.

[13] Artikel 122 § 3 van de telecomwet voorziet in de omzetting van artikel 6 § 3 van de ePrivacyrichtlijn.

[14] Het begrip 'fraude' wordt door het nieuwe artikel 122 § 4, eerste lid van de telecomwet als volgt gedefinieerd: *"een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of het contract en om zichzelf of iemand anders een ongeoorloofd voordeel te doen, via het gebruik van een elektronische-communicatiedienst*."

[15] Het begrip "kwaadwillig gebruik" wordt door het nieuwe artikel 122 § 4, tweede lid van de telecomwet als volgt gedefinieerd: *"een gebruik van het netwerk teneinde zijn contactpersoon te ontrieven of schade te berokkenen".*

[16] Het begrip "interpersoonlijke communicatiedienst" is afkomstig uit het nieuwe Europees wetboek voor elektronische communicatie (vastgesteld door Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018). Dit begrip wordt er als volgt in gedefinieerd: "*een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronische communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst*" (artikel 2.5) van de Richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie).

Volgens het nieuwe artikel 122 § 4 van de telecomwet **kan de Koning - maar moet hij niet - de verkeersgegevens bepalen die moeten worden bewaard** op grond van deze bepaling.

4) De operatoren **moeten gedurende minstens 12 maanden**[17] de **verkeersgegevens bewaren** die nodig zijn **om de veiligheid en de correcte werking van hun netwerken en diensten voor elektronische communicatie te garanderen**, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren (**nieuw artikel 122 § 4/1** van de telecomwet).

   Deze bepaling geeft een **functionele definitie van de gegevens die moeten worden bewaard**: de verkeersgegevens nodig om de veiligheid en correcte werking van de netwerken en diensten voor elektronische communicatie te garanderen. Ze geeft **geen definitie van de precieze categorieën van gegevens** die moeten worden bewaard en **machtigt de Koning evenmin om deze categorieën te bepalen**.

5) De operatoren **moeten de verkeersgegevens bewaren die nodig zijn** om te voldoen aan een **wettelijke verplichting** die op hen rust, voor de daartoe benodigde duur (**nieuw artikel 122 § 4/2** van de telecomwet)[18].

6) De **operatoren van mobiele netwerken mogen andere locatiegegevens dan verkeersgegevens** bewaren in de volgende gevallen (**nieuw artikel 123** van de telecomwet)[19]:

   - Wanneer **dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst**, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is;

[17] Het nieuwe artikel 122 § 4/1 van de telecomwet geeft aan dat de operatoren de gegevens "*voor een langere periode kunnen bewaren, die beperkt is tot het strikt noodzakelijke*".
[18] In de memorie van toelichting staat hierover het volgende te lezen: *"Een operator moet verkeersgegevens kunnen bewaren om te voldoen aan zijn wettelijke verplichtingen, bijvoorbeeld de boekhoudkundige of fiscale wetgeving of om te voldoen aan een bevel vanwege een autoriteit om de gegevens te bevriezen (ook bekend onder de naam "quick freeze"), wat bijvoorbeeld vervat is in het Wetboek van Strafvordering. Deze wettelijke verplichtingen vloeien niet voort uit deze paragraaf maar wel degelijk uit specifieke wetgevingen die daarin voorzien. Deze bepaling maakt het ook mogelijk om rekening te houden met de toekomstige ontwikkelingen (nieuwe verplichtingen).* Vervolgens preciseert de memorie van toelichting: "*Conform artikel 15, § 1, van de Richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG), moet elke wettelijke verplichting tot bewaring van verkeersgegevens in een democratische samenleving noodzakelijk, redelijk en proportioneel zijn, om het streefdoel te bereiken, en aangenomen worden met naleving van de algemene beginselen van het Europees recht, waaronder diegene die beoogd worden in het Handvest van de grondrechten van de Europese Unie en in het Europese Verdrag tot bescherming van de rechten van de mens*".
[19] Deze bepaling voorziet in een gedeeltelijke omzetting van artikel 9 van de ePrivacyrichtlijn.

- Wanneer dat **noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren**, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is;
- Wanneer **de gegevens anoniem gemaakt zijn**;
- Wanneer **de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens** en de abonnee of, in voorkomend geval, de eindgebruiker **zijn toestemming heeft gegeven**;
- Wanneer de **verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting** in hoofde van de operator.

7) De operatoren die aan de eindgebruikers elektronische communicatiediensten, alsook de operatoren die de onderliggende elektronische communicatienetwerken leveren, **moeten de abonnementsgegevens van de abonnee bewaren,** alsook **de technische gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische communicatiedienst te identificeren,** met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie (**nieuw artikel 126** van de telecomwet).

Die gegevens – met uitzondering van de andere dynamische IP-adressen dan datgene dat is gebruikt om in te tekenen op de dienst – **worden bewaard vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is** (nieuw artikel 126 van de telecomwet).

De **andere dynamische IP-adressen** dan datgene dat is gebruikt om in te tekenen op de dienst worden van hun kant **tot twaalf maanden na het einde van de sessie bewaard** (nieuw artikel 126 van de telecomwet).

Volgens het nieuwe artikel 126 § 2 van de telecomwet **bepaalt de Koning de te bewaren gegevens** alsook de vereisten waaraan deze gegevens moeten beantwoorden. **De artikelen 3 § 1, 4 § 1, 5 § 1 en 6 § 1 van het koninklijk besluit van 19 september 2013** tot uitvoering van de artikelen 126 en 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie en de artikelen 16/2/1 en 18/17/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna het "besluit van 19 september 2013"), zoals gewijzigd door het ontwerpbesluit, **voeren deze machtiging-wetgeving uit**.

8) De operatoren die aan de eindgebruikers elektronische communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische communicatienetwerken aanbieden, **moeten bepaalde verkeersgegevens en locatiegegevens voor bepaalde geografische zones bewaren en dit, in beginsel, gedurende 12 maanden**, tenzij een andere termijn is bepaald in het voorontwerp van wet (**nieuw artikel 126/1** van de telecomwet).

Het nieuwe artikel 126/1 § 1, derde lid, van de telecomwet preciseert als volgt: "*Die gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon*".
Het nieuwe artikel 126/1 § 2 van de telecomwet **bepaalt de categorieën van gegevens die moeten worden bewaard**:

- De **gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur** met het netwerk en **met de dienst en met betrekking tot de plaats van die apparatuur**, inclusief het netwerkaansluitpunt;
- De **communicatiegegevens**, met uitzondering van de inhoud, en met inbegrip van hun herkomst en hun bestemming;
- De **gegevens van oproeppogingen zonder resultaat**, voor zover die gegevens in het kader van de aanbieding van de bedoelde communicatiediensten worden gegenereerd of verwerkt door de operatoren (telefoongegevens) of door deze operatoren worden gelogd (internetgegevens).

De **Koning moet de te bewaren gegevens** bepalen en de vereisten waaraan deze gegevens moeten voldoen. **De artikelen 3 § 2, 4 § 2, 5 § 2 en 6 § 2 van het besluit van 19 september 2013**, zoals gewijzigd door het ontwerpbesluit, **voorzien in de uitvoering** van deze machtiging.

Het nieuwe artikel 126/1 § 3 van de telecomwet **bepaalt de geografische zones** waarbinnen de operatoren de gegevens bedoeld in het nieuwe artikel 126/1 § 2 van de telecomwet moeten bewaren. Het betreft de volgende geografische zones:

1° **De geografische zone bestaande uit**:

- De gerechtelijke arrondissementen waar **minstens 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar zijn vastgesteld,** over een gemiddelde van de drie voorbije kalenderjaren

- **De politiezones waar minstens 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar zijn vastgesteld** over een gemiddelde van de drie voorbije kalenderjaren, die deel uitmaken van een gerechtelijk arrondissement waar in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de 3 voorbije kalenderjaren.

De **bewaringstermijn van de gegevens varieert naargelang het aantal strafbare feiten zoals bedoeld in artikel 90ter van het WSV dat per 1000 inwoners per jaar is vastgesteld** over een gemiddelde van de drie voorbije kalenderjaren. Hoe groter dit aantal, hoe langer de bewaringstermijn (de telecomwet stelt drie drempels vast: 6 maanden indien er 3 of 4 strafbare feiten zoals bedoeld in artikel 90ter van het WSV per jaar per 1000 inwoners vastgesteld zijn, 9 maanden indien er 5 of 6 strafbare feiten zoals bedoeld in artikel 90ter van het WSV per jaar per 1000 inwoners vastgesteld zijn of 12 maanden indien er 7 of meer dan 7 strafbare feiten zoals bedoeld in artikel 90ter van het WSV per jaar per 1000 inwoners vastgesteld zijn).

2° **Alle zones waar het terroristische of extremistische dreigingsniveau**, bepaald door het Coördinatieorgaan voor de dreigingsanalyse (hierna "het OCAD") **ten minste niveau 3 bedraagt.** De gegevens moeten worden **bewaard zolang in deze zones niveau 3 blijft bestaan**.

In de memorie van toelichting wordt als volgt gepreciseerd: "*De bewaring is gericht, in de zin dat de bewaring geldt zolang het dreigingsniveau op 3 (dreiging mogelijk en waarschijnlijk) of op 4 (dreiging ernstig en zeer nabij) wordt ingeschaald. In deze gevallen wordt een algemene en ongedifferentieerde dataretentie opgelegd over heel het grondgebied*"[20].

3° **De gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit**. Het voorontwerp van wet noemt 17 categorieën van plaatsen.

4° **De zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking.** Het

[20] Memorie van toelichting, p. 52.

voorontwerp noemt 8 categorieën van plaatsen (waarvan sommige met 'subcategorieën' van plaatsen).

5° **De zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen**. Het voorontwerp noemt 6 categorieën van plaatsen.

9) De operatoren **moeten de nodige gegevens bewaren opdat de autoriteiten die gerechtigd zijn om de identiteit van de abonnees van de operatoren te verkrijgen, hen kunnen identificeren** (**nieuw artikel 127** van de telecomwet).

Die gegevens *"worden bewaard vanaf de datum van activering van de dienst tot twaalf maanden na de datum vanaf wanneer communicatie voor het laatst mogelijk is aan de hand van de gebruikte dienst"* (nieuw artikel 127 van de telecomwet*).*

Deze bepaling machtigt de Koning (maar verplicht hem niet) om de "*nadere bepalingen voor identificatie"* van de eindgebruiker/abonnee vast te leggen.

19. Behalve de preventieve bewaringsverplichtingen die de telecomwet oplegt aan de operatoren, voorziet het voorontwerp van wet ook in **de invoering van een artikel 39quinquies in het WSV** op grond waarvan **de procureur des Konings** tijdens het onderzoek van misdaden en wanbedrijven en als er sterke aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, **de bewaring, voor een duur die hij bepaalt, bevelen van bepaalde verkeers- en locatiegegevens** ten behoeve van het onderzoek (gegevens bedoeld in artikel 88bis, §1, eerste lid van het WSV[21]). De bewaring moet beperkt zijn tot enkel die gegevens die kunnen bijdragen tot de opheldering van het strafbare feit.

❖ Aangaande de mogelijkheden voor de autoriteiten om de door de operatoren bewaarde gegevens te raadplegen

20. De memorie van toelichting benadrukt dat het **nieuwe artikel 127/1 van de telecomwet** "*de lijst bevat van de categorieën van autoriteiten die toegang kunnen vragen tot de identificatie-, verkeers- en locatiegegevens bewaard bij de operatoren krachtens [artikelen 122, 123, 126, 126/1 en 127] ten behoeve van de autoriteiten, de eindgebruikers of voor hun eigen behoeften*".

[21] Het betreft de volgende gegevens: de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties werden of worden gedaan en gegevens betreffende de oorsprong of de bestemming van elektronische communicatie.

21. Deze bepaling luidt als volgt:

> "*Enkel de volgende autoriteiten mogen […] van de operatoren gegevens ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 en 27 om de doeleinden hieronder en volgens de vastgelegde voorwaarden die hen daartoe machtigen:*
> *1° de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronische-communicatienetwerk, zoals de inbreuken die online worden gepleegd;*
> *2° de inlichtingen- en veiligheidsdiensten teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;*
> *3° de autoriteiten belast met het verlenen van hulp aan personen, inclusief de Ombudsdienst voor telecommunicatie wat betreft het kwaadwillig gebruik van het netwerk, de hulpdiensten en de Cel Vermiste Personen van de federale politie;*
> *4° het Instituut in het kader van de uitvoering en controle van deze wet;*
> *5° de autoriteiten bevoegd voor het onderzoek van een veiligheidsprobleem op het netwerk of van de dienst*".

22. Om uit te maken tot welke gegevens welke autoriteiten toegang kunnen krijgen en waarom ("**wie kan toegang krijgen en waarom?** ") moet met name **het nieuwe artikel 127/1** van de telecomwet worden gelezen **in het licht van de (nieuwe versies van) de artikelen 122, 123, 126, 126/1 en 127 van de telecomwet**:

    - De **autoriteiten die een van de doeleinden nastreven** die zijn bedoeld in artikel 127/1 van de telecomwet[22] **kunnen toegang krijgen tot de gegevens die worden bewaard krachtens de** (nieuwe versies van de) **artikelen 122, 123, 126 en 127 voor elk van de doeleinden die zijn aangegeven in dit artikel 127/1** van de telecomwet. De autoriteiten die bevoegd zijn om een van de doeleinden na te streven die zijn opgesomd in artikel 127/1 van de telecomwet **kunnen dus toegang krijgen tot alle gegevens die worden bewaard in toepassing van de artikelen 122 en 123, 126 en 127 van de telecomwet**, ook als de bewaring ervan oorspronkelijk werd toegelaten of opgelegd voor een ander doeleinde dan

[22] In tegenstelling tot eerdere versies van de telecomwet herneemt het nieuwe artikel 127/1 een lijst van de doeleinden waarvoor de autoriteiten toegang kunnen krijgen tot de bewaarde gegevens, en niet langer een lijst van autoriteiten die toegang kunnen krijgen tot de gegevens. De memorie van toelichting rechtvaardigt deze perspectiefwijziging als volgt: *"Zo kan ervoor gezorgd worden dat de wetgeving de verschillende gevallen en de toekomstige ontwikkelingen beslaat. In dat kader dient te worden opgemerkt dat al snel is gebleken dat de besloten lijst van autoriteiten bedoeld in artikel 126, § 2, onvolledig was. De aanpassing van deze lijst is een moeilijke oefening (bijvoorbeeld omdat de wet werd aangevochten bij het Grondwettelijk Hof en maar moeilijk kan gewijzigd worden) en erg trage oefening gebleken, terwijl een overheid onmiddellijk operationele problemen ondervindt wanneer ze niet op de lijst staat, terwijl dat wel nodig is. De identificatie- en abonnementsgegevens bedoeld in de artikelen 126 en 127 zijn basisgegevens die benodigd zijn door een niet-verwaarloosbaar aantal autoriteiten. Dat aantal zal wellicht toenemen in de toekomst gezien de groei van het aantal online-inbreuken. Het is ook erg moeilijk om een volledige lijst op te stellen, met alle wettelijke bepalingen die de verschillende autoriteiten in staat stellen om de identificatie-, verkeers- en locatiegegevens te verkrijgen van de operatoren."*

datgene dat wordt nagestreefd door de autoriteit die toegang wenst tot de betreffende gegevens[23].

- De **autoriteiten die een van de doeleinden nastreven** die zijn bedoeld in artikel 127/1 van de telecomwet **kunnen toegang krijgen tot de krachtens het nieuwe artikel 126/1** van de telecomwet **bewaard**e **gegevens enkel voor de doeleinden waarvoor ze werden bewaard**, namelijk de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijk persoon.

23. Bovendien moet worden gepreciseerd dat opdat een autoriteit gegevens kan krijgen van een operator, het nodig is dat zij **van de doeleinden bedoeld in artikel 127/1** van de telecomwet nastreeft **en** dat **haar organieke of sectorale wet haar machtigt om deze gegevens te krijgen van de operator**[24].

24. Het voorontwerp van wet wil bovendien **een aantal bepalingen wijzigen die bepalen onder welke voorwaarden bepaalde autoriteiten toegang kunnen krijgen tot** de verkeers- en/of locatiegegevens die worden bewaard door de operatoren:

- Het voorontwerp wil een **§ 2, 2°/1 invoegen in artikel 14 van de wet betreffende het statuut van het BIPT** zodat het BIPT "*van de operatoren identificatie-, verkeers- of locatiegegevens kan vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten".*

- **Artikel 88bis van het SWV** geeft de onderzoeksrechter de volgende mogelijkheid: "*wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaarder straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij de verkeersgegevens doen opsporen van elektronische*

[23] De nieuwe artikelen 122 § 7 en 123 § 6 van de telecomwet bepalen immers als volgt, elk van hun kant: "*dit artikel [namelijk respectievelijk artikel 122 en artikel 123] doet geen afbreuk aan artikel 127/1*". Het nieuwe artikel 126 § 1, derde lid, luidt als volgt: "Deze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1 " en het nieuwe artikel 127 § 1, tweede lid: "*Deze gegevens en documenten worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1".*
[24] Artikel 127/1 bepaalt immers als volgt: "Enkel de volgende autoriteiten mogen […] van de operatoren gegevens ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1 en 127, om de doeleinden hieronder en volgens de vastgelegde voorwaarden die hen daartoe machtigen" (woorden onderlijnd door de Autoriteit).

communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan [en] de oorsprong of bestemming van de elektronische communicatie laten lokaliseren". Het voorontwerp **voert er opnieuw een paragraaf 3 aan toe** die door het Grondwettelijk Hof werd vernietigd in zijn arrest nr. 57/2021. Deze paragraaf bepaalt **bijzondere regels aangaande het doen opsporen van gegevens betreffende de elektronische communicatiemiddelen van advocaten en artsen** aangezien deze personen gebonden zijn door het beroepsgeheim.

- Het nieuwe **artikel 42 § 2 van de wet op het politieambt** bepaalt het volgende: *"Een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kan, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood en de opsporing van personen van wie de verdwijning onrustwekkend is, en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon opvorderen […]"*.

- De **wet op de inlichtingendiensten** die de voorwaarden bepaalt onder welke deze diensten toegang kunnen krijgen tot de gegevens die worden bewaard door de operatoren

- **Artikel 84 § 1van de FSMA-wet** bepaalt: "*mits de voorafgaandelijke toestemming van een onderzoeksrechter, kan de auditeur, of in zijn afwezigheid de adjunct-auditeur, wanneer hij van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen: 1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties werden gedaan; 2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren, met inbegrip van de telefoonnummers en netwerkadressen; 3° de betalingsdetails van de elektronische communicatiediensten opvragen […]. De auditeur of, in zijn afwezigheid, de adjunct-auditeur doet in zijn beslissing opgave van de feitelijke omstandigheden die de maatregel rechtvaardigen en hij houdt rekening met het evenredigheids- en subsidiariteitsbeginsel bij de motivering van zijn beslissing. […]*'. Het voorontwerp van wet **wil een nieuwe § 1bis/1 toevoegen** aan artikel 84 van de FSMA-wet **op grond waarvan de auditeur de operatoren kan bevelen om bepaalde gegevens te bewaren indien deze gegevens riskeren te worden verwijderd of anoniem te worden gemaakt,** tot hij de

toestemming van een onderzoeksrechter heeft bekomen voor de opvraging van deze gegevens.

- Het voorontwerp wil de "*daartoe door de Koning aangewezen statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu"*, die belast zijn met de uitvoering van de wet betreffende de bescherming van de gezondheid en van zijn uitvoeringsbesluiten, evenals van de verordeningen van de Europese Unie en die behoren tot de bevoegdheden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, de mogelijkheid geven om "*natuurlijke en rechtspersonen te identificeren aan de hand van het telefoonnummer van de betrokkene of het IP-adres dat aan de bron van de elektronische communicatie ligt".* **Volgens het nieuwe artikel 11 § 1 van de wet betreffende de bescherming van de gezondheid** mogen deze statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu "*met gemotiveerd verzoek de verstrekking van de identificatiedocumenten en gegevens vorderen […]*".

- Het voorontwerp wil **een § 2 toevoegen aan artikel 62 van de NIS-wet** dat bepaalt dat het Centrum voor Cybersecurity België (hierna "het CCB" genaamd) "[v*]an elektronische communicatieoperatoren identificatie-, verkeers- of locatiegegevens die door hen worden bewaard kan verkrijgen, indien dat strikt noodzakelijk is voor de uitvoering van de taken opgesomd in artikel 60, a) tot e), van de NIS-wet.*"[25]

C. HERHALING VAN DE VOORWAARDEN WAARAAN DE NORMEN DIE VOORZIEN IN EEN BEWARING VAN VERKEERS_ EN/OF LOCATIEGEGEVENS EN IN DE EVENTUELE COMMUNICATIE ERVAN AAN DE AUTORITEITEN MOETEN VOLDOEN

25. De **bewaring van verkeers- en locatiegegevens vormt een ernstige inmenging in de privacyrechten en in het recht op bescherming van de persoonsgegevens.** Het HvJ-EU heeft al meermaals benadrukt dat "*verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke*

[25] De taken opgesomd in artikel 60 a) tot e) van de NIS-wet zijn de volgende:
"*a) monitoren van incidenten op nationaal en internationaal niveau, met inbegrip van de verwerking van persoonsgegevens met betrekking tot het monitoren van deze incidenten;*
b) ten behoeve van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;
c) reageren op incidenten;
d) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis;
e) computerbeveiligingsproblemen opsporen, observeren en analyseren"

of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale n het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie"[26].

26. **De eventuele communicatie** van deze gegevens aan de autoriteiten is **een andere inmenging** dan deze die wordt veroorzaakt door hun bewaring**,** maar eveneens **ernstig**.

27. De Autoriteit wijst erop dat elke inmenging in het recht op bescherming van persoonsgegevens, vooral als het gaat om een ernstige inmenging zoals in deze, slechts toelaatbaar is **als ze wordt omkaderd door een voldoende duidelijke en nauwkeurige norm waarvan de toepassing voor de betrokken personen voorzienbaar is.** Elke norm die de verwerking van persoonsgegevens omkadert, in het bijzonder wanneer die verwerking een ernstige inmenging vormt in de rechten en vrijheden van de betrokken personen, moet voldoen aan de **eisen van voorzienbaarheid en nauwkeurigheid** zodat **de betrokken personen bij het lezen van de norm duidelijk zien aan welke verwerkingen hun gegevens worden onderworpen en in welke omstandigheden een gegevensverwerking is toegelaten**. In uitvoering van artikel 6.3 van de AVG, gecombineerd met de artikelen 22 van de Grondwet en 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, moeten de **essentiële factoren van de verwerking** er **nauwkeurig in worden beschreven**. Het betreft in het bijzonder het of de precieze **doeleinde(n)** van de verwerking; de **identiteit van de verwerkingsverantwoordelijke(n)**; de **categorieën van verwerkte gegevens**, met dien verstande dat ze - in overeenstemming met artikel 5.1. van de AVG, "*ter zake dienend, relevant en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt*" moeten zijn; de **categorieën van betrokken personen** (personen van wie de gegevens worden verwerkt); de **bewaringstermijn van de gegevens**; de ontvangers of **categorieën van ontvangers** waaraan hun gegevens worden meegedeeld en de **omstandigheden waarin en de redenen waarvoor ze worden meegedeeld** en **alle maatregelen om een rechtmatige en behoorlijke verwerking van deze persoonsgegevens te garanderen.**

28. De inmenging in het recht op gegevensbescherming moet niet alleen wettelijk zijn, maar is ook slechts toelaatbaar als ze noodzakelijk is en evenredig met het (de) beoogde doel(en). Via verschillende arresten waarin het zich uitsprak over de conformiteit van de bewaring van de verkeers- en

[26] Zie bijvoorbeeld, HvJ-EU, 8 april 2014, *gevoegde zaken C-293/12 en C-594/12 "Digital Rights Irland* et *al*", § 27; HvJ-EU, 21 december 2016, *gevoegde zaken C-203/15 en C-698/15 "Tele2 Sverige et al"*, § 99; HvJ-EU, 2 oktober 2020, *gevoegde zaken C-511/18, C-512/18 en C-520/18 "Quadrature du Net et al "*, § 117.

locatiegegevens en de eventuele latere communicatie ervan aan de autoriteiten met het recht op privacy en op bescherming van de persoonsgegevens[27] heeft het **HvJ-EU de reikwijdte van de eisen van noodzaak en evenredigheid verduidelijkt**. Het Hof van Luxemburg heeft daarmee **de voorwaarden verduidelijkt** waaraan de wetgevende maatregelen moeten voldoen die **een bewaring van de verkeers- en locatiegegevens** en **hun eventuele communicatie aan de autoriteiten,** vooral voor repressieve doeleinden, moeten voldoen.

