DOC 55 **2572/002**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

16 mai 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

AMENDEMENTS

Voir:

Doc 55 **2572/ (2021/2022)**:
001: Projet de loi.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

16 mei 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

AMENDEMENTEN

Zie:

Doc 55 **2572/ (2021/2022)**:
001: Wetsontwerp.

N° 1 **DU GOUVERNEMENT**

Art. 8

Remplacer l'article 126 proposé 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 suivantes, pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture de ces réseaux ou services:

1° le numéro de Registre national ou un numéro équivalent, le nom et le prénom de l'utilisateur final qui est une personne physique ou la dénomination de l'abonné qui est une personne morale;

2° l'alias éventuel choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service;

3° les coordonnées de contact de l'abonné qui ont été fournies lors de la souscription au service, notamment son numéro de téléphone, son adresse e-mail et son adresse postale;

4° la date et l'heure de la souscription au service et de l'activation du service et les éléments permettant de déterminer le lieu à partir duquel cette souscription et cette activation ont été effectuées, à savoir notamment:

— l'adresse physique du point de vente où la souscription ou l'activation ont eu lieu, ou;

— l'adresse physique du point de terminaison du réseau ayant servi à la souscription ou à l'activation, ou;

— l'adresse IP ayant servi à la souscription ou à l'activation ainsi que le port source de la connexion et l'horodatage, ou;

Nr. 1 **VAN DE REGERING**

Art. 8

Het voorgestelde artikel 126 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 aanbieden, alsook de operatoren die de elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de volgende gegevens, voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten:

1° het Rijksregisternummer of een equivalent nummer, de naam en voornaam van de eindgebruiker die een natuurlijke persoon is of de naam van de abonnee die een rechtspersoon is;

2° de eventuele alias gekozen door de eindgebruiker bij de inschrijving op of de activering van de dienst;

3° de contactgegevens van de abonnee die verstrekt zijn bij de inschrijving op de dienst, met name zijn telefoonnummer, zijn e-mailadres en zijn postadres;

4° de datum en het tijdstip van inschrijving op de dienst en van de activering van de dienst en de elementen aan de hand waarvan de plaats kan bepaald worden waarvandaan die inschrijving en die activering zijn uitgevoerd, met name:

— het fysieke adres van het verkooppunt waar de inschrijving of activering heeft plaatsgevonden, of;

— het fysieke adres van het netwerkaansluitpunt dat gediend heeft voor de inschrijving of de activering, of;

— het IP-adres dat gediend heeft voor de inschrijving of de activering, alsook de bronpoort van de verbinding en het tijdstempel, of;

— dans le cadre d'un réseau téléphonique mobile, la localisation géographique de l'équipement terminal qui a permis la souscription ou l'activation au moyen d'un numéro de téléphone;

5° l'adresse physique de livraison du service;

6° l'adresse de facturation du service et les données relatives au type et au moyen de paiement, à la date des paiements, et la référence de l'opération de paiement en cas de paiement en ligne;

7° le service principal et les services annexes que l'abonné peut utiliser;

8° la date à partir de laquelle ces services peuvent être utilisés, la date de la première utilisation de ces services et la date de fin de ces services;

9° en cas de transfert de l'identifiant de l'abonné, tel son numéro de téléphone, l'identité de l'opérateur qui transfère l'identifiant et l'identité de l'opérateur auquel l'identifiant est transféré et la date à laquelle le transfert est effectué;

10° le numéro de téléphone attribué;

11° l'adresse de messagerie principale et les adresses de messagerie employées comme alias;

12° l'identité internationale d'abonné mobile ("International Mobile Subscriber Identity", "IMSI");

13° l'identifiant permanent d'abonnement ("Subscription Permanent Identifier", "SUPI");

14° l'identifiant caché d'abonnement ("Subscription Concealed Identifier" "SUCI");

15° l'adresse IP à la source de la connexion, l'horodatage de l'attribution ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, les ports qui lui ont été attribués;

— in het kader van een mobiel telefoonnetwerk, de geografische locatie van de eindapparatuur die de inschrijving of de activering aan de hand van een telefoonnummer mogelijk heeft gemaakt;

5° het fysieke leveringsadres van de dienst;

6° het facturatieadres van de dienst en de gegevens betreffende de betalingswijze en het betaalmiddel, het tijdstip van de betalingen en de referentie van de betalingstransactie in geval van onlinebetaling;

7° de hoofddienst en de aanvullende diensten die de abonnee kan gebruiken;

8° de datum vanaf wanneer die diensten gebruikt kunnen worden, de datum van het eerste gebruik van die diensten en de datum van beëindiging van die diensten;

9° in geval van overdracht van de identifier van de abonnee, zoals zijn telefoonnummer, de identiteit van de operator die de identifier overdraagt en de identiteit van de operator naar wie de identifier wordt overgedragen en de datum waarop de overdracht wordt uitgevoerd;

10° het toegewezen telefoonnummer;

11° het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden;

12° de internationale identiteit van de mobiele abonnee ("International Mobile Subscriber Identity", "IMSI");

13° de permanente identifier van het abonnement ("Subscription Permanent Identifier", "SUPI");

14° de verdoken identifier van het abonnement ("Subscription Concealed Identifier" "SUCI");

15° het IP-adres aan de bron van de verbinding, het tijdstempel van de toewijzing alsook, in geval van gedeeld gebruik van een IP-adres van de eindgebruiker, de poorten die daaraan zijn toegewezen;

16° l'identifiant de l'équipement terminal de l'utilisateur final, ou lorsque l'opérateur ne le traite pas ou ne le génère pas, l'identifiant de l'équipement qui est le plus proche de cet équipement terminal, à savoir notamment:

— l'identité internationale d'équipement mobile ("International Mobile Equipment Identity", "IMEI");

— l'identifiant permanent de l'équipement ("Permanent Equipment Identifier", "PEI");

— l'adresse du contrôleur d'accès au réseau ("Media Access Control address", "MAC");

17° les autres identifiants relatifs à l'utilisateur final, à l'équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Les opérateurs ne doivent pas conserver les adresses MAC visées à l'alinéa 1er, 16°, troisième tiret, pour les services de communications électroniques qu'ils offrent uniquement à des entreprises ou à des personnes morales.

L'arrêté royal visé à l'alinéa 1er, 17°, 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.

Le Roi:

1° peut préciser les données visées à l'alinéa 1er;

2° fixe les exigences en matière de précision et de fiabilité auxquelles ces données doivent répondre.

16° de identifier van de eindapparatuur van de eindgebruiker, of indien de operator dit niet verwerkt of genereert, de identifier van de apparatuur die zich het dichtste bij die eindapparatuur bevindt, met name:

— de internationale identiteit van de mobiele apparatuur ("International Mobile Equipment Identity", "IMEI");

— de permanente identifier van de apparatuur ("Permanent Equipment Identifier","PEI");

— het adres van de controller van de toegang tot het netwerk ("Media Access Control address", "MAC");

17° de andere identifiers met betrekking tot de eindgebruiker, tot de eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, op voorwaarde dat dit besluit door de wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

De operatoren hoeven de MAC-adressen bedoeld in het eerste lid, 16°, derde streepje, niet te bewaren voor de elektronische-communicatiediensten die ze enkel aan ondernemingen of rechtspersonen aanbieden.

Het koninklijk besluit bedoeld in het eerste lid, 17°, slaat niet op de inhoud van de elektronische communicatie, noch op de elektronische-communicatiemetagegevens 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 Koning:

1° kan de gegevens bedoeld in het eerste lid preciseren;

2° bepaalt de vereisten inzake nauwkeurigheid en betrouwbaarheid waaraan deze gegevens moeten beantwoorden.

§ 2. Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 1° à 14°, aussi longtemps que le service de communications électroniques est utilisé ainsi que douze mois après la fin du service.

Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 15° et 16°, pour une durée de douze mois après la fin de la session.

Par dérogation à l'alinéa deux, la durée de conservation des données visées au paragraphe 1er, alinéa 1er, 16°, 3e tiret, est réduite à six mois après la fin de la session lorsque l'opérateur conserve une autre donnée visée au paragraphe 1er, alinéa 1er, 16°.

Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 17°, pour la durée fixée par le Roi. Cette durée ne peut pas être plus longue que la durée de conservation visée à l'alinéa 1er.

L'arrêté royal visé au paragraphe 1er, alinéa 1er, 17°, et alinéa 4 et au paragraphe 2, alinéa 4, est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres."

JUSTIFICATION

Nécessité du présent amendement à la suite de l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle.

Le 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 (ci-après le projet de loi "conservation des données") a pour objet, entre autres, de remplacer l'article 126 de la loi télécom.

Un amendement à ce projet de loi est nécessaire pour ce qui concerne cet article 126, pour tenir compte de l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle.

§ 2. De operatoren bewaren de in paragraaf 1, eerste lid, 1° tot 14°, bedoelde gegevens tot zolang de elektronische-communicatiedienst gebruikt werd en tot twaalf maanden na het einde van de dienst.

De operatoren bewaren de in paragraaf 1, eerste lid, 15° en 16°, bedoelde gegevens gedurende een periode van twaalf maanden na het einde van de sessie.

In afwijking van het tweede lid wordt de bewaringstermijn van de in paragraaf 1, eerste lid, 16°, 3e streepje, bedoelde gegevens, teruggebracht tot zes maanden na het einde van de sessie indien de operator een ander gegeven zoals bedoeld in paragraaf 1, eerste lid, 16°, bewaart.

De operatoren bewaren de gegevens bedoeld in paragraaf 1, eerste lid, 17°, gedurende de door de Koning bepaalde periode. Die periode mag niet langer zijn dan de in het eerste lid bedoelde bewaringstermijn.

Het koninklijk besluit bedoeld in paragraaf 1, eerste lid, 17°, en vierde lid, en in paragraaf 2, vierde lid, wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad."

VERANTWOORDING

Noodzaak van dit amendement ingevolge arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof.

Het 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 (hierna het wetsontwerp "gegevensbewaring") heeft, onder andere, tot doel artikel 126 van de telecomwet te vervangen.

Een amendement aan dit wetsontwerp is noodzakelijk wat artikel 126 betreft om rekening te houden met arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof.

Dans cet arrêt, la Cour constitutionnelle a annulé l'article 2 de la loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après la loi du 1er septembre 2016), au motif que cet article 2 ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. Selon la Cour, il s'agit d'"éléments essentiels d'un traitement de données à caractère personnel" (B.8.4.2.), qui doivent donc être énumérés dans la loi.

Même si l'annulation de l'article 2 de la loi du 1er septembre 2016 ne porte pas sur l'article 126 de la loi télécom (mais bien sur l'article 127 de cette même loi), le gouvernement estime que cet arrêt a un impact sur l'article 126.

En effet, dans le même arrêt, la Cour constitutionnelle rappelle que la méthode de travail suivie par le législateur dans le cadre de l'article 127 de la loi télécom consistait à laisser au Roi le soin de déterminer les données d'identification traitées et les documents d'identification admis. La Cour constitutionnelle indique dans son arrêt (B.8.4.3.) que "Lors des travaux préparatoires, le législateur justifie cette méthode de travail par le caractère technique des données d'identification et des documents d'identification, la nécessité de pouvoir en adapter l'énumération en fonction de nouveaux enseignements et le fait que, dans le cadre de la conservation des données, ces données n'étaient pas non plus énumérées dans l'article 126 de la loi du 13 juin 2005 lui-même annulé par l'arrêt de la Cour n° 57/2021 du 22 avril 2021.

Indépendamment du fait que ces arguments ne sauraient expliquer l'absence d'une habilitation explicite et sans équivoque, le caractère technique des données d'identification et des documents d'identification et l'adaptabilité d'une telle énumération ne suffisent pas pour conclure que le fait d'ancrer de tels éléments dans une norme législative ne permettrait pas au législateur de réaliser un objectif d'intérêt général. En effet, même une norme législative peut être modifiée. Le Conseil des ministres ne démontre pas qu'une modification de ces données d'identification peut être urgente au point de ne pas pouvoir suivre le cours normal de la procédure législative. De même, une énumération des données d'identification et des documents d'identification n'est pas complexe au point de ne pas pouvoir être inscrite dans une norme législative.

Enfin, le législateur ne saurait justifier une violation de la Constitution en renvoyant à une autre disposition législative

In dat arrest heeft het Grondwettelijk Hof artikel 2 vernietigd van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna de wet van 1 september 2016), om de reden dat artikel 2 niet de identificatiegegevens bepaalt die verzameld en verwerkt worden en welke identificatiedocumenten in aanmerking komen. Volgens het Hof gaat het om "essentiële elementen van een verwerking van persoonsgegevens" (B.8.4.2.) die dus in de wet moeten worden opgesomd.