29. De regelingen die voorzien in een bewaring van de gegevens moeten een **evenwichtige afweging maken** tussen enerzijds **de doelstelling van algemeen belang** die door de inmenging wordt nagestreefd en anderzijds **de rechten op de privacy en op de bescherming van de persoonsgegevens**. Er moet onder meer **worden nagegaan of de ernst van de inmenging evenredig is met het belang van de nagestreefde doelstelling van algemeen belang[28]**. Anders gezegd, **hoe belangrijker de nagestreefde doelstelling van algemeen belang, hoe meer de regeling die een bewaring van gegevens oplegt een inmenging kan vormen** in de rechten en vrijheden van de betrokken personen. In ieder geval **moet de bewaring van de verkeers- en locatiegegevens** in een democratische samenleving **de uitzondering blijven[29]**. Die gegevens mogen dus niet systematisch en continu worden bewaard, hoezeer dat ook zware criminaliteit kan bestrijden en ernstige bedreiging van de openbare veiligheid kan voorkomen. Het Hof van Justitie is van oordeel dat een **algemene en ongedifferentieerde bewaring van de gegevens** een **zodanig grote inmenging vormt** in de grondrechten van de betrokken personen dat ze **in beginsel niet toelaatbaar is[30]** (tenzij, en daar zullen we nog op terugkomen, voor de bescherming van de nationale zekerheid[31]).

30. Bovendien eist het HvJ-EU dat de regeling die voorziet in een bewaring van de gegevens **voldoet aan objectieve criteria** die **een verband leggen tussen de te bewaren gegevens en het beoogde doel[32]**.

31. Door bij het onderzoek van verschillende categorieën van maatregelen die een bewaring van de verkeers- en/of locatiegegevens opleggen het evenredigheidsbeginsel toe te passen, **identificeerde het Hof de omstandigheden waarin dergelijke maatregelen al dan niet toelaatbaar waren**.

- ***Maatregelen die voorzien in een algemene en ongedifferentieerde bewaring van de gegevens ten behoeve van de bescherming van de nationale veiligheid***

[27] Zie meer bepaald HvJ-EU, 8 april 2014, *gevoegde zaken C-293/12 en C-594/12 "Digital Rights Irland* et *al*"; HvJ-EU, 21 december 2016, *gevoegde zaken C-203/15 en C-698/15 "Tele2 Sverige et al"* HvJ-EU, 2 oktober 2020, *gevoegde zaken C-511/18, C-512/18 en C-520/18 "Quadrature du Net et al "*, HvJ-EU, 2 maart 2021, zaak C-746/18 "Prokuratuur".
[28] HvJ-EU, arrest van 2 oktober 2018, § 55; HvJ-EU, arrest van 6 oktober 2020, § 131; HvJ-EU, arrest van 2 maart 2021, § 32.
[29] HvJ-EU, arrest van 6 oktober 2020, § 142.
[30] HvJ-EU, arrest van 6 oktober 2020, § 141.
[31] HvJ-EU, arrest van 6 oktober 2020, § -137.
[32] HvJ-EU, arrest van 6 oktober 2020, § 133.

32. De doelstelling van **bescherming van de nationale veiligheid** is zo belangrijk dat het HvJ-EU erkent dat **ze een algemene en ongedifferentieerde bewaring** van locatie- en verkeersgegevens kan rechtvaardigen, **op voorwaarde** dat er een **ernstige bedreiging van de nationale veiligheid bestaat die reëel en actueel of voorzienbaar is** (en **enkel** voor **zolang deze bedreiging bestaat**)[33].

33. Het Hof voegt eraan toe dat het essentieel is dat de **beslissing** die de aanbieders van elektronische communicatiediensten gelast **om die gegevens te bewaren** het voorwerp kan uitmaken van een **effectieve controle**, hetzij door een rechtbank, hetzij door een onafhankelijk administratief orgaan waarvan de beslissing een bindend effect heeft, met het doel om **het bestaan van een van deze situaties** te controleren en **de naleving van de voorwaarden en waarborgen die moeten worden voorzien**[34].

- ***Maatregelen die voorzien in een preventieve gerichte bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreiging van de openbare veiligheid***

34. Volgens het HvJ-EU **overstijgt een algemene en ongedifferentieerde bewaring** van verkeers- en locatiegegevens **voor de bestrijding van zelfs zware criminaliteit** in een democratische samenleving **wat strikt noodzakelijk is**[35]. De lidstaten **mogen dus geen algemene en ongedifferentieerde bewaring van deze gegevens opleggen om zware criminaliteit te bestrijden**. *A fortiori* mag een dergelijke maatregel niet worden aangewend om strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen.[36] Toch meent het Hof dat een **gerichte preventieve bewaring** van verkeers- en locatiegegevens met het oog op de **bestrijding van zware criminaliteit**, de voorkoming van **ernstige bedreigingen voor de openbare veiligheid** en, *a fortiori*, de **bescherming van de nationale veiligheid** kan worden gerechtvaardigd[37]. De bestrijding van criminaliteit in het algemeen kan een dergelijke preventieve bewaring, zelfs als ze gericht is, echter niet rechtvaardigen.

35. Volgens het Hof kunnen **verschillende criteria** worden gebruikt **om de preventieve bewaring** van gegevens te richten bij de **bestrijding van zware criminaliteit**: de bewaring kan worden beperkt tot **gegevens betreffende een bepaalde periode** en/of **een geografische zone** en/of **een kring van personen** die op de een of andere manier kunnen betrokken zijn bij een zwaar

[33] HvJ-EU, arrest van 6 oktober 2020, § 137.
[34] HvJ-EU, arrest van 6 oktober 2020, § 139.
[35] HvJ-EU, arrest van 6 oktober 2020, § 141.
[36] HvJ-EU, arrest van 6 oktober 2020, § 140.
[37] HvJ-EU, arrest van 6 oktober 2020, § 146-151.

strafbaar feit, of personen die om andere redenen via de bewaring van hun gegevens zouden kunnen bijdragen tot de bestrijding van zware criminaliteit[38].

36. Aangaande de afbakening van de bewaring van gegevens op basis van **geografische criteria**, oordeelt het HvJ-EU dat ze toelaatbaar is wanneer de bevoegde nationale autoriteiten **op basis van objectieve en niet-discriminerende factoren** van mening zijn dat er in een of meerdere geografische gebieden sprake is van een **situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd**. Het Hof preciseert: "*Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones"*[39].

37. In alle gevallen mogen **de maatregelen die voorzien in een gerichte gegevensbewaring** voor de bestrijding van zware criminaliteit **niet langer gelden dan strikt noodzakelijk is** in het licht van het ermee beoogde doel en van de **omstandigheden** waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

- ***Maatregelen die voorzien in een preventieve en algemene bewaring van de IP-adressen ten behoeve van de bestrijding van zware criminaliteit en de bescherming van de openbare veiligheid***

38. Het HvJ-EU merkt op dat dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd[40]. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens[41]. De IP-adressen die aan de bron van een verbinding zijn toegewezen, zijn volgens het HvJEU dus minder gevoelig dan andere verkeersgegevens, maar het HvJEU wijst erop dat dergelijke IP-adressen, - in combinatie met de IP-adressen van de ontvanger van de communicatie - niettemin kunnen worden gebruikt om de volledige zoekgeschiedenis en daardoor zijn online activiteiten te traceren en aan de

[38] HvJ-EU, arrest van 8 april 2014, § 59; HvJ-EU, arrest van 21 december 2016, § 106; HvJ-EU, arrest van 6 oktober 2020, § 144.
[39] HvJ-EU, arrest van 6 oktober 2020, § 150.
[40] HvJ-EU, arrest van 6 oktober 2020, § 152.
[41] HvJ-EU, arrest van 6 oktober 2020, § 152.

hand van die gegevens een gedetailleerd beeld van de betrokkene op te stellen[42]. **De bewaring en analyse van deze gegevens vormen dan ook ernstige inmengingen in de grondrechten van de internetgebruiker[43]**.

39. Evenwel meent het dat **het opleggen van een algemene en ongedifferentieerde bewaring van de IP-adressen** die zijn toegewezen aan de bron van de verbinding[44] **toelaatbaar is voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van deze gegevens dienen te regelen[45]**. Wat de ernst van de inmenging veroorzaakt door de algemene en ongedifferentieerde bewaring van de IP-adressen betreft, meent het Hof dat **enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid,** alsmede de bescherming van de nationale veiligheid, **die inmenging rechtvaardigen[46]**. Het Hof voegt eraan toe dat de **bewaartermijn niet langer mag zijn dan strikt noodzakelijk is** gelet op het nagestreefde doel[47]. Tot slot moet een dergelijke maatregel voorzien in **strikte voorwaarden en waarborgen** met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de online communicatie en de online activiteiten van de betrokken personen.[48].

- ***Maatregelen die voorzien in een algemene en ongedifferentieerde bewaring van de gegevens betreffende de burgerlijke identiteit***

40. Het HvJ-EU benadrukt dat **met gegevens betreffende de burgerlijke identiteit** van de gebruikers van elektronische communicatiemiddelen alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal keer dat in een specifieke periode met bepaalde personen is gecommuniceerd[49]. **De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als "ernstig" worden aangemerkt[50]**. Het Hof verzet zich dus niet tegen een wettelijke maatregel die de **bewaring** oplegt van **de gegevens inzake de burgerlijke identiteit van alle gebruikers** van elektronische communicatiemiddelen gedurende een niet nader bepaalde periode, **ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten** en het **waarborgen van de openbare veiligheid,** zonder dat het daarbij hoeft

[42] HvJ-EU, arrest van 6 oktober 2020, § 152-153.
[43] HvJ-EU, arrest van 6 oktober 2020, § 153.
[44] Het Hof merkt inderdaad op dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronische communicatiediensten na afloop van de periode waarvoor deze adressen werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel die de bewaring van deze gegevens oplegt.
[45] HvJ-EU, arrest van 6 oktober 2020, § 155.
[46] HvJ-EU, arrest van 6 oktober 2020, § 156.
[47] HvJ-EU, arrest van 6 oktober 2020, § 156.
[48] HvJ-EU, arrest van 6 oktober 2020, § 156.
[49] HvJ-EU, arrest van 6 oktober 2020, § 157; HvJ-EU, arrest van 2 maart 2021, § 34.
[50] HvJ-EU, arrest van 6 oktober 2020, § 157.

te gaan om ernstige strafbare feiten of om ernstige bedreigingen of verstoringen van de openbare veiligheid[51].

- ***Maatregelen die voorzien in de 'spoedbewaring' van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit***

41. De verkeers- en locatiegegevens die door aanbieders van elektronische communicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6, of 15 van de ePrivacyrichtlijn moeten in beginsel worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen die zijn vastgesteld door de nationale bepalingen tot omzetting van de ePrivacyrichtlijn[52]. Het HvJ-EU erkent echter **dat het noodzakelijk kan zijn om die gegevens ook na het verstrijken van die termijnen te doen bewaren** "*teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd*"[53].

42. Het Hof Van Luxemburg **laat toe** dat de lidstaten in hun wetgeving **voorzien in de mogelijkheid** om aanbieders van elektronische communicatiediensten **een bevel op te leggen tot 'spoedbewaring'** van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode, krachtens de wettelijke bepalingen tot omzetting van de artikelen 5, 6, 9 en 15 van de ePrivacyrichtlijn.[54]. Een 'spoedbewaring' kan worden opgelegd voor gegevens waarvan de oorspronkelijke bewaring een ander doel diende dan de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid.

43. De **beslissing** om te doen overgaan tot een spoedbewaring van gegevens is echter enkel toegelaten onder de **volgende voorwaarden**[55]:
    - De beslissing moet worden **onderworpen aan effectieve rechterlijke toetsing;**
    - De beslissing mag enkel worden genomen **voor de bestrijding van zware criminaliteit** en, *a fortiori*, de **bescherming van de nationale veiligheid;**

[51] HvJ-EU, arrest van 6 oktober 2020, § 158.
[52] HvJ-EU, arrest van 6 oktober 2020, § 160.
[53] HvJ-EU, arrest van 6 oktober 2020, § 161.
[54] HvJ-EU, arrest van 6 oktober 2020, § 163.
[55] HvJ-EU, arrest van 6 oktober 2020, § 164.

- De bewaarplicht **mag uitsluitend gelden voor** verkeers- en locatiegegevens **die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid**[56]**;**

- De **bewaringstermijn** van deze gegevens moet worden **beperkt tot wat strikt noodzakelijk is**, maar kan worden verlengd als de omstandigheden en het door de maatregel beoogde doel dit rechtvaardigen.

➢ ***Eisen aangaande de technische en organisatorische maatregelen betreffende de bewaring van de gegevens door de aanbieders van elektronische communicatiediensten***

44. Het HvJ-EU benadrukt dat in overeenstemming met artikel 4 §§ 1 en 1bis van de ePrivacyrichtlijn de aanbieders passende **technische en organisatorische maatregelen** moeten nemen om **de bewaarde gegevens doeltreffend te beschermen tegen het risico van misbruik** en **tegen elke onrechtmatige toegang tot deze gegevens**[57]. Het Hof benadrukt in het bijzonder dat de nationale regeling moet bepalen **dat de gegevens op het grondgebied van de Unie worden bewaard** en na afloop van de bewaarperiode **onherstelbaar worden vernietigd**[58]. Bovendien moeten de **lidstaten waarborgen dat een onafhankelijke autoriteit toeziet op de inachtneming van het hoge niveau van bescherming dat wordt gewaarborgd** door het Unierecht betreffende de bescherming van natuurlijke personen ter zake van de verwerking van hun persoonsgegevens.

➢ ***Aangaande de toegang tot de door de aanbieders van elektronische communicatiediensten bewaarde gegevens***

45. Om te voldoen aan de eis van voorzienbaarheid moet de mededeling van de door de aanbieders van elektronische communicatiediensten bewaarde gegevens aan de nationale autoriteiten **worden onderworpen aan duidelijke en nauwkeurige regels** die aangeven **in welke omstandigheden** en **onder welke voorwaarden** die mededeling heeft plaatsgevonden. Om te waarborgen dat de

[56] Het HvJ-EU erkent dat de spoedbewaring van gegevens betrekking kan hebben op gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht, maar ook op *"gegevens […] die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd.* " (HvJ-EU, arrest van 6 oktober 2020, § 165).
[57] HvJ-EU, arrest van 21 december 2016, § 122.
[58] HvJ-EU, arrest van 21 december 2016, § 122.

toegang tot de bewaarde gegevens niet verder gaat dan strikt noodzakelijk is, moet de nationale regeling de **materiële en procedurele voorwaarden** bepalen[59]**:**

- **De nationale regeling moet bepalen voor welk doel de autoriteiten toegang kan worden verleend tot de door de aanbieders van elektronische communicatiediensten bewaarde gegevens**. Volgens het Hof kan **een dergelijke toegang in beginsel enkel worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd[60]**. In geen geval mag toegang tot dergelijke gegevens worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het **evenredigheidsbeginsel** kan **daarentegen** de **toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit** worden **gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid**, mits de materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen. Bovendien laat het Hof de **lidstaten toe om in hun wetgeving te bepalen dat gegevens die zijn bewaard in overeenstemming met de artikelen 5, 6, 9 of 15 van de ePrivacyrichtlijn** aan de autoriteiten mogen worden meegedeeld, met inachtneming van de materiële en procedurele voorwaarden, **met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid[61]**.

  De regeling betreffende de toegang tot de gegevens moet dus bepalen met welk doel de autoriteiten toegang kunnen krijgen tot de gegevens, maar ze mag zich er niet toe beperken te eisen dat de toegang wordt verleend voor een van de in artikel 15, &1 van de ePrivacyrichtlijn genoemde doelstellingen, zelfs indien dit de bestrijding van zware criminaliteit zou zijn[62]. De regeling moet ook voorzien in de materiële en procedurele voorwaarden voor dit gebruik[63].

- **De betrokken nationale regeling moet aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden toegang tot de gegevens moet worden verleend[64]**. In dit verband kan in beginsel voor

[59] HvJ-EU, arrest van 21 december 2016, §§ 118-121.
[60] HvJ-EU, arrest van 2 maart 2021, § 31.
[61] HvJ-EU, arrest van 6 oktober 2020, § 164-165.
[62] HvJ-EU, arrest van 21 december 2018, § 118.
[63] HvJ-EU, arrest van 2 maart 2021, § 49.
[64] HvJ-EU, arrest van 2 maart 2021, § 50.

het doel van bestrijding van de criminaliteit slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf. In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter ook toegang tot de gegevens van andere personen kunnen worden verleend wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren.

- **De toegang van de bevoegde nationale autoriteiten** tot de bewaarde gegevens moet, in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, **worden onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit.** Deze rechterlijke instantie of deze entiteit **moet haar beslissing geven op een met redenen omkleed verzoek van deze autoriteiten**[65]. Bovendien benadrukte het Hof dat **de autoriteit belast met het voorafgaand toezicht**, ongeacht of het gaat om een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit, ten opzichte van de autoriteit die toegang wil krijgen tot de gegevens de **hoedanigheid van derde** moet hebben zodat ze bij de uitoefening van haar taken objectief en onpartijdig kan handelen, vrij van elke invloed van buitenaf[66].

- De autoriteiten die toegang hebben gekregen tot de gegevens **moeten de betrokken personen daarvan op de hoogte brengen als dat de door deze autoriteiten gevoerde onderzoeken niet in gevaar kan brengen**. Dit is immers noodzakelijk om de betrokken personen in staat te stellen om, in geval van schending van hun rechten, met name gebruik te maken van het recht van beroep waarin artikel 15,§ van de ePrivacyrichtlijn, gelezen in samenhang met de AVG, voorziet[67].

[65] HvJ-EU, arrest van 21 december 2018, § 120; HvJ-EU, arrest van 2 maart 2021, § 51.
[66] HvJ-EU, arrest van 2 maart 2021, § 52.
[67] HvJ-EU, arrest van vrijdag 21 december 2018, § 121.

D. ONDERZOEK VAN DE CONFORMITEIT VAN HET VOORONTWERP VAN WET EN VAN HET ONTWERPBESLUIT MET DE EISEN VAN HET EUROPEES RECHT EN VAN DE GRONDBEGINSELEN INZAKE GEGEVENSBESCHERMING

46. De Autoriteit zal nagaan of de verschillende bepalingen van het voorontwerp van wet die de bewaring van verkeers- en/of locatiegegevens toelaten of opleggen met het oog op de eventuele mededeling ervan aan de autoriteiten in overeenstemming zijn met de grondbeginselen inzake gegevensbescherming.

47. De Autoriteit acht het noodzakelijk om, voorafgaand aan dit onderzoek, eraan te herinneren dat, zoals het Grondwettelijk Hof in zijn arrest van 21 april 2021 heeft gedaan, de jurisprudentie van het HJEU "een verandering van perspectief oplegt ten aanzien van de door de wetgever gemaakte keuze": **de verplichting om verkeers- en locatiegegevens te bewaren moet de uitzondering zijn, niet de regel**. Er moet echter worden opgemerkt dat het **voorontwerp van wet** - dat bedoeld is als reactie op de vernietiging van de wet van 2016 - **deze perspectiefwijziging niet volledig doorvoert**, aangezien, zoals de Autoriteit hieronder zal toelichten, het wetsontwerp voornemens is nieuwe maatregelen voor de bewaring van verkeers- en locatiegegevens op te leggen (om fraude en kwaadwillig gebruik van het netwerk te bestrijden en de veiligheid van het netwerk te waarborgen) die ertoe kunnen leiden dat de facto opnieuw veralgemeende en ongedifferentieerde verplichtingen inzake gegevensbewaring worden ingevoerd. **De Autoriteit dringt erop aan dat de wetgever het wetsontwerp aanpast om ervoor te zorgen dat de aan te nemen wet voldoet aan alle door het HJEU en het Grondwettelijk Hof opgelegde vereisten.** Dit is een essentiële voorwaarde om het vertrouwen van de burgers te behouden.

48. De Autoriteit is zich ervan bewust dat het bewaren van verkeers- en locatiegegevens noodzakelijk kan zijn om het recht op veiligheid en het recht op een doeltreffende voorziening in rechte te waarborgen, die, net als het recht op privacy en de bescherming van persoonsgegevens, grondrechten zijn die zijn verankerd in de Belgische grondwet, het Europees Verdrag tot bescherming van de rechten van de mens en het Handvest van de grondrechten van de Europese Unie. Het HvJEU erkent in zijn arrest van 6 oktober 2020 dat deze verschillende grondrechten met elkaar moeten worden verzoend[68]. In die context herinnert zij eraan dat "een doelstelling van algemeen belang niet kan worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten"[69]. Bij de analyse van de evenredigheid van de verschillende maatregelen tot bewaring van verkeers- en locatiegegevens heeft het HvJEU dus steeds getracht deze verzoening tussen de verschillende in het geding zijnde grondrechten tot stand te brengen. **De**

[68] HvJEU, arrest van 6 oktober 2020, § 127.

[69] HvJEU, arrest van 6 oktober 2020, § 130.

Autoriteit verzoekt de wetgever de tijd te nemen om na te denken over en grondig te analyseren hoe, overeenkomstig de Europese jurisprudentie, het grondrecht op veiligheid en het recht op een doeltreffende voorziening in rechte, enerzijds, en het grondrecht op eerbiediging van het privé-leven en op bescherming van persoonsgegevens, anderzijds, met elkaar kunnen worden verzoend.

1) Voorafgaande opmerking over de interactie tussen het voorontwerp van wet en het Europees wetboek voor elektronische communicatie

49. Het voorontwerp van wet en het ontwerpbesluit brengen een aantal wijzigingen aan in de artikelen 122 en volgende van de telecomwet teneinde de terminologie die ze gebruiken af te stemmen op de terminologie van het Europees wetboek voor elektronische communicatie (hierna het "EWEC"). Het voorontwerp van wet en het ontwerpbesluit gebruiken immers, zonder ze te definiëren, verschillende begrippen die nog niet zijn gedefinieerd (in het bijzonder de begrippen "interpersoonlijke communicatiedienst" of "nomadische dienst") omdat de telecomwet deze begrippen zal definiëren nadat ze wordt gewijzigd door de wet die het EWEC omzet in intern recht. De afgevaardigde van de minister heeft bevestigd dat aan die tekst de laatste hand wordt gelegd en dat hij vóór het parlementair verlof zal worden ingediend bij het Parlement. De Autoriteit neemt daar nota van en benadrukt dat **als de tekst, die een aantal nieuwe begrippen definieert, niet wordt goedgekeurd vóór de goedkeuring van het voorontwerp van wet en het ontwerpbesluit, in het voorontwerp van wet de definities moeten worden toegevoegd die erin worden gebruikt**.

50. Bovendien benadrukt de Autoriteit **dat de omzetting van het EWEC tot gevolg zal hebben dat met name de begrippen "operatoren" en "elektronische communicatiediensten" opnieuw moeten worden gedefinieerd**. Het begrip "elektronische communicatiedienst" zal worden omschreven als "*een gewoonlijk tegen vergoeding via elektronische communicatiediensten aangeboden dienst die, met uitzondering van diensten waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd, de volgende soorten diensten omvat a) een internettoegangsdienst; b) een interpersoonlijke communicatiedienst; en c) diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten en voor omroep worden gebruikt*". Het begrip "elektronische communicatiedienst" wordt dus veel ruimer dan nu het geval is aangezien het in het bijzonder de "interpersoonlijke communicatiediensten" zal omvatten die als volgt worden omschreven: "*een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronische communicatienetwerken tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk*

dat onlosmakelijk verbonden is met een andere dienst". Het begrip "operator" zal na omzetting van het EWEC in de telecomwet worden omschreven als "*een persoon of een onderneming die een openbaar elektronisch communicatienetwerk of een elektronische communicatiedienst aanbiedt aan het publiek*".

51. Deze definitiewijzigingen zullen tot gevolg hebben dat ondernemingen die 'over the top' elektronische communicatiediensten aanbieden, zoals WhatsApp, Skype, Signal, of Telegram, zullen worden beschouwd als operatoren die zijn onderworpen aan de verplichtingen om verkeers- en locatiegegevens te bewaren die door de telecomwet zullen worden opgelegd na wijziging door het voorontwerp. **De Autoriteit benadrukt dat deze nieuwe definities van de begrippen "elektronische communicatiedienst" en "operator" het toepassingsgebied zullen verruimen van de bepalingen die de bewaring van die gegevens toelaten of opleggen**.

2) Bewaring van de gegevens voor de facturering en het doen van interconnectiebetalingen (nieuw artikel 122 § 2 van de telecomwet)

52. Het nieuwe artikel 122 § 2 van de telecomwet, dat artikel 6 § 2 van de ePrivacyrichtlijn omzet, **laat de operatoren toe om de verkeersgegevens te bewaren en te verwerken die nodig zijn voor de facturering van de abonnees of voor het doen van interconnectiebetalingen.** Voorafgaand aan de verwerking stelt de operator de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben in kennis van de soorten verkeersgegevens die worden verwerkt, de precieze doeleinden van de verwerking en de duur van de verwerking. De verwerking van de gegevens is slechts toegestaan tot het einde van de periode van de betwisting van de factuur of tot het einde van de periode waarin de betaling gerechtelijk kan worden afgedwongen.

53. De **gegevensverwerkingen** die zijn toegelaten door het nieuwe artikel 122§2 van de telecomwet **hebben een rechtsgrond in de zin van artikel 6.1 van de AVG:** de uitvoering van een overeenkomst waarbij de betrokkene partij is voor de verwerkingen nodig voor de facturering van de abonnees (artikel 6.1.b) van de AVG) en de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde voor de verwerkingen nodig voor het doen van interconnectiebetalingen (artikel 6.1.f) van de AVG).

54. De **nagestreefde doeleinden** – facturering van de abonnees of het doen van interconnectiebetalingen – zijn, conform de eis van artikel 5.1.b) van de AVG, ***"welbepaald, uitdrukkelijk omschreven en gerechtvaardigd"*.**

55. De nieuwe versie van artikel 122 § 2 van de telecomwet vermeldt niet langer – in tegenstelling tot de eerdere versie van artikel 122 § 2 van de telecomwet – de precieze gegevens die op grond van deze

bepaling mogen worden verwerkt. Deze schrapping vermindert weliswaar de voorzienbaarheid van de norm die de gegevensverwerking toelaat, maar de Autoriteit acht ze niettemin toelaatbaar. De bepaling geeft immers aan dat enkel de verkeersgegevens die nodig zijn voor de facturering van de abonnees of het doen van interconnectiebetalingen mogen worden verwerkt. Deze precisering omschrijft op vrij voorzienbare wijze de gegevens die mogen worden verwerkt[70]. De Autoriteit heeft immers begrepen dat de verkeersgegevens die voor deze doeleinden nodig zijn kunnen variëren naargelang de omstandigheden en de operatoren moeten in dit verband een zekere marge hebben. Bovendien blijkt uit artikel 122 § 2 van de telecomwet dat de betrokken personen voorafgaand aan de verwerking in kennis moeten worden gesteld van de gegevens die op grond van deze bepaling zullen worden verwerkt. Zo gezien oordeelt de Autoriteit dat artikel 122 § 2 van de telecomwet voldoende duidelijk maakt welke categorieën van gegevens mogen worden verwerkt.

56. Artikel 122 § 2 van de telecomwet, dat de **criteria geeft op basis waarvan de maximale bewaarduur wordt bepaald**[71], **voldoet aan de eis van artikel 5.1.e) van de AVG**.

3) Bewaring van de gegevens voor de marketing van de eigen elektronische communicatiediensten en het opstellen van het gebruikspatroon of voor diensten met verkeers- of locatiegegevens (nieuw artikel 122 § 3 van de telecomwet)

57. **Artikel 122 § 3 van de telecomwet**, dat artikel 6.3 van de ePrivacyrichtlijn omzet, laat de operatoren toe om de verkeersgegevens te verwerken en te bewaren (inclusief de locatiegegevens verbonden aan een communicatie) die nodig zijn om (i) de **marketing** te verzorgen van de eigen elektronische communicatiediensten en (ii) het **gebruikspatroon** op te stellen van de abonnee of de eindgebruiker, **op voorwaarde dat** de abonnee of, in voorkomend geval, de eindgebruiker daarvoor zijn **toestemming heeft gegeven**.

58. **De wijzigingen die het voorontwerp van wet aanbrengt, hebben betrekking op de definitie van "toestemming"**. In de definitie van dat begrip wordt voortaan verwezen naar artikel 4 van de AVG (nieuw artikel 122 § 3, 2°, tweede lid van de telecomwet). Volgens het voorontwerp moeten de abonnees of eindgebruikers de mogelijkheid krijgen om de gegeven toestemming makkelijk en te allen tijde in te trekken (nieuw artikel 122 § 3, 3°). **De Autoriteit neemt nota van deze wijzigingen** die het gevolg zijn van de inwerkingtreding van de AVG.

[70] De Autoriteit benadrukt dat de operatoren, die de verwerkingsverantwoordelijken zijn, het beginsel van 'minimale gegevensverwerking' moeten eerbiedigen (artikel 5.1.c) van de AVG). Als een abonnee een abonnement heeft met onbeperkte oproepen lijkt het - op het eerste gezicht - niet nodig om de verkeersgegevens te bewaren voor het tellen van het aantal of de duur van de gemaakte uitgaande oproepen.
[71] De Autoriteit stelt bovendien vast dat de door de Belgische wetgever weerhouden criteria rechtstreeks zijn ontleend aan de ePrivacyrichtlijn.

59. Daarnaast **vervangt** het voorontwerp **de verwijzing naar de wet van 8 december 1992** tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens **door een verwijzing naar de AVG en naar de WVG**. De Autoriteit **neemt daar nota van**.

4) Bewaring van de gegevens voor het opsporen en analyseren van een vermoed geval van fraude of kwaadwillig gebruik van een elektronisch communicatienetwerk, inclusief de herkomst ervan (nieuw artikel 122 § 4 van de telecomwet)

60. Het nieuwe artikel 122 § 4 van de telecomwet legt de operatoren de **verplichting op om de locatiegegevens en andere verkeersgegevens die daartoe nodig zijn te bewaren** om **een vermoed geval van fraude** of **van kwaadwillig gebruik** van het elektronische communicatienetwerk op te sporen en te analyseren.

61. Het begrip "fraude" wordt door het nieuwe artikel 122 § 4, eerste lid van de telecomwet als volgt gedefinieerd: *"een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of het contract en om zichzelf of iemand anders een ongeoorloofd voordeel te doen, via het gebruik van een elektronische-communicatiedienst*".

62. Het begrip "kwaadwillig gebruik van het netwerk" wordt door het nieuwe artikel 122 § 4, tweede lid van de telecomwet als volgt gedefinieerd: *"een gebruik van het netwerk teneinde zijn contactpersoon te ontrieven of schade te berokkenen".*

63. De memorie van toelichting geeft concrete voorbeelden van fraude of kwaadwillig gebruik van het netwerk. Er is bijvoorbeeld sprake van fraude als de eindgebruiker de algemene voorwaarden die hem aan de operator bindt niet naleeft, als een derde gebruik maakt van een elektronische communicatiedienst op naam van de abonnee buiten zijn medeweten, bij pesterijen via sms ('smishing'), bij pesterijen via het internet ('phishing') of wanneer een binnenkomende oproep de eindgebruiker misleidt over de oorsprong van deze oproep en hem daarbij nadeel berokkent (' spoofing)[72]. Kwaadwillig gebruik van het netwerk dekt bijvoorbeeld pesterijen via de telefoon[73].

64. Het nieuwe artikel 122 § 4 van de telecomwet creëert **een nieuwe juridische verplichting** voor de operatoren om de locatiegegevens en andere verkeersgegevens te bewaren en in voorkomend geval te verwerken als dat nodig is om een vermoed geval van fraude of van kwaadwillig gebruik van het elektronische communicatienetwerk op te sporen en te analyseren. **De gegevensverwerkingen die de operatoren verrichten op grond van deze bepaling zijn dus "*noodzakelijk om te voldoen***

[72] Memorie van toelichting, p. 16.
[73] Memorie van toelichting, p. 16.

aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust" (artikel 6.1.c) van de AVG).

65. Opdat die gegevensverwerkingen wettig zouden zijn, moet, zoals wordt benadrukt door de Werkgroep "Artikel 29", de wet voldoen aan "*alle vereiste voorwaarden om de verplichting geldig en bindend te maken en in overeenstemming zijn met het toepasbaar recht inzake gegevensbescherming, met name met de noodzaak-, evenredigheids- en doelbindingsbeginselen*"[74]. Met andere woorden, "***de verwerkingsverantwoordelijke mag niet kiezen of hij zich al dan niet aan de verplichting zal houden"***[75]. De wettelijke verplichting moet **duidelijk en nauwkeurig** zijn zodat **de verwerkingsverantwoordelijke geen beoordelingsmarge** heeft over de manier waarop de persoonsgegevens nodig voor de naleving van zijn wettelijke verplichting worden verwerkt[76].

66. Het nieuwe artikel 122 § 4 van de telecomwet **bepaalt de doeleinden van de nieuwe gegevensverwerkingen die het oplegt**: het opsporen en analyseren van een vermoed geval van fraude of kwaadwillig gebruik van een elektronisch communicatienetwerk, inclusief de herkomst ervan. De Autoriteit stelt vast dat **deze doeleinden** voldoen aan de eis van artikel 5.1.b) van de AVG: "***welbepaald, uitdrukkelijk omschreven en gerechtvaardigd"***. Bovendien erkent de Autoriteit dat deze doeleinden kunnen **beantwoorden aan een van de doelstellingen die zijn aangegeven in artikel 15 § 1 van de ePrivacyrichtlijn**, in het bijzonder het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten en/of bescherming van de betrokken persoon of van de rechten en vrijheden van anderen[77]. **Het volstaat evenwel niet dat de doelstellingen** van het nieuwe artikel 122 § 4 van de telecomwet **gerechtvaardigd zijn opdat de opgelegde bewaarplicht toelaatbaar zou zijn**. Bovendien **moet deze verplichting "strikt"[78] noodzakelijk zijn voor en evenredig met deze doelstellingen**.

67. De Autoriteit stelt in dat verband vast dat het nieuwe artikel 122 § 4 van de telecomwet **de operatoren de verplichting oplegt om systematisch** locatie- en andere verkeersgegevens **te bewaren van**

[74] Werkgroep "Artikel 29", Advies *06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in de zin van artikel 7 van de Richtlijn 95/46/EG*, p. 21.
[75] Werkgroep "Artikel 29", Advies *06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke' in de zin van artikel 7 van de Richtlijn 95/46/EG*, p. 21.
[76] Werkgroep "Artikel 29", Advies *06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in de zin van artikel 7 van de Richtlijn 95/46/EG*, p. 22.
[77] Artikel 15 § 1 van de ePrivacyrichtlijn somt verschillende doelstellingen van algemeen belang op die een beperking van de rechten en plichten rechtvaardigen die zijn bedoeld in de artikelen 5, 6 en 9 van deze Richtlijn. Aan het einde van deze opsomming verwijst ze naar artikel 13 § 1 van de Richtlijn 95/46, dat de toegelaten doelstellingen bepaalt van een wettelijke maatregel die de reikwijdte van de in Richtlijn 95/46 vastgestelde rechten en plichten wil beperken. Die Richtlijn werd ingetrokken door artikel 94 van de AVG dat bovendien als volgt stelt: "*Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar deze verordening*". Bijgevolg moet de verwijzing naar artikel 13 van Richtlijn 95/46 worden gelezen als een verwijzing naar artikel 23 van de AVG. Volgens artikel 23 van de AVG mag een wetgevende maatregel de reikwijdte van de rechten en plichten die in de AVG zijn voorzien beperken op voorwaarde dat *"die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van […] de bescherming van de betrokkene of van de rechten en vrijheden van anderen"*.
[78] Zie considerans 11 van de ePrivacyrichtlijn.

alle gebruikers van de elektronische communicatiemiddelen[79]. Deze bepaling vormt een **bijzonder ernstige inmenging** in de privacyrechten en in het recht op bescherming van de persoonsgegevens. **Volgens het evenredigheidsbeginsel moet de doelstelling van algemeen belang die door de maatregel tot verplichte bewaring wordt nagestreefd evenredig zijn met de ernst van de inmenging die zij veroorzaakt.** Het HvJ-EU echter oordeelt als volgt: "*Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is*"[80]. **De Autoriteit heeft bijgevolg twijfels over de proportionaliteit van de verplichting opgelegd in artikel 122 § 4 van de telecomwet ten opzichte van de doelstellingen die zij nastreeft, terwijl deze doelstellingen weliswaar gerechtvaardigd zijn, maar op het eerste gezicht niet dezelfde graad van belangrijkheid lijken te hebben als de bestrijding van zware criminaliteit[81]**. De Autoriteit benadrukt bovendien dat het voorontwerp van wet bepaalt dat de verschillende autoriteiten die zijn geïdentificeerd in het nieuwe artikel 127/1 van de telecomwet– waaronder "*de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een*

[79] Na een verzoek om verdere inlichtingen betwist de afgevaardigde van de minister dat artikel 122 § 4 van de telecomwet een algemene en ongedifferentieerde bewaring van de locatie- en andere verkeersgegevens oplegt, met de volgende argumenten (de voetnoten werden weggelaten): *"In zijn arrest "La Quadrature du Net" heeft het Hof van Justitie van de Europese Unie (HvJ-EU) benadrukt dat een regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel'. Het wetsontwerp waarvoor het advies van de Gegevensbeschermingsautoriteit wordt gevraagd, maakt echter een onderscheid op basis van het beoogde doel omdat het voorziet in de bewaring van alleen de gegevens die noodzakelijk zijn voor elk van de doeleinden die zijn bedoeld in de paragrafen 2, 3 en 4 van artikel 122 […]*". De afgevaardigde van de aanvrager oordeelt dus dat de bewaarplicht niet algemeen en ongedifferentieerd is aangezien ze wordt opgelegd voor een welbepaald doel en enkel de gegevens moeten worden bewaard die noodzakelijk zijn om dat doel te bereiken. De Autoriteit kan met dat argument niet akkoord gaan. De passage die de aanvrager citeert kan niet los worden gezien van haar context en in het bijzonder van de zin die erop volgt, namelijk: *"Een dergelijke regeling betreft algemeen alle personen die gebruikmaken van elektronische communicatiediensten, zonder dat die personen zich – zelfs maar indirect – in een situatie bevinden die aanleiding kan zijn om strafvervolging in te stellen. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – verband houdt met die doelstelling van bestrijding van zware misdrijven, en vereist met name niet dat er een verband is tussen de te bewaren gegevens en een bedreiging voor de openbare veiligheid."* Uit de globale lezing van § 143 van het arrest " Quadrature du Net" kan niet worden afgeleid dat het een bewaring van de verkeers- en locatiegegevens van alle gebruikers van een elektronisch communicatiemiddel toelaat als die verplichting een welbepaald doel nastreeft en enkel betrekking heeft op de verkeersgegevens die nodig zijn om dat doel te bereiken. Als dat het standpunt van het Hof zou zijn geweest, zou het geen gerichte bewaring van de verkeers- en locatiegegevens voor de bestrijding van zware criminaliteit hebben geëist. Paragraaf 143 van het arrest van 6 oktober benadrukt dat er een verband moet bestaan - zelfs indirect of van ver - tussen de personen van wie de gegevens worden bewaard en het doel dat met de bewaarplicht wordt nagestreefd. De verplichting opgelegd in artikel 122 § 4 van de telecomwet betreft de verkeers- en locatiegegevens van alle gebruikers van elektronische communicatiemiddelen zonder dat wordt vereist dat er een verband bestaat, zelfs indirect of van ver, met de doelstelling van bestrijding van fraude of kwaadwillig gebruik van het netwerk. Uiteraard kan iedere persoon potentieel 'fraude' plegen of 'kwaadwillig gebruik' maken van het netwerk of er het slachtoffer van zijn, maar die mogelijkheid - die ook bestaat voor ernstige misdrijven waarvan de bestrijding het doel was van de regeling waarop het arrest van het HvJ-EU betrekking had - mag volgens de rechtspraak van het HvJ-EU niet voldoende worden geacht om een systematische preventieve bewaring te rechtvaardigen van de verkeersgegevens van alle gebruikers van een elektronisch communicatiemiddel die nodig zijn voor de bestrijding van fraude en kwaadwillig gebruik van het netwerk.

[80] HvJ-EU, arrest van 6 oktober 2020, § 141.

[81] Na een verzoek om verdere inlichtingen lijkt de afgevaardigde van de minister zelf toe te geven dat de doelstelling van bestrijding van fraude en kwaadwillig gebruik van het netwerk niet dezelfde graad van ernst heeft als de bestrijding van zware criminaliteit. Hij schrijft immers: "*Artikel 127/1 sluit ten volle aan bij deze Europese rechtspraak aangezien het evenredigheidsbeginsel in concreto wordt gerespecteerd: als de bewaring van de gegevens oorspronkelijk gerechtvaardigd is om bijvoorbeeld fraude te bestrijden of de veiligheid van de netwerken te beschermen, kunnen diezelfde gegevens a fortiori later worden verwerkt voor ernstiger doeleinden, namelijk in het kader van zware criminaliteit en ernstige bedreiging van de openbare veiligheid*" (woorden onderlijnd door de Autoriteit).

administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronische-communicatienetwerk, zoals de inbreuken die online worden gepleegd" – toegang kunnen krijgen tot die gegevens[82]. De Autoriteit merkt op dat het voorontwerp van wet, door een nieuwe veralgemeende bewaarplicht voor verkeers- en locatiegegevens op te leggen met het oog op de bestrijding van fraude en kwaadwillig gebruik van het netwerk, en er tegelijkertijd voor te zorgen dat (onder meer) wetshandhavingsinstanties toegang hebben tot dergelijke gegevens, de facto leidt tot de herinvoering van een veralgemeende en ongedifferentieerde bewaarplicht voor dergelijke gegevens met het oog op de bestrijding van criminaliteit. Het HvJEU heeft echter geoordeeld dat een dergelijke bewaringsverplichting niet mag worden opgelegd, zelfs niet met het oog op de bestrijding van zware criminaliteit, waarvan hier geen sprake is.

68. De **Autoriteit vraagt zich ook af of een verplichting tot preventieve en systematische gegevensbewaring, zoals is voorzien in het nieuwe artikel 122 § 4 van de telecomwet, noodzakelijk is** om een vermoed geval van fraude of een vermoed geval van kwaadwillig gebruik van het elektronische communicatienetwerk op te sporen en te analyseren. **Kunnen die doelstellingen niet worden bereikt met maatregelen die niet zo'n zware inmenging in de rechten en vrijheden van de betrokken personen vormen?** Zou het bijvoorbeeld niet mogelijk zijn om tot de bewaring van de gegevens te verplichten voor het bestrijden van fraude en kwaadwillig gebruik als er aanwijzingen bestaan van die fraude of kwaadwillig gebruik van het netwerk?[83] De bewaring zou dan kunnen worden gericht op de personen die op de een of andere manier bij de fraude of het kwaadwillig gebruik van het netwerk kunnen betrokken zijn of die om andere redenen zouden kunnen bijdragen, via de bewaring van hun gegevens, tot de bestrijding van zware criminaliteit. Een dergelijke keuze zou voldoen aan de eis van "verandering van gezichtspunt" waarnaar wordt verwezen in het arrest van het Grondwettelijk Hof[84]: van een preventieve en algemene bewaring zou worden overgestapt op een reactieve en gerichte bewaring. De Autoriteit benadrukt dat de wetgever dient te rechtvaardigen dat de door hem gekozen maatregel om het beoogde doel te bereiken diegene is die de rechten en vrijheden van de betrokken personen het minst aantast.

69. **De Autoriteit verzoekt de wetgever bijgevolg om de maatregel die voorziet in de verplichting om de locatie- en andere verkeersgegevens te bewaren die nodig zijn om een vermoed geval van fraude of een vermoed geval van kwaadwillig gebruik van het netwerk op te sporen en te analyseren, strikt te beoordelen in het licht van de rechtspraak van het**

[82] Zoals blijkt uit een gecombineerde lezing van de nieuwe artikelen 122 § 7 en 127/1 van de telecomwet
[83] Een aanwijzing van kwaadwillig gebruik van het netwerk kan bijvoorbeeld een klacht zijn van een persoon die meent het slachtoffer te zijn van pesterijen. Pesterijen zijn per definitie een strafbaar feit dat in de tijd is gespreid en herhaaldelijk wordt gepleegd; door in het geval van een dergelijke klacht bewaarplicht te 'activeren', zou de persoon die zich schuldig maakt aan deze pesterijen waarschijnlijk kunnen worden geïdentificeerd. Een aanwijzing van fraude waarbij de algemene voorwaarden van de operator worden geschonden, kan aan het licht komen bij het onderzoek van de bewaarde gegevens voor facturatiedoeleinden.
[84] GwH, arrest van 21 april 2021, § B.18.

HvJ-EU en te rechtvaardigen waarom ze daadwerkelijk noodzakelijk is en evenredig met de beoogde doelen.

70. Behalve de fundamentele vragen die de Autoriteit zich stelt over de noodzaak en evenredigheid van de verplichting die wordt opgelegd door het nieuwe artikel 122 § 4 van de telecomwet **formuleert de Autoriteit enkele meer 'punctuele' opmerkingen over de voorzienbaarheid en evenredigheid van bepaalde nadere regels van deze verplichting**.

71. Eerst en vooral **stelt de Autoriteit vast dat deze bepaling niet nauwkeurig aangeeft welke gegevens moeten worden bewaard** om een vermoed geval van fraude of van kwaadwillig gebruik van het elektronische communicatienetwerk op te sporen en te analyseren. Ze stelt enkel als volgt: de operatoren *"bewaren de locatiegegevens en andere gegevens die daartoe nodig zijn"* en "*verwerken de noodzakelijke gegevens daartoe, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig* [nvdr: de verkeersgegevens nodig voor de facturering van de abonnees en het doen van interconnectiebetalingen]". Artikel 122 § 4 van de telecomwet **bevat een facultatieve machtiging voor de Koning** om te bepalen welke verkeersgegevens in toepassing van deze bepaling moeten worden bewaard en verwerkt. De Koning mag deze gegevens bepalen, maar moet niet[85].

72. De Autoriteit wijst erop dat **de regelgeving betreffende de gegevensverwerking moet bepalen welke gegevens moeten worden verwerkt**. Als de verwerking een aanzienlijke inmenging betekent in de rechten en vrijheden van de betrokken personen, zoals hier het geval is, **moet de wetgever minstens de categorieën van gegevens bepalen, aangezien de precieze gegevens die zullen worden verwerkt kunnen worden bepaald in een norm met verordenende waarde**. In deze kan worden erkend dat **het nieuwe artikel 122 § 4 van de telecomwet d**e **categorieën van te bewaren gegevens voldoende bepaalt,** namelijk "*de locatiegegevens en andere verkeersgegevens die nodig zijn [om een vermoed geval van fraude of kwaadwillig gebruik van een elektronische communicatienetwerk op te sporen en te analyseren, inclusief de herkomst ervan]*". **De verdere bepaling van deze gegevens kan worden gedelegeerd aan de Koning, maar dan is vereist dat de Koning inderdaad tussenkomt**. Zijn tussenkomst mag niet facultatief zijn. Zolang de regelgeving geen nadere bepaling van de te bewaren gegevens omvat, **wordt niet voldaan aan de eis van voorzienbaarheid**. Dat geldt des te meer omdat de begrippen "fraude" en "kwaadwillig gebruik van het netwerk" vrij ruim zijn gedefinieerd. Zo gezien is het voor de betrokken personen moeilijk om te weten welke gegevens precies zullen worden

[85] De memorie van toelichting rechtvaardigt het facultatieve karakter van deze machtiging als volgt: "*De aanneming van dit koninklijk besluit is niet verplicht in het licht van de volgende uitdagingen. Ten eerste evolueert fraude aanzienlijk mettertijd. Bepaalde vormen van fraude kunnen verdwijnen of minder belangrijk worden terwijl nieuwe soorten van fraude kunnen opduiken. Vervolgens kunnen de gegevens die de operatoren bewaren om fraude tegen te gaan, verschillen afhankelijk van het type van de verstrekte elektronische-communicatiedienst, de omvang van de operator en de "antifraudetools" waarover hij beschikt of het soort van gebruikers van de dienst.*"

bewaard in toepassing van deze bepaling. **Als de verwerking nodig is om te voldoen aan een wettelijke verplichting**, zoals hier het geval is, moeten – zoals al eerder aangehaald door de Autoriteit – **alle factoren die de reikwijdte van deze verplichting duidelijk maken worden bepaald door de norm die deze verplichting oplegt**, zoniet kan het bindende karakter van deze verplichting in vraag worden gesteld. Voorts, en in ieder geval, benadrukt de Autoriteit dat de bewaring van verkeersgegevens geen specifieke url van de door de betrokkenen bezochte webpagina's mag bevatten of het mogelijk maken die url's af te leiden.

73. Vervolgens stelt de Autoriteit vast dat het nieuwe artikel 122 § 4 van de telecomwet de operatoren de volgende verplichting oplegt om "de locatiegegevens en andere verkeersgegevens gedurende de tijd die ervoor nodig is en minstens vier maanden" te bewaren[86], met uitzondering van **de verkeersgegevens in verband met de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten die gedurende 12 maanden moeten worden bewaard**. De Autoriteit begrijpt dat de mogelijkheid om locatiegegevens en andere verkeersgegevens langer dan de minimumtermijn van vier maanden te bewaren, bedoeld is voor de situatie waarin een langere bewaringstermijn nodig is om geschillen in verband met fraude of kwaadwillig gebruik van het netwerk te beheren. Deze verduidelijking moet aan het voorontwerp van wet worden toegevoegd.

5) Bewaring van de gegevens die nodig zijn om de veiligheid en de correcte werking van de netwerken en diensten voor elektronische communicatiete garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren (nieuw artikel 122 § 4/1 van de telecomwet)

[86] Na een verzoek om verdere inlichtingen heeft de afgevaardigde minister de keuze voor deze minimumduur van 4 maanden als volgt gerechtvaardigd: "*Zoals aangegeven in de memorie van toelichting werd de minimumduur van 4 maanden weerhouden voor de bestrijding van fraude en kwaadwillig gebruik van het netwerk, aangezien de fraude een impact kan hebben op de facturering van de abonnee door de operator (of door een onderneming). Dat is bijvoorbeeld het geval als een derde een elektronische communicatiedienst gebruikt in naam van de abonnee, zonder dat die daarvan op de hoogte is. In dat geval is de fraudepleger een derde en de eindgebruiker het slachtoffer aan wie de operator communicaties factureert die hij niet heeft gewenst. Bij de bepaling van de minimale bewaarduur van 4 maanden werd rekening gehouden met een volledige facturatiecyclus (eerste maand na het gebruik van de dienst), een minimale periode van betwisting (15 dagen tot 1 maand, de tweede maand na het gebruik van de dienst), een periode van verwerking van de betwisting waarin uitwisselingen kunnen plaatsvinden tussen de abonnee en de operator (de derde maand na de betwisting van de dienst) en een mogelijke periode van vertraging in de verwerking (de vierde maand na het gebruik van de dienst). Het gaat bijgevolg om een raming van de nodige bewaarduur van de gegevens die, in de meeste gevallen, nodig zijn voor de bestrijding van fraude en kwaadwillig gebruik van het netwerk. Evenwel zijn die 4 maanden op zich geen maximale bewaarduur. Elke operator kan voor zichzelf een langere bewaarduur bepalen, rekening houdend met de bijzonderheden en de specifieke noodwendigheden. De nodige bewaarduur kan immers afhangen van tal van factoren die eigen zijn aan elke operator en waarin hij een zekere vrijheid moet kunnen behouden, bijvoorbeeld in de graad van bescherming tegen fraude die hij zijn klanten wil verstrekken (en de eventuele bijkomende diensten in dit verband), de methodologie die hij gebruikt en de middelen die hij toekent aan de opsporing van fraude en kwaadwillig gebruik van het netwerk*".