Zelfs al heeft de vernietiging van artikel 2 van de wet van 1 september 2016 geen betrekking op artikel 126 van de telecomwet (maar wel op artikel 127 van diezelfde wet), is de regering van oordeel dat dat arrest een impact heeft op artikel 126.

In hetzelfde arrest herinnert het Grondwettelijk Hof er immers aan dat de door de wetgever gevolgde manier van werken in het kader van artikel 127 van de telecomwet erin bestond de zorg aan de Koning over te laten om de verwerkte identificatiegegevens en de toegelaten identificatiedocumenten te bepalen. Het Grondwettelijk Hof geeft in zijn arrest (B.8.4.3.) het volgende aan "In de parlementaire voorbereiding verantwoordt de wetgever die manier van werken door te verwijzen naar de technische aard van de identificatiegegevens en identificatiedocumenten, de noodzaak om de oplijsting daarvan te kunnen aanpassen in het licht van gewijzigde inzichten, en het feit dat ook in het kader van de dataretentie die gegevens niet in het bij het arrest van het Hof nr. 57/2021 van 22 april 2021 vernietigde artikel 126 van de wet van 13 juni 2005 zelf werden opgesomd.

Nog afgezien van het feit dat die argumenten de afwezigheid van een uitdrukkelijke en ondubbelzinnige machtiging niet kunnen verklaren, volstaan de technische aard van identificatiegegevens en identificatiedocumenten en de aanpasbaarheid van een dergelijke oplijsting niet om te besluiten dat een verankering ervan in een wetskrachtige norm de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken. Ook een wetskrachtige norm kan immers worden gewijzigd. De Ministerraad toont niet aan dat een wijziging van die identificatiegegevens zo dringend kan zijn dat het normale verloop van de wetgevende procedure niet kan worden gevolgd. Een oplijsting van identificatiegegevens en identificatiedocumenten is ook niet dermate complex dat zij niet in een wetskrachtige norm kan worden opgenomen.

Tot slot kan de wetgever een schending van de Grondwet niet rechtvaardigen door te verwijzen naar een andere

qui comporterait peut-être la même inconstitutionnalité." (c'est nous qui soulignons)

Il en ressort que selon la Cour constitutionnelle, l'article 126 comporte peut-être la même inconstitutionnalité que l'article 127.

Pour tenir compte de cet arrêt, les données qui se trouvaient auparavant aux paragraphes 1er des articles 3 à 6 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 ont été déplacées vers cet article 126.

La nécessité d'obliger les opérateurs à conserver des données

Au point 27 de son avis sur l'amendement, l'Autorité de protection des données indique que la conservation obligatoire des données visées à l'article 126 de la loi télécom constitue une ingérence particulièrement grave dans la vie privée de toutes les personnes qui utilisent des services de communications électroniques.

Il convient cependant de rappeler que cet article 126 concerne des données d'identification (qui, en principe, ne donne pas d'information sur la communication ni sur la localisation précise de l'individu) et que ces informations sont moins intrusives dans la vie privée que les métadonnées visées à l'article 126/2 de la loi télécom. De plus, la CJUE autorise les États membres à imposer aux opérateurs la conservation des adresses IP à la source de la connexion.

Dans le même point de son avis, l'Autorité de protection des données indique que la conservation des données visées à l'article 126 comporte un risque important en termes de sécurité de l'information.

Il convient cependant de noter que les opérateurs conservent déjà des données d'identification pour leurs propres besoins et qu'il leur revient de prendre les mesures de sécurité nécessaires pour protéger ces données. Prendre des mesures de protection adéquates (protéger les données) permet de minimiser les risques de sécurité.

Dans le même point de son avis, l'Autorité de protection des données indique également que la conservation des données représente un coût élevé pour les opérateurs (notamment pour sécuriser les données), qui pourrait être répercuté sur les consommateurs. Ce coût supplémentaire risque également

wetsbepaling die mogelijk dezelfde ongrondwettigheid bevatte." (wij onderlijnen)

Daaruit blijkt dat volgens het Grondwettelijk Hof artikel 126 misschien dezelfde ongrondwettigheid als artikel 127 bevat.

Om rekening te houden met dat arrest zijn de gegevens die zich voordien bevonden in de paragrafen 1 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, verplaatst geweest naar dat artikel 126.

De noodzaak om de operatoren te verplichten gegevens te bewaren

In punt 27 van zijn advies over het amendement geeft de Gegevensbeschermingsautoriteit aan dat de verplichte bewaring van de gegevens bedoeld in artikel 126 van de telecomwet een bijzonder belangrijke inmenging vormt in de persoonlijke levenssfeer van alle personen die gebruikmaken van elektronische-communicatiediensten.

Er dient evenwel aan te worden herinnerd dat dit artikel 126 betrekking heeft op identificatiegegevens (die, in principe, geen informatie geven over de communicatie noch over de juiste locatie van het individu) en dat deze informatie de persoonlijke levenssfeer minder schendt dan de metagegevens waarvan sprake in artikel 126/2 van de telecomwet. Bovendien staat het HvJ-EU het aan de lidstaten toe om aan de operatoren de bewaring van de IP-adressen aan de bron van de verbinding op te leggen.

In hetzelfde punt van haar advies geeft de Gegevensbeschermingsautoriteit aan dat de bewaring van de in artikel 126 bedoelde gegevens een aanzienlijk risico inhoudt op het gebied van informatiebeveiliging.

Er moet evenwel worden opgemerkt dat de operatoren reeds voor hun eigen behoeften identificatiegegevens bewaren en dat het aan hen toekomt om de nodige veiligheidsmaatregelen te treffen om die gegevens te beschermen. Door gepaste beschermingsmaatregelen te nemen (de gegevens beschermen) kunnen de veiligheidsrisico's tot een minimum worden herleid.

In hetzelfde punt van haar advies geeft de Gegevensbeschermingsautoriteit ook aan dat de gegevensbewaring voor de operatoren hoge kosten met zich brengt (met name om de gegevens te beveiligen), die doorberekend zouden kunnen worden aan de consumenten. Die extra kosten

d'aboutir à ce que des services de communications électroniques gratuits et sans but de lucre, comme Signal ou Tor, ne soient plus en mesure d'offrir leurs services aux utilisateurs et utilisatrices en Belgique.

La réponse du gouvernement est la suivante:

— à ce jour, Tor n'est pas un opérateur au sens de la loi télécom (Signal l'est bien) et n'est donc pas soumis aux articles 126 à 126/2 de la loi télécom;

— l'Autorité de protection des données indique que "la conservation des données représente un coût élevé pour les opérateurs" mais ne donne pas de chiffres qui indiqueraient la hauteur de ces coûts;

— le coût du stockage des données diminue d'année en année;

— les opérateurs conservent déjà des données pour leurs propres besoins;

— les opérateurs qui fournissent des services de communications électroniques gratuits et sans but de lucre n'ont pas fait savoir qu'ils ne seraient plus en mesure d'offrir leurs services aux utilisateurs et utilisatrices en Belgique à cause de l'obligation de conservation des données (bien que deux consultations publiques aient été organisées sur le sujet);

— la CJUE estime que la directive e-privacy permet aux États membres d'imposer aux opérateurs la conservation généralisée et indifférenciée des adresses IP à la source de la connexion. Dans le cadre de l'article 126 de la loi télécom, il s'agit de l'obligation principale pour les opérateurs qui offrent des services de communications interpersonnelles qui ne sont pas fondés sur la numérotation. Il peut être attendu à ce que cette obligation soit imposée dans tous les États membres.

Au point 27 de son avis, l'Autorité de protection des données indique également qu'il n'y a pas de garantie que cette ingérence dans la vie privée que constitue la conservation des données sur base de l'article 126 de la loi télécom soit effective pour atteindre l'objectif poursuivi puisqu'il y aura toujours des possibilités de trouver des moyens de communications qui échapperont à la surveillance étatique.

La réponse du gouvernement est la suivante:

— si le raisonnement de l'Autorité de protection des données était suivi, cela remettrait en question de nombreuses

riskeren ook er uiteindelijk toe te leiden dat gratis en non-profit elektronische-communicatiediensten, zoals Signal of Tor, hun diensten niet meer kunnen aanbieden aan gebruikers en gebruiksters in België.

Het antwoord van de regering is als volgt:

— tot op heden is Tor geen operator in de zin van de telecomwet (Signal is dat wel) en is daardoor niet onderworpen aan de artikelen 126 tot 126/2 van de telecomwet;

— de Gegevensbeschermingsautoriteit vermeldt dat "de gegevensbewaring hoge kosten voor de operatoren vertegenwoordigt", maar geeft geen cijfers om de hoogte van die kosten aan te geven;

— de kosten voor de gegevensopslag verminderen van jaar tot jaar;

— de operatoren bewaren reeds gegevens voor hun eigen behoeften;

— de operatoren die gratis en non-profit elektronische-communicatiediensten aanbieden, hebben niet te kennen gegeven dat ze niet meer in staat zouden zijn om hun diensten aan te bieden aan de gebruikers en gebruiksters in België wegens de verplichting tot gegevensbewaring (hoewel daarover twee openbare raadplegingen zijn georganiseerd);

— het HvJ-EU is van oordeel dat de e-privacy-richtlijn het aan de lidstaten toestaat om aan de operatoren de algemene en ongedifferentieerde bewaring van de IP-adressen aan de bron van de verbinding op te leggen. In het kader van artikel 126 van de telecomwet gaat het om de voornaamste verplichting voor de operatoren die nummeronafhankelijke interpersoonlijke communicatiediensten aanbieden. Er kan worden verwacht dat deze verplichting in alle lidstaten wordt opgelegd.

In punt 27 van haar advies geeft de Gegevensbeschermingsautoriteit ook aan dat er geen garantie is dat deze inmenging in het privéleven die voortvloeit uit de gegevensbewaring op grond van artikel 126 van de telecomwet doeltreffend is om het nagestreefde doel te bereiken, aangezien er altijd mogelijkheden zullen zijn om communicatiemiddelen te vinden die aan het overheidstoezicht ontsnappen.

Het antwoord van de regering is als volgt:

— als de redenering van de Gegevensbeschermingsautoriteit zou worden gevolgd, zou dit talrijke wetgevingen

législations, dès lors qu'il existe généralement des pistes (illégales) pour les contourner;

— du point de vue des autorités, une mesure de conservation des données telle que visée à l'article 126, même si elle peut être contournée dans certains cas, est nettement préférable à l'absence d'une telle mesure: même si certains "criminels" parviennent à trouver des moyens de communications qui ne mettent pas en œuvre les obligations prévues par la loi télécom, il ne s'agit pas de l'ensemble des criminels. Par ailleurs, cela complique la tâche des criminels et ceux qui y parviennent commentent des fautes ou laissent tout de même des traces.

Au point 27 de son avis et sur base des éléments précités, l'Autorité de protection des données arrive à la conclusion suivante: "les opérateurs ne devraient être tenus de conserver, pour les besoins des autorités, les données de souscription de l'abonné et les données permettant d'identifier les utilisateurs finaux ainsi que les données techniques permettant d'identifier les équipements terminaux des utilisateurs finaux ou les équipements le plus proches de ces équipements terminaux, uniquement dans la mesure où ils génèrent et conservent ces données pour leurs propres besoins, et pour autant, bien entendu, que cette conservation respecte les principes de nécessité et de proportionnalité."

D'abord, il n'est pas clair de savoir quelle serait la plus-value en pratique de cette proposition de l'Autorité de protection des données. En effet, pourquoi obliger les opérateurs à conserver, pour les autorités, des données qu'ils conservent déjà pour leurs propres besoins, dès lors que ces autorités peuvent obtenir ces dernières données? La proposition de l'Autorité de protection des données n'a d'utilité que pour autant que les opérateurs soient obligés de prolonger au bénéfice des autorités la durée de conservation des données qu'ils conservent déjà pour leurs propres besoins.