74. Het **nieuwe artikel 122 § 4/1** van de telecomwet **legt de operatoren de verplichting op** om **de verkeersgegevens te bewaren** en te **verwerken** die nodig zijn om de **veiligheid en de goede werking van hun netwerken en diensten voor elektronische communicatie te garanderen**, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

75. Het nieuwe artikel 122 § 4/1 van de telecomwet creëert dus **een nieuwe juridische verplichting voor de operatoren om verkeersgegevens te bewaren en te verwerken** teneinde de veiligheid en de goede werking van hun netwerken en diensten voor elektronische communicatie te garanderen. Die verwerkingen hebben een rechtsgrond in de zin van artikel 6 van de AVG, want ze zijn "*noodzakelijk voor de uitvoering van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust*" (artikel 6.1.c) van de AVG). Zoals al eerder gesteld door de Autoriteit, moet de norm die de wettelijke verplichting oplegt **voldoende duidelijk en nauwkeurig** zijn opdat de verwerkingsverantwoordelijke geen beoordelingsmarge zou hebben over de manier waarop hij zijn verplichting moet nakomen[87].

76. Het nieuwe artikel 122 § 4/1 van de telecomwet **bepaalt het doel van de nieuwe gegevensverwerkingen die het oplegt**: "om de veiligheid en de correcte werking van hun netwerken en diensten voor elektronische communicatie te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren". De Autoriteit stelt vast dat **dit doel voldoet aan de eis van artikel 5.1.b) van de AVG**. Bovendien erkent de Autoriteit dat dit doel is opgenomen in de lijst van de **doelstellingen** die **overeenkomstig artikel 15 § 1 van de ePrivacyrichtlijn** een beperking kunnen rechtvaardigen van de reikwijdte van de verplichting om het vertrouwelijke karakter van de verkeersgegevens te garanderen. In dit geval gaat het om "*het voorkomen, onderzoeken, opsporen of vervolgen van onbevoegd gebruik van het elektronisch communicatiesysteem*" [88] en/of de bescherming van de "openbare veiligheid"[89].

77. Zoals reeds gezegd **volstaat het niet dat de verplichting tot gegevensbewaring een rechtmatig doel beoogt, ze moet ook "strikt"[90] noodzakelijk zijn en strikt evenredig met dat doel.**

---

[87] Werkgroep "Artikel 29", Advies *06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in de zin van artikel 7 van de Richtlijn 95/46/EG*, p. 22.
[88] Het HvJ-EU oordeelt als volgt: "Verder heeft de uitzondering betreffende het onbevoegde gebruik van het elektronische communicatiesysteem […] kennelijk betrekking op vormen van gebruik die de goede werking of de veiligheid zelf van het systeem aantasten" (HvJ-EU, arrest van 29 januari 2008, zaak C-275/06, "Promiscuae")
[89] Volgens de memorie van toelichting "*is netwerkveiligheid, wat onder staatsveiligheid valt, essentieel voor de maatschappij in haar geheel. Een incident op het netwerk van een operator kan erg schadelijke gevolgen hebben op tal van niveaus (diefstal of verlies van gegevens, impact op de diensten die worden aangeboden via het netwerk). Het belang van netwerkveiligheid zal toenemen in de toekomst met de ontwikkeling van 5G, waarvan tal van diensten en applicaties zullen afhangen.*
[90] Zie considerans 11 van de ePrivacyrichtlijn.

78. De Autoriteit stelt in dat verband vast dat het nieuwe artikel 122 § 4/1 van de telecomwet – evenals het nieuwe artikel 122 § 4 van de telecomwet waarover de Autoriteit zich al heeft uitgesproken – **de operatoren de verplichting oplegt om systematisch de verkeersgegevens te bewaren van alle gebruikers van de elektronische communicatiemiddelen**. Die nieuwe verplichting tot preventieve en algemene bewaring vormt **een bijzonder ernstige inmenging** in de rechten en vrijheden van de betrokken personen. De Autoriteit herhaalt, zoals reeds eerder, dat krachtens het voorzienbaarheidsbeginsel een ernstige inmenging in de rechten en vrijheden van de betrokken personen enkel kan worden gerechtvaardigd door een doelstelling van algemeen belang die belangrijk genoeg is. Zoals de Autoriteit echter al heeft benadrukt, oordeelt het HvJ-EU als volgt: "*Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is*"[91]. **De Autoriteit heeft derhalve twijfels over de evenredigheid van de verplichting van artikel 122 §4/1 van de Telecomwet, aangezien het doel dat met deze nieuwe verplichting tot het bewaren van gegevens wordt nagestreefd, weliswaar legitiem is, maar op het eerste gezicht niet van hetzelfde belang lijkt te zijn als de bestrijding van zware criminaliteit.**. De Autoriteit benadrukt bovendien dat het voorontwerp van wet bepaalt dat de verschillende autoriteiten die zijn geïdentificeerd in het nieuwe artikel 127/1 van de telecomwet– waaronder "*de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronische-communicatienetwerk, zoals de inbreuken die online worden gepleegd*" – toegang kunnen krijgen tot die gegevens[92]. Deze mogelijkheid om onder meer rechtshandhavingsinstanties toegang te geven tot alle gegevens die telecombedrijven bewaren om te voldoen aan de verplichting die hun bij artikel 122 §4/1 van de telecomwet is opgelegd, versterkt de twijfels van de Autoriteit over de evenredigheid van deze bewaringsverplichting.

79. De **Autoriteit vraagt zich ook af of een verplichting tot preventieve en systematische gegevensbewaring, zoals is voorzien in het nieuwe artikel 122 § 4/1 van de telecomwet, noodzakelijk is** om de veiligheid en de goede werking van de netwerken en diensten voor elektronische communicatie. De operatoren moeten uiteraard verkeersgegevens kunnen verwerken en bewaren wanner dat nodig is om de veiligheid van het netwerk en van hun diensten te garanderen. **Maar de Autoriteit vraagt zich af of hen daarvoor een bewaarplicht moet worden opgelegd**. Vandaag zijn de operatoren verplicht tot het nemen van "*de passende technische en organisatorische maatregelen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen, eventueel samen wat de veiligheid van het netwerk betreft. Deze maatregelen zorgen, gezien de stand*

[91] HvJ-EU, arrest van 6 oktober 2020, § 141.
[92] Zoals blijkt uit een gecombineerde lezing van de nieuwe artikelen 122 § 7 en 127/1 van de telecomwet

*van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen. Er worden met name maatregelen genomen om de impact van veiligheidsincidenten op gebruikers en onderling verbonden netwerken zo laag mogelijk te houden" (*artikel 114 § 1 van de telecomwet[93]). Ze hebben ook de mogelijkheid om, *"met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische-communicatiedienst te garanderen*", met opzet de personen te identificeren die die bij de overzending van de informatie en de inhoud ervan betrokken zijn en om met opzet kennis te nemen van gegevens inzake elektronische communicatie (artikelen 124 en 125 van de telecomwet). Als de correcte werking van het netwerk en de goede uitvoering van een elektronische communicatiedienst dit vereisen, mogen de operatoren de verkeersgegevens verwerken met dat doel. **Door de mogelijkheid om die gegevens te verwerken om te zetten in een verplichting om ze te bewaren, creëert het voorontwerp een grotere inmenging in de rechten en vrijheden van de betrokken personen, met name met betrekking tot diensten die dergelijke gegevens momenteel niet verzamelen en bewaren om privacy- en veiligheidsredenen. Die grotere inmenging moet strikt gerechtvaardigd worden.** De memorie van toelichting en de bijkomende informatie die werd verstrekt door de afgevaardigde van de minister rechtvaardigen waarom de operatoren verkeersgegevens moeten kunnen verwerken om de veiligheid van het netwerk en de correcte werking van hun diensten te garanderen. **De reden waarom een mogelijkheid werd omgezet in een verplichting is echter niet voldoende toegelicht en gestaafd in de memorie van toelichting.**

80. **De Autoriteit verzoekt de wetgever om de maatregel die voorziet in de verplichting om de verkeersgegevens te bewaren die nodig zijn om de veiligheid en de correcte werking van de netwerken en diensten voor elektronische communicatie te garanderen strikt te beoordelen in het licht van de rechtspraak van het HvJ-EU en te rechtvaardigen waarom ze daadwerkelijk noodzakelijk is en evenredig met de beoogde doelen**.

81. Behalve de fundamentele vragen die de Autoriteit zich stelt over de noodzaak en evenredigheid van de verplichting die wordt opgelegd door het nieuwe artikel 122 § 4/1 van de telecomwet, **formuleert de Autoriteit enkele meer 'punctuele' opmerkingen over de voorzienbaarheid en evenredigheid van bepaalde nadere regels van deze verplichting**.

82. De Autoriteit wijst erop dat **de verwerkte gegevens, krachtens de eis van voorzienbaarheid, moeten worden bepaald** door de regelgeving betreffende de gegevensverwerking, in het bijzonder wanneer de inmenging bijzonder groot is, zoals in dit geval. Artikel 122 § 4/1 van de telecomwet **identificeert de categorie van gegevens[94]** die de operatoren moeten bewaren, maar **niet de**

[93] Deze bepaling voorziet in de omzetting van artikel 4 van de ePrivacyrichtlijn.
[94] Het betreft de "*de verkeersgegevens die nodig zijn om de veiligheid en correcte werking van hun netwerken en diensten voor elektronische communicatie te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren."*

precieze gegevens die moeten worden bewaard. Het machtigt de Koning ook niet om die gegevens te bepalen. **Er wordt dus niet voldaan aan de eis van voorzienbaarheid**. Het voorontwerp moet **hetzij zelf bepalen** welke precieze gegevens moeten worden bewaard, **hetzij de Koning machtigen** om die gegevens te bepalen[95]. De Autoriteit benadrukt in ieder geval dat de bewaring van verkeersgegevens niet de specifieke url van de door de betrokken personen bezochte webpagina's mag bevatten of het mogelijk mag maken die url af te leiden.

83. Vervolgens stelt de Autoriteit vast dat het nieuwe artikel 122 § 4/1 van de telecomwet **een bewaarduur oplegt van 12 maanden,** maar de operatoren "*kunnen ze **voor een langere duur bewaren die beperkt is tot het strikt noodzakelijke**"*. De Autoriteit formuleert daarover **twee opmerkingen**.

(i) **Ten eerste**, stelt de Autoriteit **zich vragen over de evenredigheid van de bewaarduur van 12 maanden**. De Autoriteit vraagt zich meer bepaald af of het niet kan volstaan om de gegevens gedurende een kortere termijn te bewaren en om die termijn enkel te verlengen als de operator vaststelt dat de veiligheid of de correcte werking van het netwerk of de diensten voor communicatie in gevaar komt. **De Autoriteit verzoekt de wetgever om aan de hand van concrete factoren te beoordelen of en, in voorkomend geval, te rechtvaardigen waarom een bewaarduur van 12 maanden aangewezen is**. De wetgever moet daarbij rekening houden met het feit dat de operatoren overeenkomstig de telecomwet bij machte moeten zijn om een aanslag op de veiligheid van de aangeboden netwerken of diensten snel op te sporen.

(ii) **Ten tweede** stelt de Autoriteit vast dat de wetgever wil voorzien in de mogelijkheid om de bewaarduur van 12 maanden nog te verlengen als dat strikt noodzakelijk is. De Autoriteit heeft begrepen dat die mogelijkheid betrekking heeft op een situatie waarin een langere bewaarduur voor verkeers- en locatiegegevens nodig is om een geschil betreffende een aanslag op de veiligheid van het netwerk of de goede werking van de dienst te beheren, met dien verstande dat alleen de gegevens die nodig zijn voor het beheer van het geschil gedurende een langere periode mogen worden bewaard. **Die precisering moet worden toegevoegd aan het voorontwerp.**

6) Bewaring van de gegevens om te voldoen aan een wettelijke verplichting (nieuw artikel 122 § 4/2 van de telecomwet)

[95] Zoals de Autoriteit al heeft benadrukt wordt die eis van nauwkeurigheid ook opgelegd door het feit dat de bewaring van die gegevens steunt op "een wettelijke verplichting" (in de zin van artikel 6.1.c) van de AVG). Zo gezien moeten alle factoren die de reikwijdte van deze verplichting duidelijk maken - dus ook de te bewaren gegevens worden bepaald door de norm die deze verplichting oplegt, zoniet kan het bindende karakter van deze verplichting in vraag worden gesteld.

84. Het **nieuwe artikel 122 § 4/2** van de telecomwet **legt de operatoren de verplichting op** om de **verkeersgegevens** die nodig zijn om **te voldoen aan een wettelijke verplichting** die op hen rust te **bewaren** en te **verwerken** voor de daartoe benodigde duur.

85. **Het voorontwerp moet preciseren dat deze wettelijke verplichting enkel kan worden opgelegd door een formele wetgevende norm**. Gezien de ernst van de inmenging veroorzaakt door de bewaring van verkeersgegevens moet elke verplichte gegevensbewaring worden opgelegd door een formele wetgevende norm die er op voorzienbare wijze alle essentiële factoren van bepaalt. Voor zover nodig benadrukt de Autoriteit nog dat ook deze wetgevende norm moet voldoen aan de beginselen van noodzaak en evenredigheid zoals die worden geïnterpreteerd door het HvJ-EU.

7) Bewaring van andere locatiegegevens dan verkeersgegevens (nieuw artikel 123 van de telecomwet)

86. Volgens het nieuwe artikel 123 § 1 van de telecomwet **mogen** de **operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens** verwerken en bewaren in de volgende gevallen:

- Wanneer **dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst**, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is;

- Wanneer dat **noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren**, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is;

- Wanneer **de gegevens anoniem gemaakt zijn**;

- Wanneer **de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens** en de abonnee of, in voorkomend geval, de eindgebruiker **zijn toestemming heeft gegeven**;

- Wanneer de **verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting** in hoofde van de operator.

87. Hoewel de memorie van toelichting aangeeft dat artikel 123 van de telecomwet voorziet in een omzetting van artikel 9 van de ePrivacyrichtlijn, **stelt de Autoriteit vast dat deze bepaling voorziet in meer situaties waarin de bewaring van andere locatiegegevens dan**

verkeersgegevens is toegestaan dan artikel 9 van de ePrivacyrichtlijn. Volgens artikel 9 van de ePrivacyrichtlijn is een verwerking van andere locatiegegevens dan verkeersgegevens enkel toegestaan wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. Artikel 9 van de ePrivacyrichtlijn voorziet niet in de verwerking en bewaring van andere locatiegegevens dan verkeersgegevens die nodig zijn voor de correcte werking en de veiligheid van het netwerk of de dienst, om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren of om te voldoen aan een wettelijke verplichting in hoofde van de operator. Artikel 15 § 1 van de ePrivacyrichtlijn daarentegen stelt als volgt: "[*D]e lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in […] artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid of het voorkomen, onderzoeken, opsporen van strafbare feiten of onbevoegd gebruik van het elektronische communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd."* **De Belgische wetgever mag dus de verwerking en bewaring van andere locatiegegevens dan verkeersgegevens toelaten in andere situaties dan deze die zijn voorzien in artikel 9 van de ePrivacyrichtlijn**, **op voorwaarde** dat die verwerkingen **"noodzakelijk" en "evenredig" zijn** met de beoogde doelen **en dat de wettelijke bepaling die ze toelaat voldoende voorzienbaar is** voor de betrokken personen.

88. De Autoriteit stelt in dit verband vast **dat de memorie van toelichting noch de noodzaak noch de evenredigheid rechtvaardigt** van de verwerking van andere locatiegegevens dan verkeersgegevens om **de correcte werking en de veiligheid van het netwerk of de dienst te garanderen** of om **fraude of kwaadwillig gebruik van het netwerk**[96]**op te sporen of te analyseren**. Bijgevolg verzoekt de Autoriteit **de wetgever om de noodzaak en evenredigheid van deze verwerking strikt te beoordelen en, in voorkomend geval, te rechtvaardigen aan de hand van concrete factoren**. Bovendien moet het voorontwerp, **om te voldoen aan de eis van voorzienbaarheid**, worden herzien om minstens de **voorwaarden te bepalen onder welke de operatoren deze gegevens mogen bewaren en verwerken,** evenals **de maximale bewaarduur** van deze gegevens.

89. Aangaande de verwerking van andere locatiegegevens dan verkeersgegevens **nodig om te voldoen aan een wettelijke verplichting in hoofde van de operator**, benadrukt de Autoriteit dat het **voorontwerp moet preciseren –** gezien de ernst van de inmenging veroorzaakt door de bewaring

[96] Aangaande de doelstellingen van deze gegevensverwerking heeft de Autoriteit al benadrukt dat zij voldoen aan de eis van artikel 5.1.b) van de AVG en waren opgenomen in de lijst van de doelstellingen van artikel 15 § 1 van de ePrivacyrichtlijn.

van locatiegegevens – **dat die wettelijke verplichting enkel kan worden opgelegd door een formele wetgevende norm**. Voor zover nodig benadrukt de Autoriteit nog dat ook deze wetgevende norm moet voldoen aan de beginselen van noodzaak en evenredigheid zoals die worden geïnterpreteerd door het HvJ-EU.

90. Ten slotte wijst de Autoriteit erop dat het zeer moeilijk is om locatiegegevens echt anoniem te maken wanneer zij op individueel niveau worden opgeslagen[97]. Operatoren die toegang hebben tot locatiegegevens die betrekking hebben op een geïdentificeerde natuurlijke persoon (en die dus nog niet zijn geanonimiseerd), kunnen deze informatie immers gemakkelijk gebruiken om via « profiling attacks »[98] de personen te identificeren op wie de geanonimiseerde locatiegegevens betrekking hebben

8) Bewaring van de abonnementsgegevens en de technische gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische communicatiedienst te identificeren (nieuw artikel 126 van de telecomwet) en van de identificatiegegevens van de abonnees (nieuw artikel 127 van de telecomwet)

91. Het nieuwe artikel 126 van de telecomwet **verplicht** de "*operatoren die aan de eindgebruikers elektronische-communicatiediensten bieden* " en de "*operatoren die de onderliggende elektronische-communicatienetwerken leveren"* om **de abonnementsgegevens** van de abonnee te **bewaren**, evenals de **technische gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische communicatiedienst te identificeren, voor zover deze operatoren dergelijke gegevens reeds verwerken of genereren in het kader van de aanbieding van de betrokken communicatienetwerken of -diensten.** Die gegevens, met uitzondering van de andere dynamische IP-adressen dan diegene die is gebruikt om in te tekenen op de dienst, moeten worden bewaard vanaf de datum waarop de dienst wordt geactiveerd en tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is. De andere dynamische IP-adressen dan diegene die is gebruikt om in te tekenen op de dienst worden van hun kant tot twaalf maanden na het einde van de sessie bewaard.

92. Volgens het nieuwe artikel 126 § 2 **bepaalt de Koning de te bewaren gegevens** alsook de vereisten waaraan deze gegevens moeten beantwoorden. **Het besluit van 19 september 2013** dat het voor advies aan de Autoriteit voorgelegde ontwerpbesluit wil wijzigen**, bepaalt de lijst van de gegevens die moeten worden bewaard** in uitvoering van artikel 126 van de telecomwet:

---

[97] Gegevens worden op individueel niveau bewaard wanneer de geregistreerde informatie aan een persoon gekoppeld is. Integendeel, informatie die op geaggregeerde wijze wordt geregistreerd, bevat alleen informatie die betrekking heeft op meerdere personen, bijvoorbeeld een percentage

[98]. Zie bijvoorbeeld, Naini, F.M., Unnikrishnan, J., Thiran, P. and Vetterli, M., 2015. "Where you are is who you are: User identification by matching statistics". *IEEE Transactions on Information Forensics and Security*, 11(2), blz.358-372

- De aanbieders van **openbare diensten voor vaste telefonie**, de nomadische diensten inbegrepen, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren de volgende gegevens:

  1° het aan de eindgebruiker toegewezen nummer;
  2° de persoonsgegevens van de eindgebruiker (die worden omschreven als "de naam en voornaam en het facturatie- en het leveringsadres van de eindgebruiker");
  3° de datum van aanvang van het abonnement of van de registratie voor de dienst;
  4° het soort van gebruikte vaste-telefoniedienst alsook de andere soorten van gebruikte diensten waarop de eindgebruiker ingeschreven heeft;
  5° in geval van overdracht van het nummer van de eindgebruiker naar een andere operator, de identiteit van de aanbieder die het nummer en de identiteit overdraagt van de aanbieder naar wie het nummer wordt overgedragen;
  6°de gegevens betreffende betalingswijze, identificatie van het betalingsmiddel en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst;
  7° het identificatienummer van het eindtoestel van de eindgebruiker, in voorkomend geval het "Media Access Control adres (MAC adres)" of "Permanent Equipment Identifier (PEI)".

- De aanbieders van een **openbare dienst voor mobiele telefonie**, de nomadische diensten inbegrepen, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren de volgende gegevens:

  1° het aan de eindgebruiker toegewezen nummer alsook de internationale identiteit van de mobiele abonnee ("International Mobile Subscriber Identity", "IMSI") of "Subscription Permanent Identifier (SUPI)";
  2° de persoonsgegevens van de eindgebruiker en de overeenstemmende "Subscription Concealed Identifier (SUCI)";
  3° de datum en de plaats van inschrijving op het abonnement of de registratie van de eindgebruiker;
  4° de datum en het tijdstip van de eerste activering van de dienst, alsook de celidentiteit van waaruit de dienst is geactiveerd;
  5° de aanvullende diensten waarop de eindgebruiker heeft ingetekend;
  6° in geval van nummeroverdracht naar een andere operator, de identiteit van de operator vanwaar de eindgebruiker komt;
  7° de gegevens betreffende betalingswijze, identificatie van het betalingsmiddel en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst;

8° het identificatienummer van het eindtoestel van de eindgebruiker ("International Mobile Equipment Identity", "IMEI", het "Media Access Control adres (MAC adres)" of "Permanent Equipment Identifier (PEI)".

- De aanbieders van openbare **internettoegangsdiensten** en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren de volgende gegevens:

  1° de toegewezen eindgebruikersidentificatie, in voorkomend geval inclusief de "Subscription Permanent Identifier (SUPI)";
  2° a) het IP-adres;
  b) in geval van het gedeelde gebruik van een IP-adres, de toegewezen poorten van het IP-adres alsook de datum en het uur van de toewijzing;
  3° de persoonsgegevens van de eindgebruiker, in voorkomend geval inclusief de overeenstemmende "Subscription Concealed Identifier (SUCI)";
  4° de datum en het tijdstip van het nemen van het abonnement of de registratie van de eindgebruiker;
  5° het IP-adres en de bronpoort van de verbinding die gediend hebben voor het nemen van het abonnement of voor de registratie van de eindgebruiker;
  6° de identificatie van het netwerkaansluitpunt dat gediend heeft voor het nemen van het abonnement of voor de inschrijving als eindgebruiker;
  7° de aanvullende diensten waarop de eindgebruiker ingeschreven heeft bij de betrokken aanbieder van openbare internettoegang;
  8° de gegevens betreffende betalingswijze, identificatie van het betalingsmiddel en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst;
  9° het identificatienummer van het eindtoestel van de eindgebruiker, in voorkomend geval het "Media Access Control adres (MAC adres)" of "Permanent Equipment Identifier (PEI)".

- De aanbieders van een **openbare e-maildienst via internet**, de aanbieders van een **openbare internettelefoniedienst** en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren de volgende gegevens:

  1° de toegewezen eindgebruikersidentificatie, in voorkomend geval inclusief de "Subscription Permanent Identifier (SUPI)";
  2° het IP-adres en de bronpoort die worden gebruikt door de eindgebruiker;

3° de persoonsgegevens van de eindgebruiker, in voorkomend geval inclusief de overeenstemmende "Subscription Concealed Identifier (SUCI)";
4° de datum en het tijdstip waarop de e-mail- of internettelefonieaccount is gecreëerd;
5° het IP-adres en de bronpoort die gediend hebben voor de creatie van de e-mail- of internettelefonieaccount;
6° de gegevens betreffende betalingswijze, identificatie van het betalingsmiddel en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst;
7° behalve voor de openbare e-maildienst via internet, het identificatienummer van het eindtoestel van de eindgebruiker, in voorkomend geval het "Media Access Control adres (MAC adres)" of "Permanent Equipment Identifier (PEI)".

93. Het nieuwe **artikel 127** van de telecomwet van zijn kant **legt de operatoren de verplichting op** om **hun abonnees te identificeren** of om de nodige gegevens te verzamelen en te bewaren, inclusief het rijksregisternummer in voorkomend geval, opdat de autoriteiten die gerechtigd zijn om deze identiteit te verkrijgen hen kunnen identificeren. Die gegevens moeten worden **bewaard tijdens de hele duur van activering** van de dienst **en tot twaalf maanden na de datum vanaf wanneer communicatie voor het laatst mogelijk is** aan de hand van de gebruikte dienst. **De Koning** is gemachtigd – maar niet verplicht – **om** onder meer **te bepalen welke identificatiegegevens** en -documenten door de operator moeten worden verzameld en bewaard.

94. De **in uitvoering van de artikelen 126 en 127** van de telecomwet **bewaarde gegevens worden bewaard voor de volgende autoriteiten en doeleinden**:

"*1°de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronische-communicatienetwerk, zoals de inbreuken die online worden gepleegd*
2° de inlichtingen- en veiligheidsdiensten teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;
3° de autoriteiten belast met het verlenen van hulp aan personen, inclusief de Ombudsdienst voor telecommunicatie wat betreft het kwaadwillig gebruik van het netwerk, de hulpdiensten en de Cel Vermiste Personen van de federale politie;
4° het Instituut in het kader van de uitvoering en controle van deze wet;
5° de autoriteiten bevoegd voor het onderzoek van een veiligheidsprobleem op het netwerk of van de dienst"[99].

[99] Nieuw artikel 127/1 van de telecomwet

95. Uit de rechtspraak van het Hof van Justitie blijkt dat **een wetgevende maatregel genomen in toepassing van artikel 15 van de ePrivacyrichtlijn de operatoren kan verplichten om de gegevens te bewaren die nodig zijn voor de identificatie van de gebruikers van een elektronische communicatiedienst** als die bewaring nodig is voor het bereiken van een van de doelstellingen die zijn opgesomd in artikel 15.1 van de ePrivacyrichtlijn.

96. Wat de **gegevens betreffende de burgerlijke identiteit van de abonnees betreft**, oordeelt het HvJ-EU dat de bewaring daarvan - gedurende een niet nader bepaalde periode - en de mededeling ervan met als enige doel de betrokken gebruiker te identificeren, kan worden gerechtvaardigd door het nastreven van een van de doelstellingen die zijn opgesomd in artikel 15 § 1 van de ePrivacyrichtlijn zonder dat dit doel van enig bijzonder belang moet zijn (zoals bijvoorbeeld de bestrijding van zware criminaliteit). **De bewaring van de gegevens betreffende de burgerlijke identiteit van de abonnees,** om hun identificatie mogelijk te maken, is volgens het Hof **geen ernstige inmenging** in de grondrechten van de betrokken personen.

97. Aangaande **de bewaring van het IP-adres van de abonnees** stelt het Hof zich strenger op. Dat gegeven, dat nodig is om de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd, maakt het ook mogelijk – gecombineerd met de IP-adressen van de ontvangers - om een volledig beeld te krijgen van het de online activiteit van de gebruiker en aan de hand daarvan een gedetailleerd profiel van de betrokkene op te stellen. Het Hof oordeelt dan ook **dat de algemene bewaring van de IP-adressen die aan de bron van een verbinding zijn toegewezen, een ernstige inmenging vormt** in de grondrechten van de internetgebruikers. Het erkent wel dat een dergelijke preventieve algemene bewaring noodzakelijk kan zijn aangezien in het geval van een online gepleegd strafbaar feit het IP-adres mogelijk het enige onderzoeksmiddel is met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Gezien de ernst van de inmenging meent het Hof dat **enkel een voldoende belangrijk doel, zoals de bestrijding van zware criminaliteit, een dergelijke maatregel tot algemene bewaring van IP-adressen kan rechtvaardigen**[100].

98. De Autoriteit neemt nota van het feit dat de wetgever de bewaring wil verplichten van de abonnements- en identificatiegegevens van de abonnees, en van de technische gegevens die noodzakelijk zijn voor de identificatie van die abonnees, van het gebruikte eindapparaat en de gebruikte elektronische communicatiedienst. **Een dergelijke gegevensbewaring kan onder bepaalde voorwaarden immers noodzakelijk zijn en evenredig met de beoogde doelen**.

[100] HvJ-EU, arrest van 6 oktober 2020, § 156.

99. De Autoriteit benadrukt echter dat het niveau van inmenging veroorzaakt door de bewaring van die gegevens varieert naargelang het soort gegevens die worden bewaard. De bewaring van **de gegevens die de tracering mogelijk maken van de activiteiten van de abonnees, vormen** een **ernstige inmenging** in de grondrechten van de betrokken personen, terwijl de bewering van de gegevens aan de hand waarvan de abonnees kunnen worden geïdentificeerd, zonder dat hun activiteit mag worden getraceerd, een inmenging in het privéleven is die niet als ernstig kan worden aangemerkt. De Autoriteit herhaalt dat het **evenredigheidsbeginsel eist dat de bewaring van de gegevens die een beeld geven van de activiteiten van de abonnees** voor andere doeleinden dan het traceren van de elektronische communicatie, **en het eventuele latere gebruik ervan** voor de redenen opgesomd in artikel 15 van de ePrivacyrichtlijn, **aan strengere voorwaarden worden onderworpen opdat de inmenging die ze creëert strikt evenredig zou blijven met de beoogde doelen.**

100. Wat de **IP-adressen** betreft die zijn toegewezen aan de bron van een communicatie oordeelt het Hof dat ze enkel mogen worden bewaard voor doelstellingen die voldoende belangrijk zijn, dat de bewaartermijn niet langer mag zijn dan strikt noodzakelijk is gelet op het nagestreefde doel en dat moet worden voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens[101]. **Het voorontwerp moet dus worden aangepast in die zin dat wordt voorzien dat IP-adressen die zijn toegewezen aan de bron van een communicatie enkel mogen worden bewaard om het bereiken van bijzonder belangrijke doelen mogelijk te maken**.

101. De Autoriteit merkt ook op dat noch het voorontwerp van wet noch het ontwerpbesluit specificeert dat alleen de IP-adressen die zijn toegewezen aan de bron van een communicatie moeten worden bewaard op grond van het nieuwe artikel 126 van de Telecomwet, met uitsluiting van de IP-adressen van de ontvanger van die communicatie. Het voorontwerp van wet en het ontwerp-besluit zullen worden herzien om deze verduidelijking toe te voegen.

102. Het voorontwerp van wet – en het ontwerpbesluit tot uitvoering ervan – **voorziet ook in de bewaring van de identificatienummers van de eindapparaten van de eindgebruikers.** Behoudens vergissing werd de bewaring van dit gegeven nog niet eerder geëist. De identificatienummers van de eindapparaten van de eindgebruikers zijn een unieke identificatie van de eindapparaten waarmee een apparaat kan worden 'getraceerd' via alle elektronische communicatiediensten die het gebruikt. **De preventieve en systematische bewaring van deze nummers vormt dus een ernstige inmenging in de privacyrechten en in het recht op bescherming van de persoonsgegevens**. Daarom moet de bewaring ervan **strikt noodzakelijk**

[101] HvJ-EU, arrest van 6 oktober 2020, § 156. Deze eisen hebben weliswaar betrekking op de algemene en ongedifferentieerde bewaring van de IP-adressen, en niet van alle technische gegevens aan de hand waarvan de abonnee of zijn eindapparatuur kan worden geïdentificeerd. Maar zoals de afgevaardigde van de minister in een antwoord op een verzoek om verdere inlichtingen zelf aangaf: *"Dezelfde redenering kan worden gevolgd voor andere technische gegevens die nodig zijn om de eindgebruiker, de einduitrusting en de gebruikte elektronische communicatiedienst te identificeren*".

en strikt evenredig zijn met de beoogde doelen. In dit opzicht kan de rechtspraak van het Hof van Luxemburg aangaande de algemene bewaring van de IP-adressen worden aangewend om te bepalen aan welke voorwaarden een wetgevende maatregel die verplicht tot de bewaring van die unieke identificatiegegevens van de eindapparaten van de abonnees moet voldoen. In een antwoord op een verzoek om verdere inlichtingen, benadrukt ook de afgevaardigde van de minister dat de redenering van het HvJ-EU aangaande de IP-adressen "*ook kan worden gevolgd voor andere technische gegevens die nodig zijn om de eindgebruiker, het eindapparaat en de gebruikte elektronische communicatiedienst te identificeren*"**. De bewaring van die gegevens zou dus enkel mogen worden opgelegd om een doel na te streven van bijzonder belang** (zoals de bestrijding van zware criminaliteit), **de bewaartermijn zou niet langer mogen zijn dan strikt noodzakelijk** is gelet op dat doel en er zou moeten worden voorzien in **strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens**[102]. **Aangezien het voorontwerp van wet en het ontwerpbesluit** niet aan die eisen voldoen, **moeten ze worden aangepast.**

103. Naast deze opmerkingen over het beginsel van de bewaarplicht betreffende de abonnements- en identificatiegegevens van de abonnees en van de technische gegevens aan de hand waarvan de abonnees, het gebruikte eindapparaat en de gebruikte elektronische communicatiedienst kunnen worden geïdentificeerd, formuleert de Autoriteit nog **twee meer punctuele opmerkingen** over de verschillende bepalingen die deze bewaarplicht omkaderen.

104. Ten eerste stelt de Autoriteit vast dat het **nieuwe artikel 127 § 2** van de telecomwet **het gebruik van een gezichtsherkenningstechnologie** voor het identificeren van de abonnee **wil toelaten**. Het **gebruik van gezichtsherkenningstechnieken om abonnees te identificeren gaat verder dan wat nodig is in een democratische samenleving**, terwijl er in België andere, veiliger en minder indringende middelen zijn (het gebruik van eID of Itsme) om mensen elektronisch te authentiseren. Deze mogelijkheid om **gezichtsherkenning als identificatiemiddel te gebruiken**, zal derhalve uit het voorontwerp van wet worden geschrapt. De Autoriteit beklemtoont voorts dat **het gebruik van andere biometrische gegevens, zoals vingerafdrukken, ook verder zou gaan dan wat in een democratische samenleving noodzakelijk en toelaatbaar is**. **.**

105. Ten tweede machtigt het **nieuwe artikel 127 § 3** van de telecomwet de Koning, **echter louter facultatief**, om de door de operator te verzamelen en te bewaren identificatiegegevens en -documenten te bepalen. Volgens de eis van voorzienbaarheid echter moeten deze gegevens en documenten nader worden bepaald. **Ze kunnen worden bepaald door de wetgever zelf of door de Koning, maar** in dat laatste geval moet de **machtiging verplicht zijn**. **Het voorontwerp van wet moet in die zin worden aangepast.**

[102] HvJ-EU, arrest van 6 oktober 2020, § 156.

9) Bewaring van de verkeers- en locatiegegevens ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon (nieuw artikel 126/1 van de telecomwet)

106. Het nieuwe artikel 126/1 van de telecomwet **legt** de operatoren de **verplichting** op om in beginsel, **gedurende 12 maanden**[103] de **verkeers- en locatiegegevens** te bewaren voor **alle communicaties** die worden gevoerd **vanuit** of **naar** een van de **geografische gebieden** die het opsomt. In het voorontwerp van wet wordt echter gepreciseerd dat operatoren dergelijke gegevens enkel hoeven te bewaren indien zij deze reeds genereren of verwerken in het kader van de verstrekking van de door hen aangeboden elektronische-communicatiediensten of de door hen ter beschikking gestelde elektronische-communicatienetwerken[104]. Die bewaring wordt verplicht gesteld "*ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon*". Het nieuwe artikel 126/1 van de telecomwet wil zo, **met het oog op doelstellingen van bijzonder belang** zoals de bestrijding van zware criminaliteit, **een gerichte preventieve bewaring verplichten van de verkeers- en locatiegegevens, afhankelijk van geografische criteria**. Een dergelijke **gerichte bewaarplicht voldoet in beginsel aan** de **Europese eisen** zoals geïnterpreteerd door het HvJ-EU.

107. De Autoriteit stelt evenwel vast dat **het nieuwe artikel 126/1 van de telecomwet een aantal commentaren oproept** aangaande de grondbeginselen van de gegevensbescherming.

- ***Commentaar over het nieuwe artikel 126/1 § 2 van de telecomwet:***

108. Het nieuwe artikel 126/1 § 2 van de telecomwet **bepaalt de categorieën van gegevens die door de operatoren moeten worden bewaard**: Het betreft de volgende gegevens:

[103] Tenzij dit nieuwe artikel 126/1 van de telecomwet in een andere bewaarduur voorziet. In sommige omstandigheden voorziet die bepaling in kortere bewaarperiodes. Zie het nieuwe artikel 126/1 § 3, 1° van de telecomwet.

[104] In de memorie van toelichting wordt uitgelegd dat: "de gegevens enkel bewaard worden door de betrokken operatoren voor zover deze gegevens werden gegenereerd of behandeld door hen in het kader van de verstrekking van de betrokken communicatiediensten, en enkel binnen de vooraf bepaalde geografische zones. Er is m.a.w. geen verplichting gegevens te bewaren wanneer deze:

1° niet gegenereerd of verwerkt worden door de betrokken operatoren

2° niet gegenereerd of verwerkt worden binnen de geografische zones bepaald in paragraaf 3".

"1° de gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt;
2° de communicatiegegevens, met uitzondering van de inhoud, en met inbegrip van hun herkomst en hun bestemming;
3° de gegevens van oproeppogingen zonder resultaat, voor zover die gegevens in het kader van de aanbieding van de bedoelde communicatiediensten:
i° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren; of
ii° wat de internetgegevens betreft, door deze operatoren worden gelogd.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens en kan de vereisten waaraan deze gegevens moeten beantwoorden bepalen."

109. Eerst en vooral stelt de Autoriteit vast dat **het nieuwe artikel 126/1 § 2 van de telecomwet het begrip "*communicatiegegevens*"** gebruikt om de te bewaren categorieën van gegevens te bepalen, terwijl de andere bepalingen van de telecomwet die een gegevensbewaring toelaten of opleggen de begrippen "*verkeersgegevens*", "*locatiegegevens*" of "*andere locatiegegevens dan verkeersgegevens*" hanteren. De laatste drie categorieën van gegevens worden in de telecomwet rechtstreeks of onrechtstreeks gedefinieerd; dat is niet het geval voor het begrip "communicatiegegevens". **Dit gebrek aan definitie schaadt de voorzienbaarheid van de wet**. Dat geldt des te meer als het gebruik van een ander begrip om de krachtens het nieuwe artikel 126/1 van de telecomwet te bewaren gegevens te identificeren doet vermoeden dat het begrip "communicatiegegevens" betrekking heeft op andere gegevens dan "verkeersgegevens" en "locatiegegevens". Na een verzoek om verdere inlichtingen gaf de afgevaardigde van de minister het volgende antwoord: "*Het begrip "communicatiegegevens" is een subgeheel van het begrip "verkeer". Het zijn gegevens die informatie geven over de afzender of de bestemmeling van de communicatie (wie heeft wie/wat gecontacteerd)".* **Om te voldoen aan de eis van voorzienbaarheid moet het voorontwerp van wet worden aangepast om het begrip "communicatiegegevens" te definiëren**.

110. **Eenzelfde opmerking moet worden geformuleerd over het begrip "gegevens van oproeppogingen zonder resultaat".** Waar het begrip "oproeppoging zonder resultaat" in de

telecomwet is gedefinieerd[105], geldt dat niet voor het begrip 'gegevens van oproeppogingen zonder resultaat'. Op een verzoek om verdere inlichtingen antwoordde de afgevaardigde van de minister als volgt: "*De "gegevens van oproeppogingen zonder resultaat" zijn de verkeersgegevens die verband houden met de oproeppogingen zonder resultaat. Het kan bijvoorbeeld gaan om de datum en het tijdstip van deze oproep en om het nummer van de oproeper*". **Om te voldoen aan de eis van voorzienbaarheid van de wet moet het voorontwerp van wet worden aangepast om deze precisering erin aan te brengen: het begrip "gegevens oproeppogingen zonder resultaat" moet worden vervangen door het begrip "verkeersgegevens van de oproeppogingen zonder resultaat".**

111. Het nieuwe artikel 126/1 § 2 **delegeert** het bepalen van de te bewaren gegevens **aan de Koning.** Die machtiging is verplicht: de Koning dient de te bewaren gegevens te bepalen. **De Autoriteit meent dat een dergelijke delegatie aan de Koning toelaatbaar is in het licht van het wettelijkheidsbeginsel**: de categorieën van gegevens worden voldoende nauwkeurig bepaald in de wet (op voorwaarde echter dat het voorontwerp van wet wordt gewijzigd om tegemoet te komen aan de opmerkingen die de Autoriteit in de voorgaande paragrafen heeft geformuleerd) en de materie behelst een zekere techniciteit die rechtvaardigt dat de Koning bepaalt welke precieze verkeersgegevens moeten worden bewaard.

112. **Het koninklijk besluit van 19 september 2013,** dat wordt gewijzigd door het ontwerpbesluit dat voor advies wordt voorgelegd aan de Autoriteit, **is de tenuitvoerlegging van het nieuwe artikel 126/1 § 2 van de telecomwet** en bepaalt de gegevens die de operatoren moeten bewaren in uitvoering van deze bepaling:

- De aanbieders van **openbare diensten voor vaste telefonie**, de nomadische diensten inbegrepen, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren **"ten minste**" de volgende gegevens:

  1° de identificatie van het telefoonnummer van de oproeper en van de opgeroepen;
  2° de plaats van het netwerkaansluitpunt van de oproeper en van de opgeroepene;
  3° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;
  4° de datum en het juiste tijdstip van aanvang en einde van de oproep;
  5° de beschrijving van de gebruikte telefoniedienst.

[105] Dit begrip wordt gedefinieerd in artikel 2 van het voorontwerp van wet dat een punt 74° toevoegt aan artikel 2 van de telecomwet: "een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord".

- De aanbieders van een **openbare dienst voor mobiele telefonie**, de nomadische diensten inbegrepen, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren **"ten minste"** de volgende gegevens:

  1° de identificatie van het telefoonnummer van de oproeper en van de opgeroepene;
  2° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;
  3° de "International Mobile Subscriber Identity" ("IMSI") of "Subscription Permanent Identifier (SUPI) van de oproepende en opgeroepen deelnemer;
  4° de "International Mobile Equipment Identity" ("IMEI") of "Permanent Equipment Identifier (PEI) van het mobiele eindapparaat van de oproepende en opgeroepen deelnemer;
  5° de datum en het juiste tijdstip van aanvang en einde van de oproep;
  6° de locatie van het netwerkaansluitpunt bij aanvang en bij het einde van elke verbinding;
  7° de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt;
  8° de technische karakteristieken van de gebruikte telefoondienst.

- De aanbieders van openbare **internettoegangsdiensten** en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren **"ten minste"** de volgende gegevens:

  1° de toegewezen eindgebruikersidentificatie;
  2° de identificatie en de locatie van de netwerkaansluitpunten die door de eindgebruiker worden gebruikt van het begin tot en met het einde van een verbinding of een communicatie;
  3° de datum en het tijdstip van de log-in en log-off van een sessie van de internettoegangsdienst;
  4° het tijdens de sessie of een andere opgevraagde tijdseenheid geüploade en gedownloade volume van gegevens;
  5° de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt;

- De aanbieders van een **openbare e-maildienst via internet**, de aanbieders van een **openbare internettelefoniedienst** en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie bewaren de volgende gegevens:

1° de identificatie van de eindgebruiker van de e-mail- of internettelefonieaccount, alsook het nummer of de identificatie van de beoogde ontvanger van de communicatie;
2° het telefoonnummer toegewezen aan elke communicatie die het openbare telefoonnetwerk binnenkomt in het kader van een internettelefoniedienst;
3° a) het IP-adres en de bronpoort die worden gebruikt door de eindgebruiker;
b) het IP-adres en de bronpoort die worden gebruikt door de bestemmeling;
4° de datum en het tijdstip van de log-in en log-off van een sessie van de e-mail- of internettelefoniedienst;
5° de datum en het tijdstip van de verbinding die tot stand wordt gebracht met behulp van de internettelefonieaccount;
6° de technische karakteristieken van de gebruikte dienst.

113. De Autoriteit stelt vast dat **de opsomming van gegevens in het besluit van 19 september 2013 niet volledig is.** Het koninklijk besluit stelt immers als volgt: "*de aanbieders […] bewaren ten minste de volgende gegevens […]* "[106]. **Een onvolledige opsomming van de te bewaren gegevens kan niet voldoen aan de eis van voorzienbaarheid**. Het **ontwerpbesluit moet worden aangepast** opdat het koninklijk besluit van 19 september 2013 een volledige opsomming zou geven van de door de operatoren te bewaren gegevens.

114.114. Voorts benadrukt de Autoriteit dat de bewaring van verkeersgegevens geen specifieke url van de door de betrokkenen bezochte webpagina's mag bevatten of mag toelaten die url's af te leiden.

115. De Autoriteit heeft **geen verdere opmerkingen** over de gegevens die zijn bepaald in het koninklijk besluit van 19 september 2013.

- ***Commentaar over het nieuwe artikel 126/1 § 3 van de telecomwet:***

116. Het nieuwe artikel 126/1 § 3 van de telecomwet identificeert **de verschillende geografische zones waarbinnen de operatoren preventief de verkeersgegevens moeten bewaren die betrekking hebben op de communicaties die er worden gevoerd** (omdat zich daar de herkomst of de bestemming van de communicatie bevindt).

117. Uit de Europese rechtspraak blijkt dat een wetgevende maatregel een "gerichte" preventieve bewaarplicht kan opleggen op basis van geografische criteria ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de

[106] Woorden onderlijnd door de Autoriteit.

openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon. Het HvJ-EU meent inderdaad dat een dergelijke maatregel in beginsel voldoet aan het evenredigheidsbeginsel. **Er moet evenwel op worden toegezien dat de criteria die het voorontwerp van wet weerhoudt voor de bepaling van de geografische zones waarbinnen een verplichting tot preventieve bewaring van de verkeersgegevens wordt opgelegd, in de praktijk niet neerkomt op een verplichting tot algemene en ongedifferentieerde bewaring van de verkeersgegevens**.

118. Ter herinnering: volgens het HvJ-EU mogen de lidstaten een dergelijke algemene en ongedifferentieerde bewaring van de verkeersgegevens enkel opleggen wanneer er voldoende concrete aanwijzingen zijn om dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid en die bedreiging werkelijk en actueel of voorzienbaar is. Het HvJ-EU preciseert dat de nationale veiligheid overeenstemt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving en het voorkomen en bestrijden bevat van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en met name een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als dusdanig, zoals terroristische activiteiten[107].

119. Het **nieuwe artikel 126/1 § 3, 1° van de telecomwet** voorziet in de verplichting tot bewaring van deze gegevens voor "*de gerechtelijke arrondissementen waar minstens 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren*" of voor *"de politiezones waar minstens 3strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan 3 strafbare feiten zoals bedoeld in artikel 90ter van het Wetboek van Strafvordering per 1000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de 3 voorbije kalenderjaren"*.

120. Artikel 90ter § 2 van het WSV bevat een lange lijst van strafbare feiten. Voor de betreffende strafbare feiten bepaalt het als volgt: "*De onderzoeksrechter kan, met een heimelijk oogmerk, niet voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen of de zoeking in een informaticasysteem of een deel ervan uitbreiden*". De afgevaardigde van de minister verklaarde in een antwoord op een verzoek om verdere inlichtingen als volgt: deze lijst "*wordt over het algemeen beschouwd als de lijst met de meest zware vormen van criminaliteit. De lijst wordt in het wetboek*

[107] HvJ-EU, arrest van 6 oktober 2020, § 135.

meerdere keren gebruikt als drempel voor de proportionaliteitsvereiste voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer. Dit is o.a. het geval voor:

- *De proactieve recherche (artikel 28bis, § 2)*
- *Het blokkeren van banktegoeden (artikel 46quater, § 2, tweede lid)*
- *De inkijkoperatie (artikel 46quinquies/89ter)*
- *De infiltratie (artikel 47octies)*
- *De observatie met gebruik van technische middelen om zicht te krijgen in de woning van een advocaat of een arts (artikel 56bis)*
- *De volledige anonimiteit van getuigen (artikel 86bis)*
- *De onderschepping en kennisname van private elektronische communicatie en de geheime zoeking in een informaticasysteem (artikel 90ter)*
- *Het toekennen van bijzondere beschermingsmaatregelen aan bedreigde getuigen (artikel 104, § 2)*
- *Het toekennen van bijzondere beschermingsmaatregelen aan bedreigde personen die een openbaar ambt uitoefenen (artikel 111quater, § 1, tweede lid)* ».