Ensuite, ne permettre aux autorités de n'obtenir que les données que les opérateurs conservent pour leurs propres besoins présente de nombreux inconvénients:

— certaines données sont traitées ou générées par les opérateurs mais ne sont pas conservées pour leurs propres besoins alors que la conservation de ces données est primordiale pour les autorités (par exemple l'adresse IP à la source de la connexion);

— certaines données sont conservées par l'opérateur pour ses propres besoins mais pendant une durée insuffisante pour les besoins des autorités;

op losse schroeven zetten, aangezien er meestal (illegale) pistes bestaan om die te omzeilen;

— vanuit het oogpunt van de veiligheidsdiensten, is een maatregel inzake gegevensbewaring zoals bedoeld in artikel 126, ook al kan die in sommige gevallen worden omzeild, duidelijk te verkiezen boven de afwezigheid van zo'n maatregel: zelfs als sommige "criminelen" erin slagen om communicatiemiddelen te vinden die de verplichtingen van in de telecomwet niet vervullen, gaat het niet om alle criminelen. Bovendien maakt dit de taak van de criminelen moeilijker en zij die erin slagen, maken fouten of laten toch sporen na.

In punt 27 van haar advies en op basis van de voormelde elementen komt de Gegevensbeschermingsautoriteit tot de volgende conclusie: "operatoren voor de behoeften van de autoriteiten alleen verplicht zouden wij moeten worden tot het bewaren van abonneegegevens en gegevens waarmee eindgebruikers kunnen worden geïdentificeerd, alsmede technische gegevens waarmee de eindapparatuur van eindgebruikers of de apparatuur die zich het dichtst in de buurt van deze eindapparatuur bevindt, kan worden geïdentificeerd, alleen voor zover zij deze gegevens voor hun eigen behoeften genereren en bewaren, en uiteraard op voorwaarde dat deze bewaring in overeenstemming is met de beginselen van noodzakelijkheid en evenredigheid."

Allereerst is het niet duidelijk wat de meerwaarde van dit voorstel van de Gegevensbeschermingsautoriteit zou zijn. Want waarom zouden de operatoren verplicht worden om voor de autoriteiten gegevens te bewaren die ze reeds voor hun eigen behoeften bewaren, als die autoriteiten deze laatste gegevens kunnen verkrijgen? Het voorstel van de Gegevensbeschermingsautoriteit heeft maar nut voor zover de operatoren verplicht worden om de bewaringstermijn van de gegevens die ze al voor hun eigen behoeften bewaren, ten voordele van de autoriteiten te verlengen.

Vervolgens houdt het slechts toestaan aan de veiligheidsdiensten om enkel de gegevens te verkrijgen die de operatoren voor hun eigen behoeften bewaren, talrijke nadelen in:

— sommige gegevens worden door de operatoren verwerkt of gegenereerd, maar niet voor hun eigen behoeften bewaard, terwijl de bewaring van die gegevens van essentieel belang is voor de veiligheidsdiensten (bijvoorbeeld het IP-adres aan de bron van de verbinding);

— sommige gegevens worden door de operator voor zijn eigen behoeften bewaard, maar voor een periode die niet lang genoeg is voor de behoeften van de autoriteiten;

— il y a de grandes différences entre opérateurs en termes de conservation de données pour leurs propres besoins (certains en conservent plus que d'autres et les durées de conservation varient également);

— les autorités deviennent entièrement dépendantes de la politique d'un opérateur; ainsi, ce dernier peut décider un jour de conserver certaines données pour ses propres besoins mais peut décider ultérieurement de ne plus le faire;

— les opérateurs ne sont pas toujours transparents par rapport aux données qu'ils conservent pour leurs propres besoins; ainsi, il est apparu de dossiers judiciaires que certains opérateurs conservent plus de données pour leurs propres besoins que ce qu'ils prétendent;

— en pratique, il peut être difficile pour les opérateurs de fournir (rapidement) aux autorités des données qu'ils conservent pour leurs propres besoins, à défaut d'outil informatique adéquat (nécessité de recherches manuelles complexes). Ces données peuvent aussi être fournies sans garantie de fiabilité, dès lors que ces données commerciales ou techniques ne sont pas conservées avec les liens nécessaires pour les besoins des autorités.

Ce sont ces différentes considérations qui ont amené l'État à obliger les opérateurs à conserver un set minimum de données. Il est important pour les autorités judiciaires de pouvoir recouper les données conservées et ce, tant à charge qu'à décharge.

Les différentes législations en matière de conservation des données (de la directive "conservation des données" de 2006 jusqu'à la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électronique) se basent sur le principe que l'opérateur conserve certaines données qu'il traite ou qu'il génère, sans ajouter la condition qu'il les conserve pour ses propres besoins.

Les entreprises qui doivent conserver les données (paragraphe 1er)

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 après 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).

— tussen operatoren bestaan grote verschillen in termen van gegevensbewaring voor hun eigen behoeften (sommige bewaren er meer dan andere en ook de bewaringstermijnen verschillen);

— de veiligheidsdiensten worden helemaal afhankelijk van het beleid van een operator; zo kan die laatste op een dag beslissen om bepaalde gegevens voor zijn eigen behoeften te bewaren, maar later beslissen om dat niet meer te doen;

— de operatoren zijn niet altijd transparant wat betreft de gegevens die ze voor hun eigen behoeften bewaren; zo is uit gerechtelijke dossiers gebleken dat sommige operatoren meer gegevens voor hun eigen behoeften bewaren dan wat ze beweren;

— in de praktijk kan het voor de operatoren moeilijk zijn om aan de autoriteiten (snel) gegevens te verstrekken die ze voor hun eigen behoeften bewaren, bij gebrek aan een geschikte IT-tool (noodzaak tot ingewikkeld manueel opzoekingswerk). Die gegevens kunnen ook zonder garantie inzake betrouwbaarheid worden verstrekt, omdat die commerciële of technische gegevens nu eenmaal niet worden bewaard met de verbanden die voor de behoeften van de autoriteiten noodzakelijk zijn.

Het zijn deze verschillende overwegingen die de Staat ertoe hebben gebracht om de operatoren te verplichten om een minimumreeks van gegevens te bewaren. Het is voor de gerechtelijke autoriteiten belangrijk dat de bewaarde gegevens geverifieerd kunnen worden en dat zowel *à charge* als *à décharge*.

De verschillende wetgevingen inzake gegevensbewaring (van de "Dataretentierichtlijn" van 2006 tot de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie) zijn gebaseerd op het principe dat de operator bepaalde gegevens die hij verwerkt of genereert, bewaart, zonder daaraan de voorwaarde toe te voegen dat hij die bewaart voor zijn eigen behoeften.

De bedrijven die de gegevens moeten bewaren (paragraaf 1)

Bepaalde wijzigingen werden aangebracht in artikel 126 om zich te conformeren aan de terminologie en definities die in de telecomwet gebruikt worden na 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).

Concernant le paragraphe 1er et vu que la notion de service de communications électroniques est définie dans le Code de manière plus large qu'auparavant, il n'est plus nécessaire de viser les opérateurs et les fournisseurs de services (version de l'article 126 tel que remplacé par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques) mais il suffit de viser les opérateurs.

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

Les données à conserver (paragraphe 1er)

Introduction

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.

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 du 6 octobre 2020, ne sont plus visées dans l'article 126 de la loi télécom que les données de souscription et les données qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou l'équipement le plus proche de cet équipement terminal.

À l'instar des données énumérées à l'article 126/2, § 2, le présent article reprend et adapte les données précédemment listées aux paragraphes 1er des articles 3 à 6 de l'arrêté royal du 19 septembre 2013 non plus au moyen de listes de données distinctes par type de service de communications électroniques (téléphone fixe, téléphonie mobile, service d'accès à internet, service de courrier électronique et service de téléphonie par internet), mais au moyen d'une seule liste de données commune pour l'ensemble de ces services. Une liste commune se justifie compte tenu de la convergence croissante des services de communications électroniques et de l'extension de cette dernière notion, ainsi que de la notion d'opérateur aux acteurs OTT, à la suite de la transposition dans la loi télécom 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). Il incombe dès lors à l'opérateur de vérifier quelles données de cette liste sont traitées ou générées par lui dans le cadre des services ou réseaux qu'il offre. Cette vérification doit être effectuée pour chaque type de service offert par l'opérateur, de sorte

Wat betreft paragraaf 1 en aangezien het begrip van elektronische-communicatiedienst in het Wetboek ruimer gedefinieerd is dan voordien, is het niet meer noodzakelijk om de operatoren en de aanbieders van diensten te beogen (versie van artikel 126 zoals vervangen door de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie), maar volstaat het om de operatoren te beogen.

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

De te bewaren gegevens (paragraaf 1)

Inleiding

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.

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 van 6 oktober 2020, worden in artikel 126 van de telecomwet enkel nog de abonnementsgegevens en gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de apparatuur die zich het dichtst bij deze eindapparatuur bevindt, beoogd.

Naar het voorbeeld van de gegevens opgesomd in artikel 126/2, § 2, neemt het onderhavige artikel de gegevens over die voordien waren opgesomd in de paragrafen 1 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013 en past deze aan, niet langer door middel van afzonderlijke lijsten van gegevens per categorie van elektronische-communicatiedienst (vaste telefonie, mobiele telefonie, internettoegangsdienst, e-maildienst via internet en een internettelefoniedienst), maar door middel van een enkele gemeenschappelijke lijst van gegevens voor al die diensten. Een gemeenschappelijke lijst is gerechtvaardigd rekening houdend met de toenemende convergentie van de elektronische-communicatiediensten en met de uitbreiding van dat laatste begrip alsook van het begrip operator naar de OTT-spelers naar aanleiding van de omzetting in de telecomwet 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). Het is dus de verantwoordelijkheid van de operator om te verifiëren welke gegevens van die lijst verwerkt of gegenereerd

que l'ensemble des données pertinentes soient conservées pour chaque service et pour chaque utilisateur final.

Le numéro de Registre national ou un numéro équivalent, le nom et le prénom de l'utilisateur final qui est une personne physique ou la dénomination de l'abonné qui est une personne morale (1°).

La notion d'utilisateur final (article 2, 13°, de la loi télécom) inclut la notion d'abonné (article 2, 15°, de la loi télécom), soit la personne qui conclut le contrat avec l'opérateur, et l'utilisateur effectif du service.

Les données reprises sous 1° ne seront pas nécessairement conservées dans le cadre de l'article 127 de la loi télécom (en particulier si l'opérateur permet uniquement aux autorités de retrouver l'identité de ses abonnés).

Les données complémentaires qui permettent aux autorités de vérifier l'identité de l'abonné ou de retrouver l'utilisateur effectif du service.

L'article 127 oblige les opérateurs à identifier leurs abonnés ou à permettre aux autorités de retrouver cette identité. Cependant, la pratique montre que des personnes mal intentionnées parviennent à s'identifier:

— sous un faux nom, à savoir un nom qui n'est pas le leur; dans certains cas, il sera manifeste qu'il s'agit d'un faux nom (par exemple car le nom correspond à une personne célèbre, fictive ou pas) mais pas toujours (car le nom renseigné est crédible);

— avec un document d'identité falsifié;

— avec un document d'identité d'une autre personne.

Généralement, un nom que l'abonné renseigne en ligne sera peu fiable.

L'utilisation fréquente de fausses données d'identité impose de pouvoir recouper les données d'identification conservées avec d'autres données disponibles chez les opérateurs:

— les alias (2°);

— les coordonnées de contact de l'abonné (3°);

zijn door hem in het kader van de diensten of netwerken die hij aanbiedt. Die verificatie moet worden uitgevoerd voor elk type van dienst die door de operator aangeboden wordt, zodat alle relevante gegevens bewaard worden voor elke dienst en voor elke eindgebruiker.

Het rijksregisternummer of een equivalent nummer, de naam en voornaam van de eindgebruiker die een natuurlijke persoon is of de naam van de abonnee die een rechtspersoon is (1°).

Het begrip eindgebruiker (artikel 2, 13°, van de telecomwet) omvat het begrip abonnee (artikel 2, 15°, van de telecomwet), ofwel de persoon die het contract met de operator sluit en de effectieve gebruiker van de dienst.

De gegevens vermeld onder 1° zullen niet noodzakelijk bewaard worden in het kader van artikel 127 van de telecomwet (in het bijzonder indien de operator het slechts mogelijk maakt om de identiteit van zijn abonnees terug te vinden).

De aanvullende gegevens die het voor de autoriteiten mogelijk maken de identiteit van de abonnee te verifiëren of de effectieve gebruiker van de dienst terug te vinden.

Artikel 127 verplicht de operatoren hun abonnees te identificeren of om het aan de autoriteiten mogelijk te maken die identiteit terug te vinden. De praktijk toont echter aan dat personen met kwaadwillige intenties erin slagen zich te identificeren:

— onder een valse naam, namelijk een naam die niet van hen is; in sommige gevallen zal het duidelijk zijn dat het om een valse naam gaat (bijvoorbeeld omdat de naam overeenstemt met een beroemde persoon, al dan niet fictief), maar niet altijd (omdat de vermelde naam geloofwaardig is);

— met een vervalst identiteitsstuk;

— met een identiteitsbewijs van een andere persoon.