121. **De Autoriteit neemt nota van de keuze van de aanvrager om aan de hand van deze lijst te bepalen welke strafbare feiten onder de noemer "zware criminaliteit" vallen.**

122. Ze **stelt zich echter wel vragen over de keuze van de drempel van "3 strafbare feiten 90ter per 1000 inwoners per jaar"** om een zone aan te merken als bijzonder blootgesteld aan feiten van zware criminaliteit. De memorie van toelichting geeft het totale aantal strafbare feiten aan dat in een gerechtelijk arrondissement moet worden vastgesteld opdat de bewaring van de gegevens er kan worden verplicht, maar geeft geen statistieken over het aantal strafbare feiten "90ter" dat daadwerkelijk werd vastgesteld in de verschillende gerechtelijke arrondissementen. De Autoriteit heeft deze statistieken opgevraagd om te kunnen beoordelen of de weerhouden drempel *de facto* kan leiden tot een algemene en ongedifferentieerde verplichting om de verkeersgegevens te bewaren van alle gebruikers van een elektronisch communicatiemiddel. Deze informatie werd haar evenwel niet meegedeeld. **Bijgevolg is de Autoriteit niet bij machte om de relevantie en evenredigheid van dit weerhouden criteria te beoordelen**. **De wetgever moet de door hem weerhouden drempel rechtvaardigen en aantonen dat deze *de facto* niet kan leiden tot een verplichting tot algemene en ongedifferentieerde bewaring van de gegevens op (bijna) het hele nationale grondgebied**. Het weerhouden criterium (een gemiddelde van 3 strafbare feiten 90ter per 1000 inwoners per jaar) is uiteraard een dynamisch criterium; derhalve is het niet mogelijk om voor eens en voor altijd te bepalen of het *de facto* zal leiden tot een algemene en ongedifferentieerde bewaring van de gegevens op (bijna) het volledige nationale grondgebied. **De wetgever moet er echter wel op toezien dat de impact van deze drempel in de praktijk evenredig is met de**

huidige statistieken; dat zou niet het geval zijn als bij de inwerkingtreding van het voorontwerp van wet het hele nationale grondgebied (of toch bijna) "onder toezicht" zou worden geplaatst. **De wetgever moet een strenge en kwantitatieve analyse maken van de evenredigheid van het criterium/de drempel die in het voorontwerp van wet wordt gehanteerd**.

123. Het voorontwerp van wet bepaalt als volgt: "*De gebruikte statistieken zijn afkomstig van de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet op het politieambt*" (hierna "de A.N.G." genoemd). **De Autoriteit neemt daar nota van, maar benadrukt dat de wetgever hoe dan ook moet aantonen dat de A.N.G de meest geschikte databank is voor dat doel**. De Autoriteit stelt zich vragen bij de relevantie van het gebruik van de A.N.G. aangezien die in de databank wordt bijgehouden door de politie die van nature, gezien haar wettelijke opdracht, zal geneigd zijn om er alle vermoedens van strafbare feiten 90ter in op te nemen en/of, zoals het C.O.C. heeft benadrukt in zijn advies van 21 mei 2020, om een vermoeden van strafbaar feit al te makkelijk aan te merken als een vermoeden van ernstig misdrijf in de zin van artikel 90ter van het W.S.V. **In die context meent de Autoriteit dat het passender zou zijn om een databank te gebruiken waarvan de kwaliteit van de statistische gegevens is vastgelegd bij wet, zoals de wet van 4 juli 1962 betreffende de openbare statistiek**[108].

124. Om te vermijden dat de politiediensten geneigd zouden zijn om een vermoeden van strafbaar feit "te makkelijk" aan te merken als een vermoeden van ernstig strafbaar feit in de zin van artikel 90ter van het W.S.V. oordeelt de Autoriteit bovendien dat **bij de berekening van de drempel** die wordt

[108] Artikel 1 bis van de wet van 4 juli 1962 bepaalt als volgt: "*De statistieken worden geregeld volgens de volgende principes:*
1° Principe van rechtmatigheid en eerlijkheid:
a) het verzamelen en verwerken van gegevens steunt ofwel op een wettelijke of reglementaire basis, ofwel op de toestemming van de aangever in de zin van artikel 1, § 8, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, onverminderd de bijzondere bepalingen van deze wet;
b) eerlijke gegevensverzameling veronderstelt een goede informatie voor de aangever over het verzamelen en verwerken van de gegevens. De aangever heeft het recht informatie te krijgen over de rechtsgrond, het doel van de gegevensverzameling en de toegepaste beschermingsmaatregelen;
2° Principe van finaliteit:
a) individuele gegevens worden uitsluitend voor statistische doeleinden gebruikt, tenzij de aangever ondubbelzinnig toestemming heeft gegeven dat de gegevens voor een andere aanwending worden gebruikt;
b) gegevens die voor een welbepaald statistisch doel werden verzameld mogen enkel voor andere statistische doeleinden worden gebruikt, wanneer die met het eerste doel verenigbaar zijn;
c) gegevens die voor statistische doeleinden werden verzameld en verwerkt, mogen niet worden gebruikt om gegevensbestanden aan te vullen of te verbeteren die voor andere dan statistische, onder meer voor administratieve doeleinden dienen;
d) op basis van de individuele statistische gegevens die bij het opmaken van een statistiek werden verzameld, mag geen enkele beslissing genomen worden die tot doel of gevolg heeft de individuele situatie van de aangever te beïnvloeden;
3° Principe van evenredigheid:
a) bij de keuze van de methode van verzamelen wordt de voorrang gegeven aan de secundaire verzameling boven de primaire verzameling. In elk geval zal de verzameling bij voorkeur steekproefsgewijs gebeuren, eerder dan exhaustief en zijn vrijwillige enquêtes te verkiezen boven verplichte enquêtes;
b) de gegevens zijn toereikend, ter zake dienend en niet overmatig uitgaande van het vastgestelde statistische doeleinde, dit wil zeggen dat de verzameling en de verwerking van de gegevens beperkt zijn tot die gegevens die noodzakelijk zijn voor de nagestreefde statistische doeleinden;
4° Principe van onpartijdigheid, objectiviteit en professionele onafhankelijkheid:
a) de statistieken moeten met inachtneming van de wetenschappelijke onafhankelijkheid en op objectieve, professionele en transparante wijze worden geproduceerd en verspreid, waarbij alle gebruikers gelijk worden behandeld;
b) het produceren en verspreiden van statistieken moet worden verricht door een orgaan dat professioneel onafhankelijk is tav andere regelgevende, administratieve of beleidsdepartementen en lichamen, en van de particuliere sector".

weerhouden om te bepalen of de zone bijzonder is blootgesteld aan "zware criminaliteit" **rekening moet worden gehouden met het aantal strafbare feiten die hebben geleid tot een veroordeling door de rechtbank**, en niet met het aantal strafbare feiten die werden vastgesteld door de politiediensten. De basis van het aantal veroordelingen biedt immers meer garanties dat de bewaring van de verkeersgegevens wordt 'geactiveerd' "*op basis van objectieve en niet-discriminerende factoren*"[109].

125. Het nieuwe artikel 126/1 § 3, 3° van de telecomwet noemt 16 categorieën van *"gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit*". Het nieuwe artikel 126/1 § 3, 4° van de telecomwet noemt 14 categorieën van "*zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking*". Het nieuwe artikel 126/1 § 3, 5° van de telecomwet noemt 5 categorieën van "*zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen*". Het voorontwerp van wet laat de Koning telkens toe om andere zones te bepalen bij koninklijk besluit. De Autoriteit formuleert daarover twee opmerkingen:

i. Ten eerste stelt de Autoriteit vast dat het voorontwerp van wet ervoor kiest om talrijke zones te weerhouden waar de verplichting wordt opgelegd tot preventieve bewaring van de verkeersgegevens van de communicaties die er worden gevoerd (hetzij omdat de herkomst van de communicatie zich er bevindt, hetzij de bestemmeling van de communicatie). **De Autoriteit benadrukt dat de wetgever er bij de beraadslaging die de stemming voorafgaat op moet toezien dat de noodzaak en evenredigheid van de keuze van de verschillende weerhouden plaatsen wordt beoordeeld[110]**. Het is in ieder geval van belang dat deze keuze van locaties niet leidt tot de feitelijke herinvoering van een verplichting om de gegevens van een te groot deel van de gebruikers van elektronische communicatie in België te bewaren.

[109] HvJ-EU, arrest van 6 oktober 2020, § 150.

[110] De Autoriteit vraagt zich bijvoorbeeld af of het werkelijk nodig en evenredig is om te voorzien in een bewaring van de verkeersgegevens van alle communicaties die worden gevoerd vanaf of naar de autosnelwegen of de bijhorende openbare parkeerterreinen. Na een verzoek om verdere inlichtingen antwoordt de afgevaardigde van de minister als volgt: "*De autosnelwegen zijn het belangrijkste netwerk voor wegtransport van ons land. Dankzij dat netwerk kan het hele land worden bevoorraad met voedsel, energie, enz. Het is ook het belangrijkste netwerk dat wordt gebruikt door de diensten die dringende hulp bieden aan de bevolking. De bijhorende parkeerterreinen maken wezenlijk deel uit van het autosnelwegennet. Het zijn zones waar de automobilisten even halt houden en op de meeste parkeerterreinen kan er ook worden getankt. Vanwege de bijzondere kenmerken van de autosnelwegen (wegen waarop aan hoge snelheid wordt gereden en waar enkel op de pechstrook kan worden stilgestaan) zijn de parkeerterreinen langs de autosnelwegen ook zones van uitwisseling, rust, enz. De wegcode bepaalt in haar artikel 21.4 dat een voertuig enkel mag stilstaan of geparkeerd worden op de parkeerstroken aangewezen door het verkeersbord. De veiligheid op de parkeerterreinen langs de autosnelweg i s niet alleen belangrijk voor de vrachtwagenchauffeurs, maar ook voor alle gebruikers van deze autosnelwegen"*. Die factoren tonen echter niet de noodzaak en de evenredigheid aan van een verplichte bewaring van de gegevens van de communicaties van en naar de autosnelwegen.

ii. Ten tweede is hoe dan ook **het wettelijkheidsbeginsel** dat wordt bekrachtigd in artikel 22 van de Grondwet **in strijd met het feit dat de wetgever de Koning kan machtigen om de bewaarplicht uit te breiden tot andere plaatsen** dan deze die zijn geïdentificeerd in het voorontwerp van wet. Het voorontwerp van wet **moet worden gewijzigd om die mogelijkheid te schrappen**.

126. Ten slotte acht de Autoriteit het **noodzakelijk te zorgen voor transparantie** met betrekking tot (1) **het percentage van het nationale grondgebied waarvoor de verplichting tot preventieve bewaring** krachtens het nieuwe artikel 126/1 van de Telecomwet geldt en (2) **het percentage van de bevolking dat door deze verplichting wordt getroffen**. Een dergelijke transparantie zou het mogelijk maken na te gaan of de door de wetgever vastgestelde criteria niet hebben geleid tot de feitelijke herinvoering van een algemene en ongedifferentieerde verplichting om verkeers- en locatiegegevens te bewaren met het oog op de bestrijding van zware criminaliteit, die door het Hof van Justitie van de Europese Unie onevenredig is bevonden. **Deze statistieken moeten worden opgenomen in het verslag dat de minister van Telecommunicatie en de minister van Justitie jaarlijks aan de Kamer van Volksvertegenwoordigers moeten voorleggen op grond van het nieuwe artikel 127/2, § 1, van de telecomwet**. Ze zouden ook kunnen worden gepubliceerd op de website van het BIPT, die volgens het nieuwe artikel 127/1 § 2 van de telecomwet al algemene informatie moet bevatten over de toegang van de autoriteiten tot de gegevens die door de operatoren worden bijgehouden.

127. Meer in het algemeen is het **essentieel dat het jaarverslag dat aan het Parlement wordt voorgelegd alle gegevens bevat die nodig zijn om de doeltreffendheid en de evenredigheid van de verschillende maatregelen inzake de bewaring** van verkeers- en locatiegegevens te kunnen beoordelen. Daartoe dient het **jaarverslag ten minste de volgende gegevens te bevatten**:

- het soort en de hoeveelheid verkeers- en locatiegegevens die door de operatoren worden verzameld overeenkomstig de bepalingen van de telecomwet en het C.I.C. (met inbegrip van het percentage van het grondgebied en de bevolking waarvoor gegevens worden bewaard overeenkomstig het nieuwe artikel 126/1 van de telecomwet);
- Het aantal keren dat een autoriteit om toegang tot gegevens van operatoren heeft verzocht;
- De redenen waarom de autoriteiten toegang hebben gevraagd (en gekregen) tot de door de operatoren bewaarde gegevens (zonder uiteraard in detail en in concreto te treden) en informatie om het nut van deze toegang vast te stellen.

Het voorontwerp van wet moet worden herzien om de in het jaarverslag op te nemen informatie aan te vullen.

➢ ***Commentaar over het nieuwe artikel 126/1 § 4 van de telecomwet:***

128. Het nieuwe artikel 126/1 § 4, eerste lid van de telecomwet bepaalt als volgt: "*De operatoren bewaren de gegevens voor alle communicaties die vanuit of naar een geografisch gebied als bedoeld in paragraaf 3 worden gevoerd*"[111]. **Om de vereiste duidelijkheid en nauwkeurigheid te garanderen, moet het voorontwerp van wet preciseren dat onder "*de gegevens*" de "*gegevens bedoeld in § 2*"" moet worden verstaan.**

129. Het nieuwe artikel 126/1 § 4, laatste lid bepaalt als volgt: "*Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.*" **Deze bepaling is problematisch gezien het beginsel van minimale gegevensverwerking en, maar fundamenteel, het evenredigheidsbeginsel** waaraan elke maatregel tot bewaring van de gegevens moet voldoen. Ze dreigt immers te leiden tot een bewaring van de gegevens die verder gaat dan wat strikt noodzakelijk en evenredig is voor de beoogde doelen. Het feit dat de operatoren, in uitvoering van artikel 126/1 van de telecomwet, de verkeersgegevens mogen bewaren die betrekking hebben op communicaties die buiten de door de bepaling afgebakende geografische zones worden gevoerd, is in strijd met het evenredigheidsbeginsel. Bovendien zijn die geografische zones in het voorontwerp van wet zeer ruim bepaald en geldt de verplichting tot bewaring van de gegevens niet alleen voor de communicaties "afkomstig" van deze zones, maar ook voor de communicaties naar deze zones. **Het voorontwerp van wet moet worden herzien om de mogelijkheid te schrappen die de operatoren wordt geboden om gegevens te bewaren van buiten de geografische zones waarbinnen het voorontwerp van wet voorziet in een bewaarplicht wanneer het voor hen technisch niet mogelijk is om de gegevensbewaring te beperken tot die zones**.

130. De Autoriteit benadrukt dat de wetgever moet nagaan of de oprichting van een gegevensbewaringssysteem dat beperkt is tot bepaalde geografische zones technisch mogelijk is voordat hij beveelt tot een gerichte bewaring op basis van geografische criteria. **Als het technisch onmogelijk is om de bewaring te beperken tot de verkeersgegevens van communicaties die worden gevoerd in bepaalde geografische zones, mag de wetgever niet voorzien in de oprichting van een dergelijk systeem**.

[111] Woorden onderlijnd door de Autoriteit.

10) Bepaling van de verwerkingsverantwoordelijke van de bewaring van de verkeers- en locatiegegevens die is opgelegd door de artikelen 122, 123, 126, 126/1 en 127 van de telecomwet (nieuw artikel 127/3 § 2 van de telecomwet)

131. Het nieuwe artikel 127/3 § 2 van de telecomwet stelt als volgt: "*Elke operator wordt beschouwd als verantwoordelijk voor de verwerking in de zin van de AVG, voor de gegevens behandeld op basis van de artikelen 122, 123, 126, 126/1 en 127*".

132. De Autoriteit **neemt nota van deze aanduiding, maar wijst op het feit dat de verwerkingsverantwoordelijke verantwoordelijk is voor een of meerdere verwerkingen en niet voor gegevens**. Elke operator is verantwoordelijk voor de verwerkingen bedoeld in de artikelen 122, 123, 126, 126/1 en 127, maar niet voor de gegevens die op basis van die bepalingen worden verwerkt. **De formulering van artikel 127/3 § 2 moet in die zin worden aangepast.**

11) Technische en organisatorische maatregelen die de operatoren worden opgelegd voor de bewaring van de verkeers- en locatiegegevens (nieuwe artikelen 127/2 en 127/3 van de telecomwet)

133. De nieuwe **artikelen 127/2 en 127/3** van de telecomwet willen de operatoren de verplichting opleggen om technische en organisatorische maatregelen te nemen voor de bewaring van de verkeers- en locatiegegevens.

134. De meeste van deze maatregelen worden opgelegd om de veiligheid van de door de operatoren bewaarde gegevens te garanderen. De Autoriteit stelt vast dat **deze maatregelen, in overeenstemming met de rechtspraak van het HvJ-EU, erop gericht zijn om een bijzonder hoog niveau van bescherming en veiligheid te garanderen**. De maatregelen voldoen aan verschillende eisen die uitdrukkelijk werden opgelegd door het HvJ-EU, in het bijzonder:

- De verplichting om **de gegevens op het grondgebied van de Europese Unie te bewaren** (zie het nieuwe artikel 127/2 § 3, eerste lid, 2° van de telecomwet);
- De verplichting om **de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt van elke drager te verwijderen of om deze gegevens te anonimiseren** (zie het nieuwe artikel 127/2 § 3, tweede lid, 1° van de telecomwet);
- De goedkeuring van maatregelen **om het risico van misbruik of onrechtmatige toegang tot de gegevens te beperken** (zie met name het nieuwe artikel 127 § 3, eerste lid, 3° van de telecomwet dat oplegt om **de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben** of het nieuwe artikel 127 § 3,

tweede lid, 4° van de telecomwet dat de operatoren verplicht om **ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord aan de hand van een logboek**).

135. Toch formuleert de Autoriteit **meerdere opmerkingen** over deze bepalingen betreffende de veiligheid van de gegevens.

136. Eerst en vooral stelt de Autoriteit vast **dat de verplichting om de gegevens te bewaren op het grondgebied van de Europese Unie enkel geldt voor de gegevens die de operatoren bewaren ten behoeve van de autoriteiten, en niet voor de gegevens die ze bewaren voor hun eigen behoeften** (zie het nieuwe artikel 127/2 § 3, eerste lid, 2° van de telecomwet). De Autoriteit formuleert hierbij **twee opmerkingen**:

(i) **Ten eerste ontbreekt het aan duidelijkheid over het onderscheid tussen gegevens die de operatoren bewaren ten behoeve van de autoriteiten en de gegevens die ze bewaren voor hun eigen behoeften**. De nieuwe artikelen 122 en 123 van de telecomwet leggen immers verplichtingen op tot bewaring met het oog op het bestrijden van fraude (waarvan de operatoren het slachtoffer kunnen zijn) en met het oog op de veiligheid van de netwerken (wat een verplichting is in hoofde van de operatoren). Bovendien voorziet het voorontwerp dat de autoriteiten onder bepaalde voorwaarden toegang kunnen krijgen tot die gegevens, ook voor andere doeleinden dan deze waarvoor ze oorspronkelijk werden bewaard. Worden die gegevens dan bewaard ten behoeve van de autoriteiten of voor de eigen behoeften van de operatoren?[112]

(ii) **Ten tweede** benadrukt de Autoriteit dat het HvJ-EU oordeelt dat gezien de hoeveelheid bewaarde gegevens, het gevoelige karakter van die gegevens en het risico van onrechtmatige toegang ertoe, de bewaring op het grondgebied van de Unie een noodzakelijke maatregel is om een zeer hoog niveau van bescherming en veiligheid te garanderen. **Het HvJ-EU maakt geen onderscheid naargelang het doel waarvoor de gegevens worden bewaard en de Autoriteit ziet niet in waarom een dergelijk onderscheid relevant zou zijn**. **Het voorontwerp moet dus worden gewijzigd om te voorzien dat alle door de operatoren bewaarde gegevens, worden bewaard op het grondgebied van de Unie**.

137. Vervolgens formuleert de Autoriteit **twee belangrijke opmerkingen over de informatie die moet worden opgenomen in het logboek**:

[112] De Autoriteit benadrukt dat haar opmerking over het gebrek aan duidelijkheid en onderscheid tussen gegevens die worden bewaard ten behoeve van de autoriteiten en gegevens bewaard voor hun eigen behoeften uiteraard ook, mutati mutandis, geldt voor de andere verplichtingen die worden opgelegd door artikel 127/3 § 3, eerste lid van de telecomwet.

(i) Het voorontwerp stelt als volgt: "*Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan"*. De Autoriteit benadrukt echter **dat het concrete doel waarvoor de toegang tot de gegevens werd gevraagd in de informatie in het logboek moet worden vermeld** aangezien die informatie nodig is om het gebruik van de gegevens *a posteriori* daadwerkelijk te kunnen controleren. Gezien de gevoeligheid van die informatie **moet ze echter 'omfloerst' worden opgetekend.**

(ii) Het voorontwerp bepaalt: "*De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen en, in het bijzonder, om elke niet-toegestane handeling in verband met dat logboek te voorkomen*. De Autoriteit benadrukt **dat elke handeling in het logboek hoe dan ook zelf moet worden opgetekend** of dat de noodzaak moet worden benadrukt dat de gegevens van het logboek niet kunnen worden gewist.

138. Bovendien wil het voorontwerp van wet de operatoren een aantal technische en/of organisatorische eisen opleggen om, zo lijkt het, de beschikbaarheid en de kwaliteit van de bewaarde gegevens te garanderen.

139. Het **nieuwe artikel 127/2 § 2, eerste lid** van de telecomwet bepaalt: *"De operatoren zorgen ervoor dat de gegevens die ze bewaren voor hun eigen behoeften en deze die ze bewaren voor de autoriteiten onbeperkt toegankelijk zijn vanuit België".* Het doel en de reikwijdte van die bepaling zijn hierbij niet duidelijk. De memorie van toelichting verschaft geen duidelijkheid in dit verband. Na een verzoek om verdere inlichting antwoordde de afgevaardigde van de minister als volgt: "*Het feit dat de gegevens toegankelijk moeten zijn vanuit België betekent niet dat ze in België moeten worden bewaard. […] Het doel van de zinsnede "onbeperkt toegankelijk vanuit België" bestaat erin dat de operator de door de overheid gevraagde gegevens in België moet verstrekken. Het Belgisch recht blijft zo van toepassing*". De bepaling lijkt de operatoren de verplichting op te leggen om de toegankelijkheid van de door hen bewaarde gegevens te allen tijde te garanderen, ongeacht de plaats waar die gegevens worden bewaard. **De bepaling moet worden aangepast om de reikwijdte ervan te verduidelijken**. Deze opmerking geldt *mutatis mutandis* ook voor het nieuwe artikel 127/4, laatste lid die een gelijkaardige bepaling bevat.

140. Het **nieuwe artikel 127/2 § 2, laatste lid** van de telecomwet bepaalt als volgt: "*De operatoren zijn in staat verbanden te leggen tussen de gegevens bewaard voor de autoriteiten".* Volgens de memorie van toelichting: "*Het is aan de operatoren om te beslissen hoe ze zich organiseren voor de bewaring van de gegevens ten behoeve van de autoriteiten (in het bijzonder de gegevens bewaard conform de artikelen 126, 126/1, 127). Wanneer eenzelfde gegeven wordt bedoeld in verscheidene*

artikelen, mogen ze dat gegeven dus één keer bewaren. De operatoren moeten daarentegen in staat zijn om verbanden te leggen tussen de gegevens bewaard voor de autoriteiten. Dat is nodig aangezien een operator, om te antwoorden op een verzoek van een autoriteit, genoopt zou kunnen zijn om gegevens te raadplegen die zijn bewaard op basis van verschillende artikelen." Na een verzoek om verdere inlichtingen preciseerde de afgevaardigde van de minister als volgt: "*Bedoeling is om te vermijden dat die bewaarde gegevens onbruikbaar zouden zijn bij gebrek aan verband tussen de gegevens. Het is bijvoorbeeld van essentieel belang dat de operatoren een verband kunnen leggen tussen de toegangs-, verbindings- of communicatiegegevens die worden bewaard in uitvoering van artikel 126/1 en de gegevens bewaard op basis van het nieuwe artikel 126. De identificatiegegevens werden in artikel 126/1, § 2, 3° niet opgenomen om te vermijden dat dezelfde gegevens tweemaal worden bewaard".* De Autoriteit begrijpt de wil van de wetgever, maar benadrukt dat de reikwijdte van artikel 127/2 § 2 niet voldoende blijkt uit de bewoordingen. **De bepaling moet worden aangepast om de reikwijdte ervan te verduidelijken**. De Autoriteit benadrukt in dit verband dat als de wetgever de autoriteiten wil toelaten om op basis van de verschillende gegevens die worden bewaard door de operatoren onderzoek te doen naar de betrokken personen, hij - overeenkomstig het evenredigheidsbeginsel - de zoekcriteria moet bepalen aan de hand waarvan de bevoegde autoriteiten hun onderzoek kunnen verrichten en de verbanden kunnen leggen.