In het algemeen zal een naam die de abonnee online ingeeft weinig betrouwbaar zijn.

Het frequente gebruik van valse identiteitsgegevens maakt het noodzakelijk de bewaarde identificatiegegevens te kunnen toetsen aan andere bij de operatoren beschikbare gegevens:

— de aliassen (2°);

— de contactgegevens van de abonnee (3°);

— la date et le lieu de souscription au service et de l'activation du service (4°);

— l'adresse physique de livraison du service (5°);

— les données de paiement (6°).

Ces données supplémentaires permettent d'exclure que les victimes d'une fraude à l'identité soient impliquées à tort en tant qu'auteur dans un dossier judiciaire qui ne les concerne en rien. Les données supplémentaires évitent également la violation ultérieure de la vie privée de ces personnes innocentes par des mesures d'enquête subséquentes plus intrusives, telles que l'interception de leurs communications ou une perquisition.

Ces données supplémentaires (comme l'alias ou l'adresse physique de livraison du service) constituent donc dans certains cas des pistes complémentaires qui peuvent s'avérer déterminantes pour retrouver l'utilisateur effectif du service.

La Justice demande déjà aux opérateurs ces données supplémentaires.

Le Conseil d'État français, qui a été amené à examiner la législation française en matière de conservation de métadonnées 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).

L'alias (2°)

L'opérateur doit conserver l'alias (dans ce contexte le nom par lequel l'utilisateur final se fait connaître auprès des autres utilisateurs finaux). Si l'utilisateur final a la possibilité de modifier son alias lors l'activation du service, l'opérateur devra conserver tant l'alias lors de la souscription que celui lors de l'activation.

Dans le cadre des enquêtes judiciaires ou des services de renseignement, les autorités sont quasi systématiquement confrontées à des difficultés très importantes pour identifier

— de datum en de plaats van inschrijving op de dienst of de activering van de dienst (4°);

— het fysieke leveringsadres van de dienst (5°);

— de betalingsgegevens (6°).

Die bijkomende gegevens kunnen uitsluiten dat slachtoffers van identiteitsfraude onterecht worden betrokken als dader in een gerechtelijk dossier dat geen betrekking heeft op hen. De bijkomende gegevens voorkomen zo ook dat de privacy van deze onschuldige personen verder zou worden geschonden door meer indringende, navolgende onderzoeksmaatregelen zoals een interceptie van hun communicatie of een huiszoeking.

Die bijkomende gegevens (zoals de alias of het fysieke leveringsadres van de dienst) zijn dus in sommige gevallen een bijkomende en mogelijke beslissende aanwijzing naar het terugvinden van de effectieve gebruiker van de dienst.

Justitie vraagt al die bijkomende gegevens reeds aan de operatoren.

De Franse Conseil d'État, die de wetgeving betreffende bewaring door de operatoren van metagegevens voor de autoriteiten moest onderzoeken (arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK en anderen), 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).

De alias (2°)

De operator moet de alias bewaren (in die context de naam waarmee de eindgebruiker zich bekendmaakt aan andere eindgebruikers). Indien de eindgebruiker de mogelijkheid heeft om bij de activering van de dienst zijn alias te wijzigen, zal de operator zowel de alias bij de inschrijving als die bij de activering moeten bewaren.

In het kader van de gerechtelijke onderzoeken of onderzoeken van de inlichtingendiensten worden de autoriteiten bijna systematisch geconfronteerd met zeer belangrijke

ou confirmer l'identité de l'utilisateur effectif d'un service. La conservation des alias utilisés est essentielle à cette fin.

Ceci est particulièrement le cas pour l'identification auprès de services en ligne, ou lorsqu'il apparait au cours de l'enquête que des documents d'identité faux ou falsifiés ont été utilisés.

Déterminer l'identité d'un utilisateur effectif est la première démarche de toute approche des autorités judiciaires dans le cadre d'une enquête.

Dans le cas d'une obfuscation voulue de l'identité par l'utilisateur, ce processus de vérification de l'identité réelle de l'utilisateur effectif s'apparente à souvent à chercher une aiguille dans une meule de foin. Dans ce contexte, le recours à l'alias peut s'avérer souvent cruciale.

Dans le cadre d'une enquête de phishing, un même alias peut être utilisé dans diverses tentatives. Cet alias peut correspondre à l'activation de divers services en ligne. Un même alias peut être utilisé à diverses reprises et dans diverses communications dont l'une d'elle va, par erreur du ou des auteurs, pouvoir être liée à une identité réelle.

Les coordonnées de contact de l'abonné (3°)

Le 3° renvoie aux coordonnées de contact de l'abonné, sans donner une liste exhaustive de toutes les manières dont dispose l'opérateur pour pouvoir contacter l'abonné. En effet, avec les évolutions et en particulier le développement des médias sociaux, un numéro de téléphone, une adresse e-mail ou une adresse postale ne sont plus nécessairement les (seuls) moyens à la disposition de l'opérateur pour contacter l'abonné.

La date et le lieu de la souscription au service et de l'activation du service (4°)

Dans le cadre d'une enquête judiciaire, déterminer la localisation du point de vente où la souscription ou l'activation ont eu lieu, permet de faire un premier tri parmi les éventuels suspects du dossier. Si l'affaire est grave (meurtre par exemple), interroger les préposés du point de vente concerné ou visionner les images des éventuelles caméras de sécurité font partie des moyens d'enquête régulièrement utilisés, de manière à identifier le titulaire réel d'un moyen de communication électronique, qui s'est par exemple identifié avec une fausse identité.

moeilijkheden om de identiteit van de effectieve gebruiker van een dienst te identificeren of bevestigen. Hiertoe is het van essentieel belang dat de gebruikte aliassen bewaard blijven.

Dit geldt in het bijzonder voor de identificatie bij de onlinediensten of wanneer uit het onderzoek blijkt dat valse of vervalste identiteitsdocumenten werden gebruikt.

In het kader van een onderzoek vormt de identificatie van een effectieve gebruiker de eerste stap in elke aanpak van de gerechtelijke autoriteiten.

In het geval van een door de gebruiker gewenste identiteitsobfuscatie lijkt dit proces van verificatie van de werkelijke identiteit van de effectieve gebruiker vaak op het zoeken naar een naald in een hooiberg. In dit verband kan het gebruik van aliassen vaak cruciaal zijn.

In het kader van een phishing-onderzoek kan dezelfde alias in verschillende pogingen worden gebruikt. Deze alias kan met de activering van verschillende onlinediensten overeenkomen. Dezelfde alias kan meermaals en in verschillende communicaties gebruikt worden, waarvan er één, bij vergissing van de auteur(s), gekoppeld kan worden aan een echte identiteit.

De contactgegevens van de abonnee (3°)

3° verwijst naar de contactgegevens van de abonnee zonder een volledige lijst te geven van alle manieren waarover de operator beschikt om contact te kunnen opnemen met de abonnee. Door de evoluties en in het bijzonder de ontwikkeling van sociale media zijn een telefoonnummer, een e-mailadres of een postadres immers niet meer noodzakelijkerwijs de (enige) middelen waarover de operator beschikt om contact op te nemen met de abonnee.

De datum en de plaats van inschrijving op de dienst en van de activering van de dienst (4°)

In het kader van een gerechtelijk onderzoek laat het identificeren van het verkooppunt waar de inschrijving of de activering heeft plaatsgevonden toe een eerste selectie te maken onder de mogelijke verdachten in het dossier. Als het om een ernstige zaak gaat (bijvoorbeeld een moord), behoren het ondervragen van de aangestelden van het betrokken verkooppunt of het bekijken van de beelden van eventuele bewakingscamera's tot de regelmatig gebruikte onderzoeksmethoden. De bedoeling ervan is de identificatie van de werkelijke houder van een elektronische-communicatiemiddel, die zich bijvoorbeeld met een valse identiteit heeft geïdentificeerd.

Tel est également le cas pour ce qui concerne la localisation du point de terminaison du réseau, l'adresse IP utilisée ou la localisation de l'équipement terminal ayant permis cette souscription ou cette activation.

La conservation de l'adresse du point de terminaison du réseau (voir définition dans l'article 2, 16°, de la loi télécom) ne permettra de déterminer le lieu de la souscription au service ou de l'activation du service que si cette souscription ou cette activation se fait à partir du même réseau que le réseau de l'opérateur qui offre le service auquel il est souscrit.

Au point 77 de son avis sur les amendements, l'Autorité de protection des données "s'interroge, plus largement, sur la pertinence de la conservation au-delà de 12 mois après la fin de la session de l'adresse IP ayant servi à la création du compte […] pour identifier les abonnés à un service de communications électroniques gratuit, étant donné que 12 mois après la fin de la session, il semblerait qu'il ne soit plus possible d'identifier la personne à qui l'adresse IP ayant servi à la création du compte […] a été attribuée. En effet, les fournisseurs d'accès à Internet, qui attribuent les adresses IP, doivent conserver les adresses IP attribuées à la source d'une connexion pendant 12 mois après la fin de la session. Si une personne souscrit à un service de communications électroniques gratuit par internet, l'opérateur de ce service conservera l'adresse IP à partir de laquelle le compte (voire toutes les adresses IP qui se sont connectées à ce service) a été créé; et ce en vue de rencontrer son obligation d'identifier – ou au moins de permettre l'identification par les autorités – tous ses abonnés. Mais pour pouvoir effectivement identifier cette personne, les autorités devront, non seulement collecter l'adresse IP ayant servi à la création du compte […] auprès de l'opérateur dudit service, mais elles devront ensuite demander au fournisseur d'accès à internet l'identité de l'abonné à qui cette adresse IP a été attribuée au moment auquel le compte a été créé […]. Or, si l'attribution a eu lieu il y a plus de 12 mois, le fournisseur d'accès à Internet n'aura plus accès à cette information."

Ce point de l'avis n'a pas été suivi pour les raisons suivantes:

— les adresses IP ayant servi à la création du compte sont systématiquement demandées dans les enquêtes judiciaires;

— conserver l'adresse IP ayant servi à la création du compte pendant la durée du contrat et 1 an après la fin du contrat a du sens car la pratique montre que cette adresse

Dit geldt ook voor de lokalisering van het netwerkaansluitpunt, het gebruikte IP-adres of de locatie van de eindapparatuur waarvandaan die inschrijving en die activering zijn uitgevoerd.

De bewaring van het adres van het netwerkaansluitpunt (zie definitie in artikel 2, 16°, van de telecomwet) zal het maar mogelijk maken om de plaats van de inschrijving op de dienst of de activering van de dienst te bepalen wanneer die inschrijving of die activering gebeurt op hetzelfde netwerk als het netwerk van de operator die de dienst aanbiedt waarop hij ingeschreven is.

In punt 77 van haar advies over de amendementen "vraagt de Autoriteit zich meer in het algemeen af of het relevant is om het IP-adres dat is gebruikt om de account aan te maken [...], ook na twaalf maanden na het einde van de sessie te bewaren met het oog op de identificatie van abonnees op een gratis elektronische-communicatiedienst, aangezien het twaalf maanden na het einde van de sessie blijkbaar niet meer mogelijk is om de persoon te identificeren aan wie het IP-adres dat is gebruikt om de account aan te maken [...] is toegewezen. Internetproviders, die IP-adressen toewijzen, moeten de IP-adressen die aan de bron van een verbinding zijn toegewezen immers nog 12 maanden na het einde van de sessie bewaren. Indien een persoon zich abonneert op een gratis elektronische-communicatiedienst via het internet, zal de operator van die dienst het IP-adres bewaren van waaruit de account (of alle IP-adressen die op die dienst zijn aangesloten) is aangemaakt; dit is om te voldoen aan zijn verplichting om al zijn abonnees te identificeren – of ten minste de identificatie door de autoriteiten mogelijk te maken. Om deze persoon daadwerkelijk te kunnen identificeren, zullen de autoriteiten echter niet alleen het IP-adres dat is gebruikt om de account aan te maken [...], bij de operator van die dienst moeten opvragen, maar zullen zij vervolgens de internetprovider moeten vragen naar de identiteit van de abonnee aan wie dit IP-adres was toegewezen op het moment dat de account werd aangemaakt [...]. Indien de toewijzing echter meer dan 12 maanden geleden heeft plaatsgevonden, zal de internetprovider geen toegang meer hebben tot deze informatie."

Dit punt van het advies is niet gevolgd om de volgende redenen:

— de IP-adressen die gebruikt zijn om de account aan te maken worden systematisch opgevraagd in gerechtelijke onderzoeken;

— het is zinvol om het IP-adres dat gebruikt is om de account aan te maken, te bewaren gedurende de looptijd van het contract en 1 jaar na het einde van het contract omdat uit

IP peut avoir été attribuée à l'abonné par un fournisseur d'accès à internet qui se trouve à l'étranger et qui conserve les adresses IP attribuées plus longtemps que 12 mois après la fin de la session;

— l'adresse IP qui est attribuée par le fournisseur d'accès à internet peut aussi être une adresse IP fixe, qui sera conservée aussi longtemps que l'adresse IP fixe est utilisée;

— l'adresse IP donne aussi certaines informations générales sur la localisation de l'équipement (pays concerné, éventuellement la région concernée).

Si comme l'indique l'Autorité de protection des données, l'adresse IP ayant servi à la création du compte n'a plus d'utilité, car le fournisseur d'accès à l'internet a cessé de conserver cette adresse, alors cette adresse IP ne constitue plus un risque d'atteinte à la vie privée de la personne concernée.

Dans certains cas, un service de communications électroniques est activé par SMS. Dans ce cas, l'opérateur devra conserver la localisation géographique de l'antenne qui a servi à l'envoi du SMS.

Adresse de livraison et de facturation du service (5° et 6°)

Les adresses de livraison et de facturation ne sont pas toujours les mêmes. L'adresse de livraison est évidemment primordiale et indispensable. L'adresse de facturation est tout aussi essentielle car elle permet également de dépister la personne ou l'organisation qui paie l'abonnement. Les autorités ont constaté dans différents dossiers qu'une personne morale se chargeait de régler les factures des connexions téléphoniques ou Internet utilisées par des criminels. L'adresse de facturation a conduit les autorités à cette personne morale.

Données de paiement (6°)

Les données de paiement sont parfois pour les autorités judiciaires et les services de renseignement et de sécurité la seule trace conduisant à l'utilisateur final d'un service de communications déterminé.

En effet, les abonnements télécom sont souvent souscrits sous un faux nom mais doivent néanmoins être payés. Il importe dès lors de conserver le numéro de compte ou de carte de paiement utilisé pour régler l'abonnement ou pour recharger le crédit d'utilisation.

de praktijk blijkt dat dit IP-adres aan de abonnee kan zijn toegewezen door een internetprovider die zich in het buitenland bevindt en die de toegewezen IP-adressen langer bewaart dan 12 maanden na het einde van de sessie;

— het IP-adres dat door de internetprovider toegewezen is, kan ook een vast IP-adres zijn, dat zolang zal worden bewaard als het vaste IP-adres wordt gebruikt;

— het IP-adres geeft ook bepaalde algemene informatie over de plaats van de apparatuur (betrokken land, eventueel de betrokken regio).

Indien, zoals de Gegevensbeschermingsautoriteit zegt, het IP-adres dat is gebruikt om de account aan te maken, geen nut meer heeft, omdat de internetprovider de bewaring van dat adres heeft stopgezet, dan vormt dat IP-adres geen risico meer voor een schending van de privacy van de persoon in kwestie.

In sommige gevallen wordt een elektronische-communicatiedienst via sms geactiveerd. In dat geval zal de operator de geografische locatie van de antenne die gebruikt is voor het versturen van de sms moeten bewaren.

Leverings- en het facturatieadres van de dienst (5° en 6°)

Het leveringsadres en het facturatieadres zijn niet steeds gelijk. Het leveringsadres is natuurlijk primordiaal en noodzakelijk. Het facturatieadres is even belangrijk en noodzakelijk omdat we op deze manier ook een spoor vinden naar de persoon of organisatie die dit abonnement betaalt. In diverse dossiers stelden de autoriteiten vast dat een rechtspersoon instond voor de afhandeling van de facturen voor telefoon- of internetaansluitingen die werden gebruikt door criminelen. Het facturatieadres leidde de autoriteiten naar deze rechtspersoon.

Betalingsgegevens (6°)

De betalingsgegevens vormen voor de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten soms het enige spoor naar de eindgebruiker van een bepaalde communicatiedienst.

Telecomabonnementen zijn immers vaak afgesloten op valse naam maar dienen wel betaald te worden. Het is dan ook van belang dat er wordt bijgehouden vanaf welk rekeningnummer of betaalkaartnummer betaald wordt voor het abonnement of voor het herladen van het gebruikskrediet.

Il est demandé aux opérateurs de conserver les données suivantes:

— type de paiement (PayPal, virement, ATM, paiement par carte de crédit, etc.);

— identification du moyen de paiement (organisme émetteur de la carte de crédit, etc.);

— date et heure du paiement;

— référence de l'opération de paiement en cas de paiement en ligne.

Les données demandées sont actuellement disponibles chez les opérateurs et sont régulièrement demandées par les autorités judiciaires. Ces données de paiement constituent pour le magistrat une trace susceptible de le mener à l'utilisateur final pour lequel il pourra ensuite ouvrir une enquête auprès des organismes bancaires concernés.

Il convient de noter qu'il n'est pas demandé aux opérateurs de conserver des données qui ne pourraient pas l'être en vertu de la législation bancaire (comme par exemple des informations confidentielles sur la carte de crédit).

Données sur le service et sur l'opérateur qui l'offre (7°, 8° et 9°)

Certaines données supplémentaires concernant l'abonnement au service de communications électroniques considéré doivent fournir aux autorités des indices complémentaires quant à l'utilité d'une demande d'information auprès d'un opérateur: les services supplémentaires ou annexes auxquels l'utilisateur final est abonné, le commencement et la fin de l'abonnement et l'opérateur précédent en cas de portabilité du numéro.

Services annexes (7°)

Par "services annexes", on entend les services supplémentaires auxquels un client peut souscrire gratuitement, ou contre paiement. Pour la téléphonie, il s'agit par exemple des exemples suivants: service de répondeur, fax, service SMS, déviation d'appel, formule particulière pour appeler à tarif avantageux certains numéros ou destinations, service de Calling Card, conversation à plusieurs, etc.

Ces services annexes fournissent aux autorités bénéficiaires de la conservation des données des indices utiles quant à l'utilité d'une demande d'information auprès d'un opérateur. Ainsi, à titre d'illustration, il est intéressant pour les

Aan de operatoren wordt gevraagd de volgende gegevens te bewaren:

— type betaling (PayPal, overschrijving, ATM, kredietkaartbetaling, enz.);

— identificatie van het betaalmiddel (instantie van afgifte van de kredietkaart, enz.);

— datum en tijdstip van de betaling;

— referentie van de betalingstransactie in geval van onlinebetaling.

De gegevens die worden gevraagd zijn momenteel beschikbaar bij de operatoren en worden regelmatig opgevraagd door de gerechtelijke overheden. Deze betalingsgegevens vormen voor de magistraat dus het spoor naar de eindgebruiker waarvoor hij dan vervolgens een onderzoek kan instellen bij de betrokken bankinstellingen.

Er dient te worden opgemerkt dat de operatoren niet gevraagd wordt om gegevens te bewaren die krachtens de bankwetgeving (zoals de vertrouwelijke informatie op de kredietkaart) niet zouden mogen bewaard worden.

Gegevens over de dienst en over de aanbiedende operator (7°, 8° en 9°)

Een aantal bijkomende gegevens over het abonnement voor de beschouwde elektronische-communicatiedienst moeten de autoriteiten bijkomende aanwijzingen geven over het nut van een bevraging bij een operator: de aanvullende of bijkomende diensten waarop de eindgebruiker is geabonneerd, het begin en einde van een abonnement, de vorige operator bij nummeroverdraagbaarheid.

Aanvullende diensten (7°)

Onder "aanvullende diensten" wordt verstaan de aanvullende diensten waarop een klant gratis of tegen betaling kan intekenen. Voor de telefonie gaat het bijvoorbeeld over de volgende voorbeelden: antwoorddienst, fax, sms-dienst, doorschakeling van oproepen, bijzondere formule om bepaalde nummers of bestemmingen tegen voordeeltarief te bellen, Calling Card-dienst, groepsgesprek, enz.

Deze andere soorten van diensten verstrekken de overheden, die gebaat zijn bij de gegevensbewaring, nuttige aanwijzingen over het nut van een verzoek om informatie bij een operator. Het is bijvoorbeeld interessant dat de autoriteiten

autorités de savoir qu'un utilisateur final a souscrit un service de déviation d'appel. Cela pourrait, par exemple, indiquer que les recherches des autorités doivent plutôt s'orienter vers le numéro vers lequel la déviation d'appel est effectuée.

Pour citer un autre exemple, un abonnement de téléphonie mobile sans forfait de volume de données mobiles indique qu'il est peu probable que ce moyen de communication ait été utilisé pour une extorsion en ligne ou soit utilisé pour échanger des messages cryptés.

Pour le service d'accès à internet, il est par exemple intéressant de savoir que l'abonné bénéficie d'une bande passante particulièrement importante. Il est aussi par exemple intéressant pour les autorités de savoir que l'utilisateur final a souscrit un service similaire à Skype, mais offert par le fournisseur de l'accès à Internet, ce qui pourrait indiquer que les recherches doivent s'orienter vers les communications sur ce type de service.

La date à partir de laquelle ces services peuvent être utilisés, la date de la première utilisation du service et la date de fin des services (8°)

Il est intéressant pour les autorités de connaître la date à laquelle le service peut être utilisé et la date à laquelle il est utilisé pour la première fois. Ainsi, par exemple, l'utilisation du service peut indiquer qu'un acte a été commis avec préméditation. L'absence d'utilisation du service ou une utilisation très sporadique peut indiquer un cas de fraude et une tentative de création d'une fausse identité.

Une activation en dernière minute ou toute nouvelle activité peut être une indication intéressante dans un enlèvement avec demande de remise de rançon, par exemple.

Transfert de l'identifiant (9°)

Grâce à la libéralisation du marché des télécommunications, il est beaucoup plus facile pour les utilisateurs finaux de téléphonie de changer d'opérateur tout en conservant leur numéro. Avec l'évolution, on ne peut pas exclure qu'il soit également possible de changer d'opérateur en gardant son adresse de messagerie. Pour pouvoir s'informer auprès du bon opérateur, il importe que les services publics bénéficiaires de la conservation des données sachent précisément depuis quand l'utilisateur final est affilié à son opérateur actuel et quel était son opérateur d'origine en cas de transfert de numéro. Grâce à ces informations, les autorités (par exemple le juge d'instruction ou le procureur du Roi) peuvent adresser des requêtes supplémentaires aux bons opérateurs. Demander

weten dat een eindgebruiker geabonneerd is op een dienst voor oproepdoorschakeling. Dit zou er bijvoorbeeld op kunnen duiden dat het onderzoek van de autoriteiten eerder gericht moet zijn op het nummer waarnaar de oproep doorgeschakeld is.

Om een ander voorbeeld te vernoemen, geeft een abonnement voor mobiele telefonie zonder volume van mobiele data aan dat het onwaarschijnlijk is dat dit communicatiemiddel voor een online afpersing of een geëncrypteerde communicatie is gebruikt.

Voor de internettoegangsdienst is het bijvoorbeeld interessant om te weten dat de abonnee een bijzonder grote bandbreedte krijgt. Zo is het bijvoorbeeld ook voor de autoriteiten interessant te weten of de eindgebruiker zich heeft ingeschreven voor een dienst zoals Skype, maar die door de internetprovider wordt aangeboden, wat erop zou kunnen wijzen dat het onderzoek zich moet toespitsen op de communicatie via dit soort van dienst.

De datum vanaf wanneer die diensten gebruikt kunnen worden, de datum van het eerste gebruik van de dienst en de datum van beëindiging van de diensten (8°)

Het is interessant voor de autoriteiten om de datum te kennen waarop de dienst kan gebruikt worden en de datum waarop hij voor de eerste keer gebruikt is. Het gebruik van de dienst kan bijvoorbeeld erop wijzen dat een daad is gepleegd met voorbedachten rade. Het niet gebruiken van de dienst of een erg sporadisch gebruik kan wijzen op een geval van fraude en een poging om een valse identiteit te creëren.

Een activering op het laatste moment of elke nieuwe activiteit kan een interessante aanwijzing zijn in het kader van een ontvoering tegen losgeld, bijvoorbeeld.