12) Bewaring van de gegevens voor de identificatie van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische communicatiedienst door de aanbieders van <u>private</u> elektronische communicatienetwerken en elektronische communicatiediensten die niet openbaar beschikbaar zijn (nieuw artikel 127/4 van de telecomwet)

141. Het **nieuwe artikel 127/4 van de telecomwet** bepaalt dat de Koning de voorwaarden moet vaststellen waaronder de aanbieders van **private** elektronische communicatienetwerken en elektronische communicatiediensten die niet openbaar beschikbaar zijn **de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische communicatiedienst registreren en bewaren**. Met die bewaarplicht worden de **volgende doelen beoogd**:
    - Het opsporen en de beteugeling van strafbare feiten,
    - De beteugeling van kwaadwillige oproepen naar de nooddiensten,
    - Het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk of -dienst,
    - De vervulling van de inlichtingenopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

142. Het nieuwe artikel 127/4 van de telecomwet **delegeert aan de Koning** het **vaststellen van de technische en administratieve maatregelen die aan de aanbieders van private** elektronische communicatienetwerken en -diensten die niet openbaar beschikbaar zijn, worden opgelegd **om betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennis nemen en opnemen van privécommunicatie mogelijk te maken** onder de voorwaarden bepaald door de artikelen 46bis, 88bis, 90ter tot 90decies en 464/13, 464/25 en 464/26 van het Wetboek van Strafvordering, evenals de voorwaarden bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

143. De Autoriteit herhaalt dat het wettelijkheidsbeginsel eist dat de essentiële factoren van een gegevensverwerking, die een inmenging vormt in de grondrechten van de betrokken personen, worden bepaald door een formele wetgevende norm. Die norm moet bovendien voldoende duidelijk en nauwkeurig zijn opdat de betrokken personen op voorzienbare wijze zouden weten in welke omstandigheden de gegevensverwerking is toegelaten. De **fundamentele begrippen die worden gebruikt om de reikwijdte van de verplichting tot gegevensbewaring te omschrijven, moeten dus worden vastgelegd door de wetgeving.** Behoudens vergissing worden **de begrippen "aanbieders van private elektronische communicatienetwerken" en "aanbieders van elektronische communicatiediensten die niet openbaar beschikbaar zijn" in de telecomwet niet gedefinieerd**. Zoals de Autoriteit net heeft benadrukt, **is dat echter een essentiële factor** van de gegevensverwerkingen die worden opgelegd door artikel 127/4 van de telecomwet **aangezien de definitie van deze begrippen een invloed heeft op de reikwijdte van de opgelegde bewaarplichten**. Worden met het begrip ”private netwerken” enkel de netwerken van de ondernemingen bedoeld of heeft het betrekking op om het even welk privaat netwerk, ook op de netwerken die personen bij hen thuis hebben geïnstalleerd? En verwijst het begrip naar de netwerken van om het even welke onderneming, of wil de wetgever de bewaarplichten enkel opleggen als de onderneming een zekere omvang heeft? **Het voorontwerp moet worden aangepast om deze begrippen te definiëren, met dien verstande dat de definitie van die begrippen** – en de bewaarplichten die moeten worden opgelegd naargelang die definities – **moet voldoen aan de beginselen van noodzaak en evenredigheid**.

144. De Autoriteit benadrukt dat het voorontwerp de vaststelling van de technische nadere regels betreffende de door het nieuwe artikel 127/4 van de telecomwet opgelegde bewaarplichten mag delegeren - wat het ook doet.

13)Toegang tot de gegevens

145. Het nieuwe artikel 127/1 van de telecomwet identificeert de categorieën van autoriteiten die toegang kunnen krijgen tot de gegevens die de operatoren bewaren in uitvoering van de (nieuwe) artikelen 122, 123, 126, 126/1 en 127 van de telecomwet.

146. Als artikel 127/1 van de telecomwet wordt gelezen in het licht van de artikelen 122, 123, 126, 126/1 en 127 van diezelfde wet, blijkt dat de **autoriteiten die een van de doeleinden nastreven** die zijn bedoeld in artikel 127/1 van de telecomwet **toegang kunnen krijgen tot de gegevens die worden bewaard krachtens de** (nieuwe versies van de) **artikelen 122, 123, 126 en 127 voor elk van de doeleinden die zijn aangegeven in dit artikel 127/1** van de telecomwet.

147. Volgens de nieuwe artikelen 126 en 127 van de telecomwet moeten de gegevens die op grond van deze bepalingen worden bewaard, "*worde*n *bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1*".

148. De artikelen 122 en 123 van de telecomwet staan toe of leggen daarentegen de verplichting op om gegevens te bewaren voor specifieke doeleinden (facturering, marketing van de diensten met toegevoegde waarde, bestrijding van fraude en kwaadwillig gebruik van het netwerk of veiligheid van de netwerken en correcte werking van de communicatiediensten). Het nieuwe artikel 127/1 bepaalt echter dat de autoriteiten die bevoegd zijn om een van de opgesomde doeleinden na te streven **toegang kunnen krijgen tot alle gegevens die worden bewaard in toepassing van die artikelen 122 en 123 van de telecomwet**, ook als de bewaring ervan oorspronkelijk werd toegelaten of opgelegd voor een ander doeleinde dan datgene dat wordt nagestreefd door de autoriteit die toegang wenst tot de betreffende gegevens[113].

149. Aangaande de **gegevens die worden bewaard krachtens het nieuwe artikel 126/1** leert een gecombineerde lezing van de artikelen 126/1 en 127/1 dat de **autoriteiten die een van de doeleinden nastreven** die zijn bedoeld in artikel 127/1 van de telecomwet **enkel toegang tot die gegevens kunnen krijgen voor de doeleinden waarvoor ze werden bewaard**, namelijk de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijk persoon.

[113] De nieuwe artikelen 122 § 7 en 123 § 6 van de telecomwet bepalen immers als volgt, elk van hun kant: "*dit artikel [namelijk respectievelijk artikel 122 en artikel 123] doet geen afbreuk aan artikel 127/1*". Het nieuwe artikel 126 § 1, derde lid, luidt als volgt: "Deze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1 " en het nieuwe artikel 127 § 1, tweede lid: "*Deze gegevens en documenten worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1"*.

150. Artikel 127/1 van de telecomwet preciseert bovendien dat de **autoriteiten enkel toegang tot de door de operatoren bewaarde gegevens kunnen krijgen volgens de voorwaarden van de bepalingen die hen daartoe machtigen**.

151. De Autoriteit formuleert **verschillende opmerkingen** over de bepalingen die de autoriteiten de mogelijkheid bieden om toegang te krijgen tot de door operatoren bewaarde gegevens.

152. Eerst en vooral wijst de Autoriteit op het feit dat het HvJ-EU oordeelde dat **de toegang tot verkeers- en locatiegegevens die door de operatoren worden bewaard in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop die bewaring werd opgelegd**. Hieruit volgt met name dat "*in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid.* ***Overeenkomstig het evenredigheidsbeginsel*** *[…],* ***kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid,*** *mits de materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen*"[114]. Het HvJ-EU vult aan als volgt: "*n zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/588*"[115]. **De wetgever kan dus bepalen dat de autoriteiten toegang tot de in toepassing van de artikelen 122 en 123 bewaarde gegevens kunnen krijgen voor andere doeleinden dan deze waarvoor ze oorspronkelijk werden bewaard, maar alleen als die latere verwerkingsdoelen de bescherming van de nationale veiligheid of de bestrijding van zware criminaliteit zijn (of een ander doel dat is vermeld in artikel 15 van de ePrivayrichtlijn en eenzelfde graad van belangrijkheid heeft)**. In zijn huidige versie laat het voorontwerp van wet een hergebruik van de in toepassing van de artikelen 122 en 123 bewaarde gegevens toe voor alle doeleinden die zijn vermeld in artikel 127/1 van de telecomwet, en niet alleen voor de doeleinden die een zekere ernst/belang hebben zoals de bestrijding van zware criminaliteit. Die mogelijkheid is niet conform de Europese eisen. **Het voorontwerp moet bijgevolg worden aangepast om er de beperking aan toe te voegen aangaande de doeleinden waarvoor een verdere verwerking van de in toepassing van de artikelen 122 en 123 bewaarde gegevens mogelijk is**.

[114] HvJ-EU, arrest van 6 oktober 2020, § 166 (vetjes toegevoegd door de Autoriteit).
[115] HvJ-EU, arrest van 6 oktober 2020, § 166 (vetjes toegevoegd door de Autoriteit).

153. Bovendien **herhaalt de Autoriteit dat de toegang tot de gegevens ondergeschikt moet zijn aan de inachtneming van de materiële en procedurele voorwaarden die zijn geïdentificeerd door het HvJ-EU**. Het voorontwerp van wet preciseert in dit verband dat de autoriteiten enkel toegang tot de gegevens kunnen krijgen "*volgens de vastgelegde voorwaarden die hen daartoe machtigen".* Het zijn dus die bepalingen die moeten voorzien in de nodige materiële en procedurele voorwaarden. **Ter herinnering, die voorwaarden zijn**:

- De betrokken nationale regeling **moet aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden toegang tot de gegevens moet worden verleend.**
- De toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens moet, in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, worden onderworpen aan een **voorafgaand toezicht** door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit. Deze rechterlijke instantie of deze entiteit moet haar beslissing geven op een met redenen omkleed verzoek van deze autoriteiten.
- De autoriteiten die toegang hebben gekregen tot de gegevens moeten **de betrokken personen daarvan op de hoogte brengen** als dat de door deze autoriteiten gevoerde onderzoeken niet in gevaar kan brengen.

154. **De wetgeving dient na te gaan of alle bepalingen die de autoriteiten machtigen om toegang te krijgen tot de door de operatoren bewaarde verkeers- en locatiegegevens voorzien in de nodige materiële en procedurele voorwaarden om aan de Europese eisen te voldoen**. De bepalingen die de toegang van de autoriteiten tot de door de operatoren bewaarde gegevens organiseren, zijn opgenomen in de organieke wetten van deze autoriteiten die doorgaans al bestaan vóór het voorontwerp van wet. Dat brengt evenwel enkele wijzigingen aan in de bepalingen die de toegang van bepaalde autoriteiten tot de door de operatoren bewaarde gegevens organiseren. De Autoriteit onderzoekt of die wijzigingen voldoen aan de eisen die voortvloeien uit de Europese rechtspraak (maar haar onderzoek beperkt zich tot de aangebrachte wijzigingen). De Autoriteit heeft daarbij vastgesteld dat het **voorontwerp van wet bepaalde autoriteiten toegang wil verlenen tot de door de operatoren bewaarde gegevens zonder te eisen dat die toegang het voorwerp moet uitmaken van een voorafgaande toestemming van een onafhankelijke bestuurlijke entiteit die de hoedanigheid van derde moet hebben** ten opzichte van de autoriteit die toegang wil krijgen tot de gegevens. Dat is met name het geval voor de volgende autoriteiten:

- Het voorontwerp bepaalt dat het BIPT "*van de operatoren identificatie-, verkeers- of locatiegegevens kan vragen in de zin van de wet van 13 juni 2005 betreffende de*

elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten" (artikel 17 van het voorontwerp van wet).

- Het voorontwerp van wet bepaalt dat het CCB, "*[w]anneer dat strikt noodzakelijk is voor de uitvoering van zijn taken opgesomd in artikel 60, a) tot e) van deze wet, […] van de operatoren als bedoeld in artikel 2, 11° van de wet van 13 juni 2005 betreffende de elektronische communicatie, identificatie-, verkeers- of locatiegegevens die door hen worden bewaard, kan verkrijgen"* (artikel 34 van het voorontwerp van wet).
- Het voorontwerp van wet bepaalt voor de statutaire of contractuele personeelsleden van de Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu: "*Zij mogen natuurlijke en rechtspersonen identificeren aan de hand van het telefoonnummer van de betrokkene of het IP-adres dat aan de bron van de elektronische communicatie ligt. Hiertoe mogen zij met gemotiveerd verzoek de verstrekking van de identificatiedocumenten en gegevens vorderen*" van de operatoren (artikel 33 van het voorontwerp van wet).
- Het voorontwerp van wet bepaalt: *"Een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kan, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood en de opsporing van personen van wie de verdwijning onrustwekkend is, en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon opvorderen*" (artikel 19 van het voorontwerp van wet).

155. De (systematische) afwezigheid van voorafgaand toezicht op de communicatie van de gegevens is niet toelaatbaar[116]. **Het voorontwerp moet worden gewijzigd om erop toe te zien dat de**

[116] Na een verzoek om verdere inlichtingen, antwoordde de afgevaardigde van de minister dat het HvJ-EU de toegang tot de gegevens niet onderwerpt aan een voorafgaande controle wanneer die toegang plaatsvindt in een andere context dan het onderzoek, de voorkoming, de opsporing of de vervolging van strafbare feiten. De Autoriteit kan zich niet aansluiten bij deze interpretatie. Het HvJ-EU heeft inderdaad de verschillende materiële en procedurele voorwaarden geïdentificeerd die van kracht zijn als de autoriteiten toegang wensen tot de gegevens die de operatoren hebben verzameld, in het kader van beslissingen aangaande de conformiteit van de nationale wetgevingen betreffende de toegang tot de verkeersgegevens voor de autoriteiten bij procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Het Hof heeft die eisen echter niet beperkt tot alleen die context. In een arrest van 21 december 2016 oordeelde het HvJ-EU immers: het is "*van wezenlijk belang dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze autoriteiten dat met name is ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten* (woorden onderlijnd door de Autoriteit). In een arrest van 2 maart 2021 oordeelde het HvJ-EU: " *De voorafgaande toetsing vereist onder meer, […], dat de rechterlijke instantie of de entiteit die belast is met die toetsing, over alle bevoegdheden beschikt en alle noodzakelijke waarborgen biedt om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht. In het specifieke geval van een strafrechtelijk onderzoek vereist een dergelijke toetsing dat die rechterlijke instantie of entiteit in staat is een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft" (woorden onderlijnd door de Autoriteit).* **Uit de onderlijnde woorden blijkt duidelijk dat het toezicht dat de toegang tot de gegevens vooraf moet gaan volgens het HvJ-EU ook een rol te vervullen heeft in andere situaties dan die waarin de toegang tot de gegevens wordt gevraagd om strafbare feiten te voorkomen, op te sporen of te vervolgen.** Het voorafgaand toezicht door een

toegang tot de gegevens, conform de Europese eisen, steeds onderworpen is aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit die de hoedanigheid heeft van derde ten opzichte van de autoriteit die de toegang tot de gegevens heeft gevraagd, **behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid[117].**

156. De Autoriteit benadrukt tevens dat de rechterlijke instantie of de onafhankelijke bestuurlijke entiteit die het voorafgaand toezicht uitvoert, moet nagaan of met de gegevensmededeling een doel wordt nagestreefd dat is toegelaten voor die mededeling. De Autoriteit herhaalt dat de mededeling van gegevens in beginsel enkel gerechtvaardigd wordt door de doelstelling van algemeen belang met het

rechterlijke instantie of een onafhankelijke administratieve entiteit wordt vereist om te waarborgen dat de autoriteiten enkel toegang krijgen tot de verkeersgegevens die hen daadwerkelijk mogen worden meegedeeld; die gegevens moeten beperkt zijn tot wat strikt noodzakelijk is voor het beoogde doel van het verzoek om toegang. Het voorafgaand toezicht is bijzonder belangrijk. De toegang tot de verkeersgegevens vormt immers een soms zeer ernstige inmenging in de privacyrechten en het recht op bescherming van de persoonsgegevens aangezien die gegevens nauwkeurige inlichtingen verschaffen over het privéleven van een gebruiker van een elektronisch communicatiemiddel, zelfs als de toegang slechts betrekking heeft op een beperkt aantal gegevens of op gegevens beperkt tot een korte periode (zie de volgende arresten van het HvJ-EU: arrest van 8 april 2014, § 62; arrest van 21 december 2021, § 118-120; arrest van 2 maart 2021, § 40). **De factoren die de noodzaak van een voorafgaand toezicht rechtvaardigen bestaan zowel wanneer de autoriteiten toegang tot de gegevens krijgen in het kader van een strafrechtelijke procedure als wanneer ze er toegang toe krijgen in een andere context**. Het bestaan van gerechtelijke verweermiddelen (*a posteriori*) kan niet volstaan om te voldoen aan de eis van voorafgaand toezicht.

[117] De afgevaardigde van de minister rechtvaardigde de afwezigheid van voorafgaand toezicht bij de toegang van een officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie tot gegevens in het kader van de opsporing van vermiste personen aan de hand van twee elementen: 1) het feit dat de Cel Vermiste Personen niet handelt in het kader van een 'strafrechtelijk' doel en 2) het feit dat vooraf toestemming moet worden gevraagd tot gevolg kan hebben dat de opsporingsdiensten uren of soms dagen tijd verliezen die vaak cruciaal zijn bij de opsporing van de betrokken persoon en voor de bescherming van zijn vitale belangen. De Autoriteit kan de aanvrager niet volgen in zijn eerste argument. Het bestaan van een behoorlijk gerechtvaardigde dringende situatie daarentegen kan rechtvaardigen dat het voorafgaand toezicht wordt overgeslagen. De wetgeving zou dus kunnen voorzien in een uitzondering op de verplichting tot voorafgaand toezicht wanneer een officier van gerechtelijke politie van de Cel Vermiste Personen toegang vraagt tot gegevens in een dringende situatie, met dien verstande dat het dan ook echt om een dringende situatie moet gaan (wat geval per geval moet worden beoordeeld). De afgevaardigde van de minister voert eenzelfde argument aan om de afwezigheid van voorafgaand toezicht te rechtvaardigen bij de toegang van het CCB tot verkeersgegevens: "Gezien d*e toename en de frequentie van incidenten inzake cybersecurity en de snelle reactie die ze vereisen, zou CCB zaken van cybercriminaliteit, bedreiging van de openbare veiligheid in verband met cybersecurity of defecten in de veiligheid van het netwerk niet tijdig kunnen voorkomen en opsporen als het systematisch eerst toestemming moet vragen van een rechterlijke instantie of een onafhankelijke nationale autoriteit om toegang te krijgen tot die elektronische communicatiegegevens"*. Opnieuw benadrukt de Autoriteit dat het bestaan van een naar behoren gerechtvaardigd geval van spoedeisendheid de afwezigheid van voorafgaand toezicht kan rechtvaardigen, maar dat moet dan *in concreto* worden beoordeeld en mag niet uit principe worden uitgevaardigd.
De afgevaardigde van de minister heeft de afwezigheid van voorafgaand toezicht bij de toegang van statutaire of contractuele personeelsleden van de FOD Volksgezondheid tot gegevens gerechtvaardigd met het argument dat de toegang beperkt is tot wat strikt noodzakelijk is om een gebruiker te kunnen identificeren en dat die gegevens als "minder gevoelig" worden aangemerkt. Ook bij dit argument kan de Autoriteit zich niet aansluiten. In het arrest dat de aanvrager inroept om zijn redenering te staven (arrest van 2 oktober 2018, *Ministerio fiscal*) was de toegang tot de identificatiegegevens onderworpen aan een voorafgaand gerechtelijk toezicht. Dat toezicht is nodig om te garanderen dat de toegang van de administratie tot de identificatiegegevens voldoet aan de wettelijke eisen (incl. noodzaak en evenredigheid). Bovendien voert de afgevaardigde van de minister aan dat" moet worden benadrukt dat die bevoegdheid is voorzien in artikel 14, c, van Verordening 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van de producten en tot wijziging van Richtlijn 2004/42/EG en de verordeningen (EG) nr.765/2008 en (EU) nr. 305/2011". De Autoriteit verwijst in dit verband naar een bepaling van de genoemde Europese Verordening: "*De markttoezichtautoriteiten oefenen hun in dit artikel vermelde bevoegdheden op efficiënte en doeltreffende wijze uit, overeenkomstig het beginsel van evenredigheid, voor zover die uitoefening verband houdt met het voorwerp, en het doel van de maatregelen en de aard en de werkelijke of potentiële schade die voortvloeit uit het geval van non-conformiteit. Bevoegdheden worden toegekend en uitgeoefend overeenkomstig het Unie- en het nationale recht, waaronder de beginselen van het Handvest van de grondrechten van de Europese Unie en de nationaalrechtelijke beginselen inzake de vrijheid van meningsuiting en de vrijheid en de pluriformiteit van de media, de toepasselijke procedurele waarborgen en de regels van de Unie inzake gegevensbescherming, in het bijzonder Verordening (EU) 2016/679.* De uitoefening van de bevoegdheid om "*marktdeelnemers te gelasten relevante informatie te verstrekken die nodig is om de eigendom van websites te kunnen nagaan wanneer de informatie in kwestie verband houdt met het voorwerp van het onderzoek*" onderwerpen aan een voorafgaand toezicht wordt door Verordening 2019/1020 toegestaan omdat het verplicht is krachtens het recht op bescherming van de persoonsgegevens zoals het door het HvJ-EU wordt geïnterpreteerd in zijn arresten aangaande de bewaring van verkeersgegevens.

oog waarop de verplichting tot bewaring werd opgelegd, tenzij de wet, in overeenstemming met het evenredigheidsbeginsel, een mededeling voor andere doeleinden toelaat. De rechterlijke instantie of de onafhankelijke bestuurlijke entiteit moet bovendien toezien op de evenredigheid van de gegevensmededeling alvorens ze toe te staan.

157. Aangaande de mogelijkheid voor het BIPT om toegang te krijgen tot de verkeersgegevens nodig voor de vervulling van zijn opdrachten, stelt de memorie van toelichting dat die toegang nodig is, bijvoorbeeld om voor het BIPT de controle mogelijk te maken van "*de inachtneming door de operatoren van hun wettelijke verplichtingen zoals de verplichting om een gedetailleerde facturering op te stellen, vastgelegd in artikel 110 van de wet van 13 juni 2005 betreffende de elektronische communicatie, of in het kader van de tenuitvoerbrenging van artikel 114 van diezelfde wet. Zo moet het BIPT, in het geval van de gedetailleerde facturering, in staat zijn om een operator een staal van zijn facturen te vragen. Deze facturen bevatten verkeersgegevens, zoals de ontvangers, data, tijdstippen en duur van de gevoerde gesprekken.*" Om de voorzienbaarheid van de wet te waarborgen en toe te zien op de noodzaak en de evenredigheid van de inmenging die wordt veroorzaakt door de toegang tot verkeersgegevens, **moet het voorontwerp van wet uitdrukkelijk de opdrachten identificeren waarvoor het BIPT toegang kan krijgen tot de door de operatoren bewaarde verkeersgegevens**;

14) Bijzondere regels die het voorontwerp van wet invoert aangaande het gebruik van versleuteling in het domein van elektronische communicatie

158. Volgens het nieuwe artikel 127/5 § 1 van de telecomwet "*is het verboden om een dienst of een toestel aan te bieden of te gebruiken waardoor de uitvoering van de volgende handelingen wordt verhinderd:*
1° noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of de verstrekking van de identificatiegegevens van de oproeper;
2° de identificatie van de eindgebruiker, het opsporen en lokaliseren van privécommunicatie onder de voorwaarden bepaald door het Wetboek van Strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;
3° het afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie onder de voorwaarden bepaald door het Wetboek van Strafvordering en door de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten".

159. Dat verbod staat al (deels) in de huidige versie van de telecomwet (zie het huidige artikel 127 van de telecomwet).

160. Het nieuwe artikel 127/5 § 2 van de telecomwet voorziet in **afwijkingen van het beginsel *"het gebruik van versleuteling is vrij"***[118]:

- Het is verboden om een versleutelingssysteem aan te bieden of te gebruiken dat de noodcommunicatie verhindert (nieuw artikel 127/5 § 2, tweede lid van de telecomwet).
- De versleutelingssystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van de betalingen te waarborgen, mogen niet verhinderen dat de operator voor de autoriteiten identificatie-, verkeers- of locatiegegevens bewaart (nieuw artikel 127/5 § 2, derde lid van de telecomwet).
- Wanneer een operator een versleutelingssysteem heeft ingesteld dat kan worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van de betalingen te waarborgen, moet hij binnen 24 uur na verzending van het verzoekschrift de wettelijke maatregelen tot onderschepping mogelijk, in het bijzonder de identificatie van de eindgebruiker, het opsporen en lokaliseren van privécommunicatie en het afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie. De operator maakt de uitvoering van die handelingen enkel mogelijk voor de communicatie waarop het verzoekschrift slaat alsook voor de communicatie die daarna volgt (nieuw artikel 127/5 § 2, vierde en vijfde lid van de telecomwet).