Overdracht van de identifier (9°)

Met de liberalisering van de telecommunicatiemarkt is het voor telefonie-eindgebruikers veel makkelijker om over te schakelen van één operator naar een andere met behoud van hun nummer. Dankzij de ontwikkelingen kan er niet worden uitgesloten dat het eveneens mogelijk is om over te schakelen van één operator naar een andere met behoud van het e-mailadres. Om bij de juiste operator een bevraging te doen is het van belang voor de openbare diensten die baat hebben bij de bewaring van de gegevens om precies te weten sinds wanneer de eindgebruiker bij zijn huidige operator is aangesloten en van welke operator hij bij nummeroverdracht afkomstig was. Met deze informatie kunnen de autoriteiten (bijvoorbeeld de onderzoeksrechter of de procureur des

des informations à un mauvais opérateur n'a, en effet, aucun sens. Ces données permettront donc d'interroger plus efficacement et de manière plus ciblée les opérateurs. Elles éviteront en outre des demandes inutiles auprès des opérateurs et les frais de justice plus élevés générés par celles-ci. Il n'est pas suffisant de savoir que le numéro a été porté d'un opérateur à un autre. Encore faut-il savoir quand cela a eu lieu.

En ce qui concerne la portabilité des numéros, l'opérateur auquel un numéro est transféré devra pouvoir fournir l'identité de l'opérateur duquel il a reçu le numéro. L'opérateur qui transfère le numéro doit également pouvoir identifier l'opérateur qui le reçoit. En d'autres termes, lorsqu'un numéro a été porté plusieurs fois, le dernier opérateur à qui un numéro est transféré doit savoir de qui il reçoit ce numéro mais ne doit pas savoir qui est le premier opérateur de la chaîne.

10° le numéro de téléphone attribué

Le numéro de téléphone attribué permet d'identifier la personne à l'origine de toutes les communications liées à ce numéro dont disposent les services de renseignement ou les autorités judiciaires.

L'adresse de messagerie principale et les adresses de messageries employées comme alias (11°)

L'adresse de messagerie doit être entendue au sens large du terme. Pour certains services de communications interpersonnelles qui ne sont pas fondés sur la numérotation, cette adresse peut par exemple être composée d'une série de lettres et de chiffres.

Certains opérateurs offrent la possibilité de créer des adresses de messagerie alias, par exemple des adresses de messagerie anonymes.

L'adresse électronique est une donnée permettant d'attribuer une communication à une personne. Ceci est nécessaire pour pouvoir, par exemple, identifier l'auteur présumé de communications se produisant sur différentes plateformes. En outre, il permet de comparer l'adresse électronique à l'identité réelle de la personne. Si les autres données utilisées sont "fausses", l'adresse peut être un indice de l'identité réelle de l'utilisateur.

Konings) bijkomende vorderingen gericht naar de correcte operatoren zenden. Het heeft immers geen zin om gegevens bij een verkeerde operator te gaan opvragen. Deze gegevens zullen dus mee zorgen voor een efficiëntere en gerichtere vraagstelling aan de operatoren. Ze zullen bijkomend voorkomen dat onnodige vraagstellingen de operatoren belasten en dat hierdoor hogere gerechtskosten worden gegenereerd. Het volstaat niet om het nummer te kennen dat van de ene operator naar de andere is overgedragen. Bovendien moet bekend zijn wanneer dat is gebeurd.

Wat de nummeroverdraagbaarheid betreft, zal elke operator naar wie een nummer is overgedragen, de identiteit van de operator van wie hij het nummer heeft ontvangen, moeten kunnen verstrekken. De operator die het nummer overdraagt, moet ook de operator die het ontvangt kunnen identificeren. Met andere woorden, wanneer een nummer meermaals overgedragen is, moet de laatste operator naar wie een nummer is overgedragen, weten van wie hij dat nummer ontvangt, maar hoeft hij niet te weten wie de eerste operator in de rij is.

10° het toegewezen telefoonnummer

Aan de hand van het toegewezen telefoonnummer kan de persoon worden geïdentificeerd aan de bron van alle communicatie gelinkt aan dat nummer dat de inlichtingendiensten of de gerechtelijke autoriteiten hebben.

Het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden (11°)

E-mailadres moet in de ruime betekenis van het woord worden opgevat. Voor sommige nummeronafhankelijke interpersoonlijke communicatiediensten kan dit adres bijvoorbeeld samengesteld zijn uit een reeks letters en cijfers.

Sommige operatoren bieden de mogelijkheid om aliasmailadressen te creëren, bijvoorbeeld anonieme e-mailadressen.

Het e-mailadres is een gegeven aan de hand waarvan een communicatie aan een persoon kan worden toegeschreven. Dit is bijvoorbeeld nodig om de vermoedelijke auteur van communicaties op verschillende platforms te identificeren. Bovendien is het mogelijk om het e-mailadres met de werkelijke identiteit van de persoon te vergelijken. Indien de andere gebruikte gegevens "vals" zijn, kan het adres een aanwijzing zijn voor de werkelijke identiteit van de gebruiker.

L'IMSI (12°), le SUPI (13°) et le SUCI (14°)

L'IMSI ou l'identité internationale d'abonné mobile ("*International Mobile Subscriber Identity*") est un identifiant qui se trouve en principe dans la carte SIM et qui permet d'identifier de manière unique chaque abonné. Il s'agit d'une donnée que les opérateurs doivent conserver depuis l'adoption 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. Les identifiants SUPI et SUCI sont des identifiants similaires à l'IMSI et qui sont apparus avec la 5G.

Dans la norme 5G, afin d'augmenter la protection de la vie privée des utilisateurs, un identifiant supplémentaire a été rattaché au SUPI (équivalent à l'IMSI). Il s'agit du SUCI, qui correspond à l'identifiant de l'utilisateur sur le réseau. Sans cette identifiant, il ne serait pas possible, pour une communication 5G, de déterminer qui a été à la base d'une communication.

L'adresse IP à la source de la connexion (15°)

Dans son arrêt La Quadrature du Net du 6/10/2020, la CJUE autorise la conservation généralisée et indifférenciée de l'adresse IP à la source de la communication (ci-après l'adresse IP source).

Cette obligation de conservation s'applique pour les adresses IP que les opérateurs qui fournissent un accès à l'internet attribuent aux équipements de leurs abonnés, de manière à leur permettre d'utiliser les services sur internet.

Cette obligation de conservation s'applique également aux adresses IP des équipements qui se connectent à un service de communications électroniques (ex. messagerie instantanée sur internet, courrier électronique ou téléphonie par Internet). Dans son avis sur les amendements (voir point 77), l'Autorité de protection des données estime que telle conservation constitue "une ingérence dans le droit à la vie privée des personnes concernées qui devrait, à l'estime de l'Autorité, être qualifiée d'importante, notamment parce qu'elle permet de déterminer la fréquence d'utilisation d'un service de communications électroniques (ce qui va au-delà de la question de savoir l'identité de la personne qui est abonné audit service) et de déduire des informations relatives à la localisation de l'utilisateur du service (en particulier s'il s'agit de services de messagerie). L'Autorité de protection des données ajoute (voir note de bas de page n° 52) qu'"il existe plusieurs techniques qui permettent de déduire, à partir d'une adresse IP, la localisation de l'équipement terminal à qui cette adresse IP a été attribuée (et donc la localisation

De IMSI (12°), de SUPI (13°) en de SUCI (14°)

IMSI, ofwel de internationale identiteit van de mobiele abonnee ("*International Mobile Subscriber Identity*") is een identificatiecode die zich in principe in de simkaart bevindt en die het mogelijk maakt om elke abonnee op een unieke manier te identificeren. Het gaat om een gegeven dat de operatoren moeten bewaren sinds de aanneming van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie. De identifier SUPI en SUCI zijn identifier die gelijkaardig zijn aan IMSI en die verschenen zijn met 5G.

In de 5G-norm is een bijkomende identifier aan de SUPI (gelijkwaardig aan de IMSI) toegevoegd om de bescherming van de persoonlijke levenssfeer van gebruikers te verbeteren. Dit betreft de SUCI, met name de identifier van de gebruiker op het netwerk. Zonder deze identifier zou het voor een 5G-communicatie niet mogelijk zijn te bepalen wie heeft gecommuniceerd.

Het IP-adres aan de bron van de verbinding (15°)

In zijn arrest-La Quadrature du Net van 6/10/2020 staat het HvJ-EU de algemene en ongedifferentieerde bewaring toe van het IP-adres van de bron van de communicatie (hierna IP-bronadres).

Deze verplichte bewaring geldt voor de IP-adressen die de operatoren die internettoegang verschaffen toewijzen aan de apparatuur van hun abonnees, zodat zij de diensten op het internet kunnen gebruiken.

Deze bewaarplicht geldt ook voor de IP-adressen van de apparatuur die verbinding maakt met een elektronische-communicatiedienst (bijv. instant messaging via het internet, e-mail of internettelefonie). In haar advies over de amendementen (zie punt 77) is de Gegevensbeschermingsautoriteit van oordeel dat zo'n bewaring "een inmenging zou vormen in het recht op persoonlijke levenssfeer van de betrokken personen die volgens de Autoriteit als significant moet worden aangemerkt, met name omdat zij het mogelijk maakt de gebruiksfrequentie van een elektronische-communicatiedienst te bepalen (hetgeen verder gaat dan de vraag wie zich op die dienst abonneert) en informatie af te leiden over de plaats waar de gebruiker van de dienst zich bevindt (met name wanneer het berichtendiensten betreft)". De Gegevensbeschermingsautoriteit voegt daaraan toe (zie voetnoot 52): "Er bestaan immers verschillende technieken waarmee de locatie van de eindapparatuur waaraan dit IP-adres is toegewezen (en dus de locatie van de gebruiker ervan) uit een IP-adres kan worden afgeleid. Er zijn op het internet zelfs

de son utilisateur). Il existe même des services facilement accessibles sur Internet qui permettent de localiser un appareil (et la personne qui l'utilise) à partir de son adresse IP ([…]). Les grands acteurs, tels que Google ou Apple, connaissent la localisation de nombreuses adresses IP (tous les appareils mobiles dotés de services de localisation) et peuvent localiser d'autres adresses IP s'ils disposent d'informations sur les SSID Wifi ou les balises BLE que l'appareil peut voir."

La réponse du gouvernement est la suivante. D'abord, dans son arrêt la Quadrature du Net du 6/10/2020, la CJUE inclut dans le champ d'application de l'obligation de conservation de l'adresse IP à la source de la connexion des services de courrier électronique ainsi que de téléphonie par Internet: "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." (c'est nous qui soulignons)

Ensuite, le degré d'ingérence dans la vie privée des personnes concernées dépendra de l'objet de la demande de l'autorité vers l'opérateur.

Ainsi, un exploitant d'un site internet (la destination de la navigation sur internet) peut indiquer à une autorité qu'une adresse IP source a communiqué avec ce site internet (par exemple pour y mettre en vente certains produits illégaux). Dans ce cas, l'autorité cherchera à obtenir du fournisseur d'accès à internet l'identité du titulaire de l'adresse IP source. Il s'agit d'une demande d'identification.

Si l'objet de la démarche de l'autorité est de localiser un utilisateur final (par exemple en demandant à un opérateur l'adresse IP ensemble avec "les SSID Wifi ou les balises BLE que l'appareil peut voir"), il va de soi que l'ingérence sur la vie privée d'un individu sera plus grande qu'une simple identification.

diensten beschikbaar die een apparaat (en de persoon die het gebruikt) kunnen lokaliseren op basis van het IP-adres ([…]). De grote spelers, zoals Google of Apple, kennen de locatie van veel IP-adressen (alle mobiele apparaten met locatiediensten) en kunnen andere IP-adressen lokaliseren als zij informatie hebben over de Wi-Fi-SSID's of BLE-tags die het apparaat kan zien."

Het antwoord van de regering is als volgt. Allereerst neemt het HvJ-EU in zijn arrest la Quadrature du Net van 6/10/2020 elektronische-communicatiediensten, alsook internettelefoniediensten op in het toepassingsgebied van de verplichting tot bewaring van het IP-adres aan de bron van de verbinding: "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 van gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens." (wij onderlijnen)

Vervolgens zal de mate van inmenging in de persoonlijke levenssfeer van de betrokken personen afhankelijk zijn van het voorwerp van het verzoek van de autoriteit aan de operator.

Zo kan een exploitant van een website (de bestemming van het internetsurfen) aan een autoriteit meedelen dat een bron-IP-adres gecommuniceerd heeft met deze website (bijvoorbeeld om daar bepaalde onwettige producten te koop aan te bieden). In dat geval zal de autoriteit proberen om van de internetprovider de identiteit van de houder van het bron-IP-adres te verkrijgen. Het gaat om een verzoek tot identificatie.

Als het doel van de actie van de autoriteit erin bestaat een eindgebruiker te lokaliseren (bijvoorbeeld door aan een operator het IP-adres samen met "de Wi-Fi-SSID's of BLE-tags die het apparaat kan zien" te vragen), dan spreekt het vanzelf dat de inmenging in het privéleven van een individu groter zal zijn dan een eenvoudige identificatie.

Qu'une même donnée (l'adresse IP) puisse intervenir dans différents types d'opérations ressort de l'arrêt La Quadrature du Net :

"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.

153[…] 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".

Il convient de rappeler que la CJUE indique que la directive e-privacy s'oppose à la conservation généralisée et indifférenciée des adresses IP de destination, justement pour empêcher le traçage de navigation sur internet.

Au point 77 de son avis sur l'amendement, l'Autorité remet également en cause l'utilité de la conservation de l'adresse IP ayant servi à la création du compte et des adresses IP attribuées à la source de la connexion en tant que moyen pour identifier l'utilisateur final. Elle indique qu'il est assez facile pour un utilisateur de contourner cette identification, "par exemple, en souscrivant au service de communications électroniques ou en l'utilisant par le biais d'un réseau wifi public ou ouvert ou en ayant recours à Tor."

Dans son arrêt La Quadrature du Net du 6/10/2020, 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).

L'adresse IP à la source de la connexion est essentielle à des fins d'enquête judiciaire. Il s'agit de la méthode la plus utilisée et la plus courante pour identifier l'utilisateur d'un moyen de communication électronique. L'adresse IP à la source d'une connexion va, par exemple, aider à identifier la personne qui a transmis des messages de menace de mort envoyés vers une victime, ou va aider à identifier la personne qui est l'auteur du message fixant rendez-vous à une fille mineure depuis lors portée disparue.

Dat eenzelfde gegeven (het IP-adres) een rol kan spelen in verschillende soorten verrichtingen, blijkt uit het arrest- La Quadrature du Net:

"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.

153[…] 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".

Er dient eraan te worden herinnerd dat het HvJ-EU aangeeft dat de e-privacy-richtlijn gekant is tegen de algemene en ongedifferentieerde bewaring van de bestemmings-IP-adressen, net om het traceren van het surfen te verhinderen.

In punt 77 van haar advies over het amendement stelt de Autoriteit ook het nut ter discussie van de bewaring van het IP-adres dat gediend heeft voor het maken van de account en van de IP-adressen die toegewezen zijn aan de bron van de verbinding als middel om de eindgebruiker te identificeren. Zij geeft aan dat het voor een gebruiker betrekkelijk eenvoudig is om deze identificatie te omzeilen,"bijvoorbeeld door zich te abonneren op of gebruik te maken van de elektronische-communicatiedienst via een openbaar of open wifi-netwerk of door Tor te gebruiken."

In zijn arrest-La Quadrature du Net van 6/10/2020 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 IP-adres aan de bron van de verbinding is essentieel met het oog op een gerechtelijk onderzoek. Dit is ook de meest gebruikte en gangbare methode voor de identificatie van een gebruiker van een elektronische-communicatiemiddel. Het IP-adres aan de bron van de verbinding is een hulpmiddel voor de identificatie van bijvoorbeeld de persoon die doodsbedreigingen aan een slachtoffer heeft gestuurd. De identificatie van de auteur van een bericht met het oog op een ontmoeting met een minderjarig meisje dat sindsdien wordt vermist, is ook een voorbeeld.

Concernant les moyens de contourner cette mesure de conservation, il convient de prendre en compte les éléments suivants.

Il se peut que l'adresse IP à la source de la connexion soit l'adresse IP d'un réseau wifi d'un tiers par rapport à la cible (par exemple le wifi d'un établissement de l'horeca). Cependant, cette adresse IP peut permettre d'identifier ce tiers et donc de déterminer le lieu où se trouvait la cible lorsque son équipement a utilisé l'adresse IP, ce qui permettra de démarrer une enquête. Lorsque c'est possible, les autorités peuvent faire des recherches sur plusieurs adresses IP utilisées par une même personne, afin d'avoir une certitude sur l'identification de cette dernière.

Concernant l'argument de l'Autorité de protection des données selon lequel il est facile pour un utilisateur de contourner cette identification prévue par l'article 126 de la loi télécom en ayant recours à Tor, il y a toujours des moyens pour contourner toute loi, de sorte que si l'argument de l'Autorité de protection des données était suivi, aucune loi ne devrait être adoptée. Par ailleurs, le fait de devoir chercher des manières de contourner la loi rend plus difficile l'activité des criminels; ils commettent des erreurs et laissent tout de même des traces.

Par ailleurs, la conservation de l'adresse IP à la source de la connexion 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 "conservation des données", des métadonnées liées à l'adresse IP source doivent être conservées avec cette adresse pour relier l'adresse IP à une personne spécifique.

En plus de l'adresse IP, il est nécessaire de conserver les ports source qui ont été attribués, et ce pour les raisons suivantes.

Jusqu'en 2011, une adresse IP utilisée à un certain moment permettait l'identification d'une seule personne.

Pour des raisons techniques et commerciales, un grand nombre de fournisseurs d'accès à internet ont migré vers le partage d'une adresse IP entre plusieurs utilisateurs finaux.

Afin de rendre cela possible, les 65 536 ports (TCP/UDP) disponibles pour une adresse IP sont divisés entre les différents utilisateurs finaux de cette adresse IP.

Wat betreft de middelen om deze bewaringsmaatregel te omzeilen, dient rekening te worden gehouden met de volgende elementen.

Het is mogelijk dat het IP-adres aan de bron van de verbinding het IP-adres is van een wifinetwerk van een derde die niet het doelwit is (bijvoorbeeld de wifi van een horecabedrijf). Toch kan het dankzij dat IP-adres mogelijk zijn om die derde te identificeren en om dus de plaats te bepalen waar het doelwit zich bevond toen zijn apparatuur het IP-adres heeft gebruikt, waardoor een onderzoek gestart zal kunnen worden. Wanneer dat mogelijk is, kunnen de autoriteiten onderzoek doen op verschillende IP-adressen die door eenzelfde persoon zijn gebruikt, om zekerheid te hebben over de identificatie van die laatste.

Wat betreft het argument van de Gegevensbeschermingsautoriteit als zou het voor een gebruiker eenvoudig zijn om deze identificatie waarin artikel 126 van de telecomwet voorziet, te omzeilen door gebruik te maken van Tor, zijn er altijd mogelijkheden om elke wet te omzeilen, zodat, als het argument van de Gegevensbeschermingsautoriteit zou worden gevolgd, geen enkele wet aangenomen zou moeten worden. Bovendien maakt het feit van manieren te moeten zoeken om de wet te omzeilen, de activiteit van de criminelen moeilijker; zij maken fouten en laten toch sporen na.

Bovendien is het bewaren van het IP-adres aan de bron van de verbinding 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 "gegevensbewaring", moeten metagegevens verbonden aan het IP-bronadres samen met dit adres worden bewaard om het IP-adres te linken aan een specifieke persoon.

Boven op het IP-adres is het noodzakelijk om de toegewezen bronpoorten te bewaren en wel om de volgende redenen.

Tot 2011 kon aan de hand van een IP-adres dat op een bepaald moment gebruikt werd, één enkele persoon geïdentificeerd worden.

Om technische en commerciële redenen zijn een groot aantal internetproviders overgestapt naar het delen van een IP-adres onder verschillende eindgebruikers.

Om dit mogelijk te maken, worden de 65 536 poorten (TCP/UDP) die per IP-adres beschikbaar zijn, verdeeld over de verschillende eindgebruikers van dat IP-adres.

La conservation des données a pour but d'identifier de manière précise et univoque l'utilisateur final internet impliqué dans un dossier judiciaire, et d'exclure les autres.

Pour différencier les différents utilisateurs finaux d'Internet partageant une même adresse IP, et identifier de manière non ambigüe un certain utilisateur final (le suspect), il est nécessaire que le fournisseur d'accès à internet qui partage les adresses IP entre plusieurs utilisateurs finaux conserve également pour chaque utilisateur final, à côté de l'adresse IP, les ports qui lui ont été attribués et la période de cette attribution.

Lorsqu'un opérateur partage une même adresse IP publique entre plusieurs utilisateurs finaux, une seule adresse IP de l'équipement qui se connecte à un service de communications électroniques (ex. messagerie instantanée sur internet, courrier électronique ou téléphonie par Internet) ne permettra pas d'identifier de manière univoque la cible. Cela implique que pour identifier la personne recherchée, il est nécessaire que ces opérateurs conservent plusieurs adresses IP à la source de la connexion des équipements qui se connectent au compte et que les enquêteurs devront faire un recoupement entre plusieurs adresses IP.

Du point de vue des autorités, l'obligation de conservation de l'adresse IP à la source de la connexion est nettement préférable à l'absence d'une telle obligation, certains opérateurs ne conservant pas cette donnée ou trop peu de temps (parfois seulement quelques jours).

Les identifiants de l'équipement terminal (16°): introduction

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 d'autres données techniques comme l'IMEI ("*International Mobile Equipment Identity*"), le PEI ("*Permanent Equipment Identifier*", identifiant développé dans le cadre de la 5G) ou l'adresse MAC (*Media Access Control address*), 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.

Les identifiants de l'équipement terminal (16°): l'avis de l'Autorité de protection des données

De gegevensbewaring is erop gericht om interneteindgebruikers die betrokken zijn in een gerechtelijk dossier op een éénduidige manier te identificeren en anderen dus uit te sluiten.

Om de verschillende interneteindgebruikers van eenzelfde IP-adres van elkaar te onderscheiden en één bepaalde eindgebruiker (een verdachte) op éénduidige manier te kunnen identificeren, is het noodzakelijk dat de aanbieder van internettoegang die IP-adressen deelt over verschillende eindgebruikers, dus ook voor elke eindgebruiker naast het IP-adres, de toegekende poorten en de periode van deze toekenning bewaart.

Wanneer een operator eenzelfde openbaar IP-adres deelt onder verschillende eindgebruikers, dan zal het aan de hand van één IP-adres van de apparatuur die de verbinding maakt met een elektronische-communicatiedienst (bijv. instant messaging via het internet, e-mail of internettelefonie) niet mogelijk zijn om het doelwit eenduidig te identificeren. Dit houdt in dat om de gezochte persoon te identificeren, het noodzakelijk is dat deze operatoren verschillende IP-adressen aan de bron van de verbinding bewaren van de toestellen die inloggen op de account en dat de onderzoekers verschillende IP-adressen met elkaar zullen moeten vergelijken.

Vanuit het oogpunt van de veiligheidsdiensten gaat de voorkeur uit tot verplichting om het IP-adres aan de bron van de verbinding te bewaren boven de afwezigheid van een dergelijke verplichting, omdat sommige operatoren dat gegeven niet of te kortstondig (soms maar enkele dagen) bewaren.

De identifier van het eindapparaat (16°): inleiding

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 andere technische gegevens zoals de IMEI ("*International Mobile Equipment Identity*"), de PEI ("*Permanent Equipment Identifier*" identifier die in het kader van 5G is ontwikkeld) of het MAC-adres (*Media Access Control address*), waarvan de bewaring eveneens noodzakelijk is voor identificatiedoeleinden.

Gelet op het nut van deze technische gegevens voor de identificatie van daders van inbreuken online en offline, is de geplande bewaringsmaatregel evenredig.

De identifier van het eindapparaat (16°): het advies van de Gegevensbeschermingsautoriteit

Dans son avis sur le projet de loi “conservation des données”, 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 de l’IMEI 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. Par contre, l’exigence de conservation de l’adresse MAC est, elle, bien nouvelle.

Dans son avis sur l’amendement (note de bas de page n° 12), l’Autorité de protection des données précise que “Les numéros d’identification des terminaux des utilisateurs finaux permettent, s’ils sont combinés à d’autres données, de tracer ces terminaux à travers l’ensemble des services de

In haar advies over het voorontwerp van wet “gegevensbewaring” 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 IMEI 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. De eis om het MAC-adres te bewaren is daarentegen wel nieuw.