161. De Autoriteit wenst **twee fundamentele opmerkingen** te maken over deze verbodsbepalingen.

162. In de eerste plaats vormt het verbod op het gebruik van systemen die de identificatie van de eindgebruiker kunnen verhinderen, het traceren en lokaliseren van niet openbaar beschikbare communicatie en het bewaren van identificatie-, verkeers- of locatiegegevens een **onevenredige aantasting** van het recht op eerbiediging van het privéleven van de betrokkenen, en gaat het dus verder dan wat in een democratische samenleving noodzakelijk is. **Het voorontwerp van wet zal worden herzien om dit verbod te schrappen.**

163. Ten tweede benadrukt de Autoriteit dat het nieuwe artikel 127/5, § 2, van de telecomwet, door van operatoren die een versleutelingssysteem opzetten te eisen dat zij rechtmatige interceptiemaatregelen mogelijk maken, in het bijzonder de identificatie van de eindgebruiker, het traceren en lokaliseren van communicatie en het afluisteren, opnemen en loggen van niet voor het publiek toegankelijke communicatie, de facto de invoeging van "achterdeurtjes" ("backdoors") in versleutelde systemen oplegt om de versleutelde berichten te kunnen ontcijferen. De Autoriteit

[118] Dit beginsel wordt momenteel bekrachtigd door artikel 48 van de telecomwet. Na goedkeuring van de wet tot omzetting van het EWEC zal het worden bekrachtigd door het nieuwe artikel 105/4 van de telecomwet (dat het huidige artikel 48 van de telecomwet overneemt).

merkt op dat er sinds de jaren negentig in de wetenschappelijke gemeenschap een sterke consensus bestaat dat het inbouwen van "achterdeurtjes" ("backdoors") in versleutelde systemen meer risico's inhoudt voor de privacy van de betrokken personen en voor de hogere belangen van staten dan dat het voordelen oplevert voor de bestrijding van zware criminaliteit[119]. **Het wetsontwerp moet derhalve worden herzien in die zin dat operatoren die een versleutelingssysteem opzetten, niet langer verplicht zijn om wettelijk toegestane interceptiemaatregelen mogelijk te maken**. Het is waar dat encryptiesystemen de toegang tot de inhoud van communicatie moeilijker hebben gemaakt dan vroeger. De Autoriteit benadrukt echter dat er nu al veel "digitale" informatie beschikbaar is op de eindapparatuur van de gebruikers (logboeken, cookies, flashgeheugen dat niet kan worden gewist, enz.), bij de operatoren (gegevens die bijvoorbeeld voor de facturering worden verzameld) en in de openbare ruimte (bewakingscamera's, ANPR-camera's, enz.). De Autoriteit wijst er voorts op dat de autoriteiten, indien nodig ter bestrijding van zware criminaliteit, telefoontoestellen kunnen "hacken" terwijl deze in gebruik zijn (Encrochat, SKY ECC, Hacking-team, NSO-groep, enz.) of speciale onderzoekstechnieken kunnen toepassen (zoals infiltratie, observatie met technische middelen, gebruik van indicatoren, enz.) De Autoriteit merkt op dat deze verschillende middelen, waarover de handhavingsautoriteiten beschikken, het ongetwijfeld gemakkelijker maken om zware criminaliteit te bestrijden dan voorheen en dat er in ieder geval geen bewijs is van het tegendeel. Onder deze voorwaarden - en met name gezien de risico's van het "afluisteren" van burgers, met inbegrip van politici (zoals Angela Merkel gedurende vijf jaar is geweest) of bedrijfsleiders, door derde landen - **dringt de Autoriteit erop aan dat de aanvrager de uitzonderingen op het beginsel dat "het gebruik van versleuteling vrij is", intrekt**.

15) Slotopmerking

164. Artikel 1 van het besluit van 19 september 2013 bepaalt als volgt: "*Dit besluit voorziet in een gedeeltelijke omzetting van Richtlijn 2006/24/CE van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG ("dataretentierichtlijn") (PbEG 13 april 2006, L 105/54) en van artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector*

[119] Zie bijvoorbeeld, The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W (1997), Keys under doormats, https://www.lawfareblog.com/keys-under-doormats-mandating-insecurity (2015); US National Academies, Decrypting the Encryption Debate, https://www.nap.edu/read/25010/chapter/1 (2018); https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf; https://www.vice.com/en/article/8qxwda/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption; https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate; https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/; https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

elektronische communicatie ("richtlijn betreffende privacy en elektronische communicatie") (PbEG 31 juli 2002, L 201/37)". De Autoriteit stelt vast dat die bepaling nog verwijst naar Richtlijn 2006/24 terwijl het HvJ-EU die in 2014 ongeldig heeft verklaard. **Het besluit van 19 september 2013 moet worden gewijzigd om die verwijzing naar een ongeldige richtlijn te schrappen.**

OM DIE REDENEN,

Oordeelt de Autoriteit dat de volgende aanpassingen moeten worden aangebracht in het voorontwerp van wet en in het ontwerpbesluit:

- De noodzaak en evenredigheid van de verplichting tot bewaring van de locatie- en andere verkeersgegevens nodig voor het opsporen en analyseren van een vermoed geval van fraude of een vermoed geval van kwaadwillig gebruik van het elektronisch communicatienetwerk onderwerpen aan een strikte analyse en het ontwerp in die zin aanpassen en/of de relevante rechtvaardiging opnemen in de memorie van toelichting (punt 67-69)

- Indien de wetgever na die analyse meent dat het strikt noodzakelijk en evenredig is om een verplichting tot bewaring van de verkeersgegevens op te leggen voor de bestrijding van fraude en kwaadwillig gebruik van het netwerk, moeten de volgende aanpassingen worden aangebracht:
  - De precieze gegevens bepalen die moeten worden bewaard in toepassing van die verplichting of de Koning verplichten om die gegevens te bepalen (punt72)
  - Preciseren dat de mogelijkheid om de gegevens na de minimumtermijn van 4 maanden te bewaren betrekking heeft op situaties waarin een langere bewaartijd nodig is om een geschil betreffende fraude of kwaadwillig gebruik van het netwerk te beheren (punt 73)

- De noodzaak en evenredigheid van de verplichting tot bewaring van de locatie- en andere verkeersgegevens nodig om de veiligheid en de correcte werking van de netwerken en diensten voor elektronische communicatie te garanderen onderwerpen aan een strikte analyse en het ontwerp in die zin aanpassen en/of de relevante rechtvaardiging opnemen in de memorie van toelichting (punt 78-80)

- Indien de wetgever na die analyse meent dat het strikt noodzakelijk en evenredig is om een verplichting tot bewaring van de verkeersgegevens op te leggen om de veiligheid en de correcte werking van de netwerken en diensten voor elektronische communicatie te garanderen, moeten de volgende aanpassingen worden aangebracht:
  - De precieze gegevens bepalen die moeten worden bewaard in toepassing van die verplichting of de Koning verplichten om die gegevens te bepalen (punt 82)
  - Beoordelen en, in voorkomend geval, rechtvaardigen waarom een bewaarduur van 12 maanden aangewezen is (punt 83)
  - Preciseren dat de mogelijkheid om de gegevens na de termijn van 12 maanden te bewaren betrekking heeft op situaties waarin een langere bewaarperiode nodig is om een geschil betreffende een aanslag of handelingen die de veiligheid van het netwerk of de correcte werking van de dienst in gevaar brengen te beheren (punt 83)

- Preciseren dat deze wettelijke verplichting die wordt vermeld in de artikelen 122 § 4/2 en 123 enkel kan worden opgelegd door een formele wetgevende norm (punt 85-89)

- De noodzaak en evenredigheid van de verplichting tot bewaring van de andere locatiegegevens dan verkeersgegevens voor de verschillende doelen die zijn geïdentificeerd door het nieuwe artikel 123 van de telecomwet onderwerpen aan een strikte analyse en het ontwerp in die zin aanpassen en/of de relevante rechtvaardiging opnemen in de memorie van toelichting (punt 87-88)

- In voorkomend geval ten minste de voorwaarden bepalen waaronder de operatoren de andere locatiegegevens dan verkeersgegevens mogen bewaren en verwerken, evenals de maximale bewaarduur van deze gegevens (punt 88)

- Bepalen dat de IP-adressen toegewezen aan de bron van de verbinding enkel mogen worden bewaard met het oog op bijzonder belangrijkste doelstellingen (punt 97,100)

- Verduidelijken dat alleen IP-adressen die zijn toegewezen aan de bron van een verbinding, en niet IP-adressen die zijn toegewezen aan de bestemming van een communicatie, mogen worden bewaard op grond van het nieuwe artikel 126 van de telecomwet (punt 100)

- Bepalen dat het preventief en systematisch bewaren van de identificatienummers van de eindapparaten van de eindgebruikers enkel wordt opgelegd om een doelstelling van bijzonder belang (zoals de bestrijding van zware criminaliteit) na te streven, dat de bewaarduur strikt beperkt is tot die doelstelling en de strikte voorwaarden en waarborgen bepalen voor het gebruik van die gegevens (punt 102)

- De mogelijkheid schrappen voor de operatoren om voor de identificatie van hun abonnees gebruik te maken van de gezichtsherkenningstechniek (of een andere techniek op basis van het gebruik van biometrische gegevens) (punt 104)

- De door de operator te verzamelen en te bewaren identificatiegegevens en -documenten bepalen of de Koning verplichten om die gegevens en documenten te bepalen (punt 105)

- Het begrip "communicatiegegevens" bepalen (punt 109)

- Het begrip "gegevens van oproeppogingen zonder resultaat" bepalen of die uitdrukking vervangen door de uitdrukking "verkeersgegevens van de oproeppogingen zonder resultaat" (punt 110)
- In het besluit van 19 september de woorden "ten minste" schrappen opdat dit besluit een volledige opsomming zou geven van de gegevens die de operatoren moeten bewaren in uitvoering van het nieuwe artikel 126/1 van de telecomwet (punt 113)

- Ervoor zorgen dat de drempel die wordt weerhouden om een zone aan te merken als bijzonder blootgesteld aan feiten van zware criminaliteit de facto niet kan leiden tot een verplichting tot algemene en ongedifferentieerde bewaring van de gegevens op (bijna) het hele nationale grondgebied (punt 117)

- Erop toezien dat de nadere regels om te bepalen of een zone bijzonder blootgesteld is aan feiten van zware criminaliteit passend zijn (punt 122-124)

- Erop toezien dat de keuze van plaatsen die worden weerhouden om er een gerichte preventieve bewaring van gegevens op te leggen voldoet aan de eisen van noodzaak en evenredigheid (punt 125)

- De machtiging aan de Koning om andere plaatsen toe te voegen dan deze die zijn opgesomd in het voorontwerp van wet schrappen (punt 125)

- Aanvulling van de gegevens die moeten worden opgenomen in het jaarlijks verslag dat de minister van Telecommunicatie en de minister van Justitie aan de Kamer moeten voorleggen (punt 126-127)

- Preciseren dat onder de "gegevens" de "gegevens bedoeld in §2" moet worden verstaan (punt 128)

- De mogelijkheid schrappen die de operatoren wordt geboden om gegevens te bewaren van buiten de geografische zones waarbinnen het voorontwerp van wet voorziet in een bewaarplicht wanneer het voor hen technisch niet mogelijk is om de gegevensbewaring te beperken tot die zones (punt 129-130)

- De formulering van de aanduiding van de verwerkingsverantwoordelijke aanpassen (punt 132)

- Bepalen dat alle door de operatoren bewaarde gegevens worden bewaard op het grondgebied van de Unie (punt 136)

- Bepalen dat de volgende gegevens moeten worden opgenomen in het logboek:
  - ✓ Het concrete doel waarvoor de toegang tot de gegevens wordt gevraagd, met dien verstande dat dit doel "omfloerst" moet worden opgetekend (punt 137)
  - ✓ Elke handeling in het logboek (punt 137)

- De reikwijdte verduidelijken van het nieuwe artikel 127/2 § 2, eerste en laatste lid (punt 139-140)

- De begrippen "aanbieders van private elektronische communicatienetwerken" en "aanbieders van elektronische communicatiediensten die niet openbaar beschikbaar zijn" definiëren (punt 143)

- Bepalen dat de autoriteiten toegang tot de in toepassing van de artikelen 122 en 123 bewaarde gegevens kunnen krijgen voor andere doeleinden dan deze waarvoor ze oorspronkelijk werden bewaard, maar alleen als die latere verwerkingsdoelen de bescherming van de nationale veiligheid of de bestrijding van zware criminaliteit betreffen (of een ander doel dat is vermeld in artikel 15 van de ePrivacyrichtlijn en eenzelfde graad van belangrijkheid heeft) (punt 152)

- De relevante bepalingen aanpassen om erop toe te zien dat de toegang tot de gegevens, conform de Europese eisen, steeds onderworpen is aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit die de hoedanigheid heeft van derde ten opzichte van de autoriteit die de toegang tot de gegevens heeft gevraagd, behalve in de gevallen van naar behoren gerechtvaardigde spoedeisendheid (punt 153-155)

- Uitdrukkelijk de opdrachten specificeren waarvoor het BIPT toegang kan krijgen tot de door de operatoren bewaarde verkeersgegevens (punt157).

- Schrapping van het verbod op het gebruik van systemen die de identificatie, tracering en plaatsbepaling van niet-openbaar beschikbare communicatie door de eindgebruiker en de bewaring van identificatie-, verkeers- of locatiegegevens kunnen verhinderen (punt 162)

- Schrapping van de verplichting voor operatoren die een versleutelingssysteem opzetten om legale interceptiemaatregelen mogelijk te maken (punt 163)

- In het besluit van 19 september 2013 de verwijzing naar Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG schrappen aangezien het HvJ-EU deze richtlijn ongeldig heeft verklaard (punt 164).

De Autoriteit vestigt de aandacht op de volgende factoren:

- De wetgeving dient na te gaan of alle bepalingen die de autoriteiten machtigen om toegang te krijgen tot de door de operatoren bewaarde verkeers- en locatiegegevens

voorzien in de nodige materiële en procedurele voorwaarden om aan de Europese eisen te voldoen (punt 154)

- De rechterlijke instantie of de onafhankelijke bestuurlijke entiteit die het toezicht uitvoert dat een communicatie van de gegevens voorafgaat, moet nagaan of met die communicatie een van de toegelaten doeleinden wordt nagestreefd en of ze voldoet aan het evenredigheidsbeginsel (punt 156)

Voor het Kenniscentrum,
(get.) Alexandra Jaspar, Directeur

BIJLAGE I

Executive Summary

De minister van Justitie, de heer Vincent Van Quickenborne, vroeg op 7 mei 2021 het advies van de Autoriteit over een voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten (hierna "het voorontwerp van wet") en over een ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna "het ontwerp van besluit").

Het voorontwerp van wet beoogt tegemoet te komen aan de vernietiging van de wet van 29 mei 2016 *betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie.* Op 21 april 2021 vernietigde het Grondwettelijk Hof deze wet van 29 mei 2016, die in beginsel was gebaseerd op een veralgemeende en ongedifferentieerde verplichting om verkeers- en locatiegegevens van gebruikers van elektronische communicatiemiddelen te bewaren. Het Grondwettelijk Hof, waarvan de motivering grotendeels verwijst naar het arrest van het Hof van Justitie van de Europese Unie (HJEU) van 6 oktober 2020 (het " Quadrature du Net "-arrest), is evenwel van oordeel **dat de verplichting om gegevens met betrekking tot elektronische communicaties te bewaren de uitzondering moet zijn, en niet de regel.** In zijn arrest herinnert het Grondwettelijk Hof eraan dat "*het aan de wetgever staat, in het licht van de rechtspraak van het Hof van Justitie een regeling uit te werken die de beginselen eerbiedigt die van toepassing zijn op de bescherming van persoonsgegevens, en in voorkomend geval rekening te houden met de verduidelijkingen die het Hof heeft aangebracht met betrekking tot de verschillende soorten wetgevingsmaatregelen die verenigbaar worden geacht met [de ePrivacyrichtlijn, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie]".*

Het voorontwerp van wet beoogt de invoering van een bewaarsysteem voor communicatiemetadata dat voldoet aan de eisen van het Europees recht, zoals geïnterpreteerd door het HvJEU (voor een overzicht van dit systeem, zie de tabel in Bijlage II). **Er zij echter op gewezen dat het voorontwerp van wet niet echt de perspectiefwijziging inhoudt als vereist door de jurisprudentie van het HvJEU en het Grondwettelijk Hof.** In haar advies merkt de Autoriteit op dat het voorontwerp van wet voornemens is nieuwe maatregelen voor de bewaring van verkeers- en locatiegegevens op te leggen, hetgeen zou kunnen leiden tot de feitelijke herinvoering van veralgemeende en ongedifferentieerde verplichtingen inzake gegevensbewaring, terwijl tegelijkertijd de mogelijkheden voor toegang tot dergelijke gegevens worden uitgebreid. **Het is waar dat de bewaring van metagegevens noodzakelijk kan zijn om het recht op veiligheid van personen te waarborgen, dat evenals het recht op bescherming van de persoonlijke levenssfeer en van persoonsgegevens een grondrecht is dat is verankerd in de Belgische Grondwet, het Europees Verdrag tot bescherming van de rechten van de mens en het Handvest van de grondrechten van de Europese Unie.** Het recht op veiligheid schept

positieve verplichtingen voor de staat om materiële en procedurele maatregelen te nemen om strafbare feiten tegen personen doeltreffend te bestrijden door middel van doeltreffende opsporing en vervolging. Het HvJEU erkent de noodzaak om deze verschillende grondrechten met elkaar te verzoenen. **De Autoriteit verzoekt de wetgever de tijd te nemen om na te denken en grondig te analyseren hoe, overeenkomstig de Europese jurisprudentie, het grondrecht op veiligheid en het recht op een doeltreffende voorziening in rechte in geval van strafbare feiten die deze veiligheid aantasten, enerzijds, en het grondrecht op eerbiediging van het privéleven en op bescherming van persoonsgegevens, anderzijds, met elkaar kunnen worden verzoend.** De Autoriteit dringt er bij de wetgever op aan het voorontwerp van wet aan te passen om ervoor te zorgen dat de aan te nemen wet voldoet aan alle door het HJEU en het Grondwettelijk Hof opgelegde vereisten. Een nieuwe nietigverklaring van de wet door het Grondwettelijk Hof zou het vertrouwen van de burgers in de democratische instellingen waarschijnlijk ondermijnen. **Het is daarom van cruciaal belang ervoor te zorgen dat het voorontwerp van wet niet *de jure* of *de facto* opnieuw een veralgemeende en ongedifferentieerde verplichting invoert om de verkeers- of locatiegegevens te bewaren van alle of een te groot deel van de gebruikers van elektronische communicatie in België.** In haar advies heeft de Autoriteit een groot aantal opmerkingen over het voorontwerp van wet, waarin wordt gewezen op de aanpassingen die moeten worden aangebracht om te waarborgen dat de ontwerpregeling voldoet aan de vereisten van het recht op bescherming van persoonsgegevens, zoals geïnterpreteerd door het HJEU.

Voorts stelt **de Autoriteit met bezorgdheid vast dat het voorontwerp van wet voorziet in een verplichting voor operatoren die een versleutelingssysteem opzetten, om rechtmatige interceptiemaatregelen mogelijk te maken**, met name de identificatie van de eindgebruiker, het traceren en lokaliseren van niet voor het publiek toegankelijke communicatie, en het aftappen en opnemen van niet voor het publiek toegankelijke communicatie. Sinds de jaren negentig bestaat er in de wetenschappelijke gemeenschap een consensus dat het inbouwen van "achterdeurtjes" (" backdoors") in versleutelingssystemen meer risico's inhoudt voor de persoonlijke levenssfeer van de betrokken personen en voor de belangen van de staten dan dat het voordelen oplevert voor de bestrijding van zware criminaliteit. **De Autoriteit is ook bezorgd over de invoering van een gegevensverzamelingsplicht door diensten, zoals de versleutelde berichtendiensten, die tot dusver om legitieme veiligheids- en privacyredenen hebben vermeden om dergelijke gegevens te verzamelen**.

81

BIJLAGE II

Overzichtstabel van preventieve retentiemaatregelen voor verkeers- en locatiegegevens

RECHTSGROND	WIE MOET BEWAREN?	MACHTIGING OF VERPLICHTING OM GEGEVENS TE BEWAREN	TE BEWAREN GEGEVENSCATEGORIEËN	OMSCHRIJVING VAN DE TE BEWAREN GEGEVENS	OORSPRONKELIJK DOEL VAN DE GEGEVENSBEWARING	AUTORITEIT(EN) MET TOEGANG TOT DE GEGEVENS EN DOEL(EN) DIE DEZE TOEGANG KUNNEN RECHTVAARDIGEN
Art. 122 §2 van de telewomwet (nieuw)	Alle operatoren	Machtiging	Verkeersgegevens die nodig zijn voor de facturering van abonnees of voor interconnectiebetalingen	Nee - er is geen gedetailleerde lijst van gegevens (noch in de wet, noch in een KB) Maar de operator moet de abonnees informeren over de gegevens die worden verwerkt	Facturen van abonnees opstellen en interconnecties betalen	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden
Art. 122, §3, 3 van de telecomwet (nieuw)	Alle operatoren	Machtiging, maar toestemming (in de zin van de AVG) van de abonnee vereist vóór verwerking	Verkeersgegevens, met inbegrip van locatiegegevens	Nee - er is geen gedetailleerde lijst van gegevens (noch in de wet, noch in een KB)	Marketing van eigen elektronische-communicatiediensten en profilering van abonnee- of eindgebruikersgebruik	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden

				Maar de operator moet de abonnees informeren over de gegevens die worden verwerkt		
Art. 122, §4 van de telecomwet (nieuw)	Alle operatoren	Verplichting (nieuw in het voorontwerp)	Locatiegegevens en andere verkeersgegevens die nodig zijn om vermoedelijke fraude of kwaadwillig gebruik van het netwerk op te sporen en te analyseren	Geen gedetailleerde lijst in het voorontwerp, maar facultatieve delegatie aan de koning, die kan - maar niet hoeft - te bepalen welke gegevens op grond van deze bepaling moeten worden bewaard	Vermoedens van fraude of kwaadwillig gebruik van het netwerk opsporen en analyseren	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden
Art. 122 §4/1 van de telecomwet (nieuw)	Alle operatoren	Verplichting (nieuw in het voorontwerp)	Verkeersgegevens die nodig zijn om de veiligheid en de goede werking van het elektronische-communicatienetwerk en de elektronische-communicatiediensten te waarborgen	Geen gedetailleerde lijst in het voorontwerp en geen delegatie aan de Koning om te bepalen welke gegevens moeten worden bewaard	De veiligheid en de goede werking van het elektronische-communicatienetwerk en de elektronische-communicatiediensten te garanderen, en met name een potentiële of feitelijke inbreuk op de veiligheid op te sporen en te analyseren, met inbegrip van het opsporen van de	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden

					oorsprong van de inbreuk	
Art. 123 van de telecomwet (nieuw)	Operatoren en mobiele netwerken	Machtiging (toestemming van de abonnee in sommige gevallen vereist)	Andere locatiegegevens dan verkeersgegevens	Geen gedetailleerde lijst in het voorontwerp en geen delegatie aan de Koning om te bepalen welke gegevens moeten worden bewaard	Goede werking en beveiliging van het netwerk/de dienst Vermoedens van fraude of kwaadwillig gebruik van het netwerk opsporen en analyseren Noodzakelijk om een dienst met toegevoegde waarde te verlenen (toestemming vereist)	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden
Art. 126 van de telecomwet (nieuw)	Operatoren die elektronische-communicatiediensten aanbieden aan eindgebruikers & operatoren die de onderliggende elektronische-communicatienetwerken leveren	Verplichting	Abonnementsgegevens van de abonnee en technische gegevens die nodig zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, met uitzondering van gegevens die betrekking hebben op één enkele elektronische communicatie	Delegatie aan de Koning om te bepalen welke gegevens precies moeten worden bewaard Cf. nieuwe artikelen 3§1, 4§1, 5§1 en 6§1 van het Koninklijk Besluit van 19/09/2013	Bewaring voor de autoriteiten en de doeleinden vermeld in artikel 127/1 van de telecomwet (opgesomd in de rechterkolom)	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden

Art. 126/1 van het wetsvoorstel: (nieuw)	Operatoren die elektronische-communicatiediensten aanbieden aan eindgebruikers & operatoren die de onderliggende elektronische-communicatienetwerken leveren	Doelgerichte verplichting op basis van geografische criteria	Gegevens betreffende de toegang tot en de aansluiting van de eindapparatuur op het netwerk en de dienst en de locatie van die apparatuur, met inbegrip van het netwerkaansluitpunt Communicatiegegevens, met uitzondering van inhoud, inclusief herkomst en bestemming Gegevens mislukte oproepen	Delegatie aan de Koning om te bepalen welke gegevens precies moeten worden bewaard Cf. nieuwe artikelen 3§2, 4§2, 5§2 en 6§2 van het Koninklijk Besluit van 19/09/2013	Vrijwaring van de nationale veiligheid Bestrijding van zware criminaliteit, Preventie van ernstige bedreigingen van de openbare veiligheid Vrijwaring van de vitale belangen van een natuurlijke persoon;	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden Maar toegang tot dergelijke gegevens is alleen mogelijk indien die toegang een van de volgende doelen dient : de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid en de vrijwaring van vitale belangen van een natuurlijk persoon.
Art. 127 van de telecomwet (nieuw)	Alle operatoren	Verplichting	Gegevens die nodig zijn voor de autoriteiten die het recht hebben de identiteit van de abonnees van de operatoren te verkrijgen, om hen te identificeren	Geen gedetailleerde lijst in het voorontwerp, maar facultatieve delegatie aan de koning, die kan - maar niet hoeft -	Bewaring voor de autoriteiten en de doeleinden vermeld in artikel 127/1 van de telecomwet (opgesomd in de rechterkolom)	De in artikel 127/1 van de telecomwet opgesomde autoriteiten en doeleinden

				te bepalen welke gegevens op grond van deze bepaling moeten worden bewaard [Het AR van 9/19/2013 voert deze bepaling niet uit].		

Het nieuwe artikel 127/1 van de telecomwet bepaalt welke autoriteiten toegang hebben tot de gegevens die de telecomoperatoren ter uitvoering van de telecomwet hebben opgeslagen en welke doeleinden die toegang kunnen rechtvaardigen. Het gaat om de volgende autoriteiten en doeleinden :

1° de handhavingsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten ;

2° de inlichtingen- en veiligheidsdiensten voor de uitvoering van hun wettelijke opdrachten ;

3° de autoriteiten die belast zijn met het verlenen van bijstand aan personen ;

4° het BIPT voor de uitoefening van zijn wettelijke opdrachten;

5° de instanties die belast zijn met het onderzoek naar een storing in de veiligheid van het netwerk of de dienst

De toegang tot de gegevens geschiedt overeenkomstig de voorwaarden die zijn vastgesteld in de organieke wetten van de verschillende in artikel 127/1 van de telecommunicatiewet genoemde autoriteiten.