In haar advies over het amendement (voetnoot 12) zegt de Gegevensbeschermingsautoriteit: “De identificatienummers van de eindgebruikersterminals maken, in combinatie met andere gegevens, de tracering van deze terminals door alle gebruikte communicatiediensten mogelijk. De situatie is

communications utilisés. La situation est semblable pour les adresses IP attribuées à la source de la connexion: ces données ne permettent pas, à elles seules, d'effectuer le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne. Mais si elles sont combinées à d'autres données, les adresses IP attribuées à la source d'une connexion peuvent révéler le parcours d'un internaute sur Internet." (c'est nous qui soulignons)

Cependant, cette autorité n'indique pas quelles sont les "autres données" qui devraient être combinées avec l'IMEI, l'adresse MAC ou l'adresse IP et qui permettraient de tracer les terminaux à travers l'ensemble des services de communications utilisés (et notamment révéler le parcours d'un internaute sur Internet) et si ces autres données sont des données en la possession des autorités et/ou d'autres données obtenues d'un tiers (l'opérateur ou une autre personne).

Pour ce qui concerne les adresses IP à la source de la connexion, ces autres données comprennent certainement les adresses IP de destination. Or, la CJUE indique que la directive e-privacy s'oppose à la conservation généralisée et indifférenciée des adresses IP de destination, justement pour empêcher le traçage de navigation sur internet.

La conservation généralisée et indifférenciée des données visées à l'article 126 (en ce compris de l'adresse IP à la source de la connexion, de l'adresse MAC, de l'IMEI et de l'IMSI) de la loi télécom est primordiale pour les autorités.

L'ingérence concrète sur la vie privée d'un individu sera fonction de l'objet de la demande d'une autorité envers un opérateur: cette demande vise-t-elle à localiser une personne ou à l'identifier?

S'il apparaissait de la pratique que les IMSI, les IMEI ou l'adresse MAC combinés avec d'autres données permettaient la localisation précise de l'équipement terminal, alors une demande envers l'opérateur d'obtenir ces données devrait être considérée comme une demande de localisation de l'abonné (et pas comme une demande d'identification).

Les identifiants de l'équipement terminal (16°): l'avis du Conseil d'État

Dans son avis sur l'amendement, le Conseil d'État indique que "L'auteur de l'amendement veillera toutefois à s'assurer que les données reprises à l'article 126, § 1er, en projet, autres que celles relatives à l'identité civile, ne présentent pas de

vergelijkbaar voor IP-adressen die zijn toegewezen aan de bron van de verbinding: met deze gegevens alleen kan het surftraject van een gebruiker, en bijgevolg zijn onlineactiviteit, niet uitputtend worden getraceerd. Maar in combinatie met andere gegevens kunnen de IP-adressen die aan de bron van een verbinding zijn toegewezen, het traject van een internetgebruiker op het internet onthullen." (we onderlijnen)

Deze autoriteit vermeldt evenwel niet wat die "andere gegevens" zijn die gecombineerd zouden moeten worden met de IMEI, het MAC-adres of het IP-adres en die het mogelijk zouden maken om de eindapparatuur te traceren door alle gebruikte communicatiediensten (en met name het traject van een internetgebruiker te onthullen) en of die andere gegevens gegevens zijn waarover de autoriteiten beschikken en/of andere gegevens die van een derde (de operator of een andere persoon) worden verkregen.

Wat betreft de IP-adressen aan de bron van de verbinding, omvatten deze andere gegevens zeker de bestemmings-IP-adressen. Welnu, het HvJ-EU geeft aan dat de e-privacyrichtlijn gekant is tegen de algemene en ongedifferentieerde bewaring van de bestemmings-IP-adressen, net om het traceren van het surfen te verhinderen.

De algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126 (inclusief van het IP-adres aan de bron van de verbinding, van het MAC-adres, van de IMEI en van de IMSI) van de telecomwet is van essentieel belang voor de veiligheidsdiensten.

De concrete inmenging in de privacy van een individu zal afhankelijk zijn van het voorwerp van het verzoek van een autoriteit aan een operator: heeft dat verzoek tot doel een persoon te lokaliseren of te identificeren?

Mocht uit de praktijk blijken dat de IMSI, de IMEI of het MAC-adres in combinatie met andere gegevens het mogelijk zouden maken om de plaats van de eindapparatuur nauwkeurig te bepalen, dan zou een verzoek aan de operator om deze gegevens te verkrijgen beschouwd moeten worden als zijnde een verzoek om lokalisatie van de abonnee (en niet als een verzoek om identificatie).

De identifier van het eindapparaat (16°): het advies van de Raad van State

In zijn advies over het amendement vermeldt de Raad van State: "L'auteur de l'amendement veillera toutefois à s'assurer que les données reprises à l'article 126, § 1er, en projet, autres que celles relatives à l'identité civile, ne présentent pas

risques similaires, en termes de traçage de l'utilisateur, à ceux évoqués par la Cour de justice en ce qui concerne les adresses IP attribuées à la source de la connexion, auquel cas l'accès à ces données devrait également être restreint, à l'instar de ce que prévoit l'article 127/1, § 3, alinéa 4, en projet."

Il convient d'abord de noter que la remarque du Conseil d'État porte sur l'accès des autorités aux données (et non pas sur les finalités de la conservation des données), ce qui est logique dès lors que l'ingérence sur la vie privée de l'individu se concrétise lorsque l'autorité demande à obtenir des données de l'opérateur. Le gouvernement est d'avis que l'adresse MAC, l'IMEI ou l'IMSI ne présentent pas un risque de traçage du parcours de navigation d'un internaute, et ce pour les raisons suivantes.

Il existe des différences entre l'adresse IP d'une part et l'adresse MAC, l'IMSI ou l'IMEI d'autre part:

— les "*brokers*" de données peuvent voir les adresses IP qui se connectent à un site Internet mais ne voient pas l'adresse MAC, l'IMSI ou l'IMEI;

— alors que la CJUE a estimé qu'il y a un risque de traçage sur base de l'adresse IP, elle n'a pas considéré qu'il en était de même pour l'IMSI, l'IMEI ou les adresses MAC.

Il n'est pas prévu que les opérateurs doivent conserver pour les autorités le parcours de navigation de l'internaute, qui ne peut donc pas être combiné avec l'adresse MAC ou l'IMEI.

Les identifiants de l'équipement terminal (16°): l'IMEI

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

de risques similaires, en termes de traçage de l'utilisateur, à ceux évoqués par la Cour de justice en ce qui concerne les adresses IP attribuées à la source de la connexion, auquel cas l'accès à ces données devrait également être restreint, à l'instar de ce que prévoit l'article 127/1, § 3, alinéa 4, en projet."

Allereerst moet erop worden gewezen dat de opmerking van de Raad van State betrekking heeft op de toegang van de autoriteiten tot de gegevens (en niet op de doeleinden van de gegevensbewaring), hetgeen logisch is omdat de inmenging in de persoonlijke levenssfeer van het individu concrete vorm aanneemt wanneer de autoriteit vraagt om van de operator gegevens te krijgen. De regering is van oordeel dat het MAC-adres, de IMEI of de IMSI geen gevaar vormen voor het traceren van de zoekgeschiedenis van een internetgebruiker, en wel om de volgende redenen.

Er zijn verschillen tussen het IP-adres enerzijds en anderzijds het MAC-adres, de IMSI of de IMEI:

— de "data brokers" kunnen de IP-adressen zien die verbinding maken met een website, maar zien niet het MAC-adres, de IMSI of de IMEI;

— terwijl het HvJ-EU geoordeeld heeft dat er een traceerrisico is op basis van het IP-adres, was het niet van oordeel dat hetzelfde gold voor de IMSI, de IMEI of de MAC-adressen.

Het is niet voorgeschreven dat de operatoren voor de autoriteiten de zoekgeschiedenis van een internetgebruiker moeten bewaren, die dus niet gecombineerd kan worden met het MAC-adres of met de IMEI.

De identifier van het eindapparaat (16°): de IMEI

Het HvJ-EU heeft in het arrest van 2 oktober 2018 *Ministerio Fiscal* (C-207/16, 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 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.

L'IMEI constitue une donnée essentielle à l'identification de l'auteur présumé d'une infraction. L'on observe en pratique que parfois les auteurs d'infractions changent de cartes SIM et les placent dans un seul et même appareil pour communiquer. Sans disposer du numéro IMEI de l'équipement terminal, la pratique fréquente décrite ci-dessus permettrait de faire obstacle à l'enquête ou à l'instruction.

Le numéro IMEI révèle également aussi certaines indications essentielles sur le type d'équipement terminal utilisé par les suspects. Il s'agit, par ailleurs, d'une donnée disponible à partir des antennes des opérateurs. Cette donnée peut donc, par exemple, permettre de déterminer quels appareils étaient présents à proximité d'un cadavre lorsque celui-ci a été déposé, dans le cadre d'une demande de métadonnées sur base de l'article 88*bis* du Code d'instruction criminelle.

Par ailleurs, l'IMEI permet par exemple également de vérifier si le même appareil utilise plusieurs cartes SIM. Cela peut indiquer qu'une personne ciblée possède plusieurs cartes SIM ou que l'appareil est transmis au sein d'un certain groupe de personnes. Si une certaine carte SIM est enregistrée sous un faux nom, mais qu'elle est utilisée dans un appareil auquel peut être associée une seconde carte SIM dont le titulaire est correctement identifié, cela donne une indication sur le véritable utilisateur de la première carte SIM.

Les identifiants de l'équipement terminal (16°): l'adresse MAC

Dans son avis sur les amendements (note de bas de page n° 13), l'Autorité de protection des données relève "que les adresses MAC sont modifiées très régulièrement (depuis 2014). La collecte de cette information nécessite dès lors un stockage massif de données et n'est que peu utile."

L'adresse MAC permet d'identifier le véritable équipement utilisé et remplit donc la même fonction que l'IMEI. Lorsque de nombreux utilisateurs sont connectés à un wifi, l'adresse MAC permet de cibler la personne recherchée par les autorités ("le *target*").

L'adresse MAC est très utile pour les services de communications électroniques pour lesquels une carte SIM n'est pas utilisée.

Même si l'adresse MAC est changeante ("*rolling MAC address*"), en cas de reconnexion à un wifi connu, elle va reprendre un format déjà préalablement utilisé, ce qui permettra aux autorités de recouper l'information en vue d'arriver à une identification.

De IMEI is een essentieel gegeven voor het identificeren van de vermoedelijke dader van een inbreuk. In de praktijk wordt vastgesteld dat daders soms SIM-kaarten verwisselen en deze in een en hetzelfde toestel plaatsen om te communiceren. Zonder het IMEI-nummer van de eindapparatuur zou de hierboven beschreven praktijk het onderzoek of het gerechtelijk onderzoek belemmeren.

Het IMEI-nummer onthult ook bepaalde belangrijke informatie over het door verdachten gebruikte type van eindapparatuur. Dit gegeven is ook beschikbaar via de antennes van de operatoren. In het kader van een verzoek tot verstrekking van metagegevens op basis van artikel 88*bis* van het Wetboek van Strafvordering maakt dit gegeven de identificatie mogelijk van toestellen die zich in de nabijheid van een lijk bevonden toen het werd gedumpt.

De IMEI kan ook worden gebruikt om na te gaan of hetzelfde toestel meerdere SIM-kaarten gebruikt. Dit kan erop wijzen dat een betrokken persoon meerdere SIM-kaarten heeft of dat het toestel binnen een bepaalde groep mensen wordt bezorgd. Indien een bepaalde SIM-kaart onder een valse naam is geregistreerd, maar wordt gebruikt in een toestel waaraan mogelijk een tweede SIM-kaart is gekoppeld waarvan de houder correct is geïdentificeerd, geeft dit een aanwijzing over de werkelijke gebruiker van de eerste SIM-kaart.

De identifier van het eindapparaat (16°): het MAC-adres

In haar advies over de amendementen (voetnoot 13) merkt de Gegevensbeschermingsautoriteit op "dat MAC-adressen zeer regelmatig worden gewijzigd (sinds 2014). Het verzamelen van deze informatie vereist dan ook massale gegevensopslag en is van weinig nut."

Het MAC-adres maakt de identificatie van de daadwerkelijk gebruikte apparatuur mogelijk en heeft daarom dezelfde functie als de IMEI. Wanneer veel gebruikers op een wifi zijn aangesloten, kunnen de autoriteiten zich via het MAC-adres op de gezochte persoon ("de target") richten.

Het MAC-adres is zeer nuttig voor elektronische communicatiediensten waarbij geen SIM-kaart wordt gebruikt.

Zelfs wanneer het MAC-adres veranderlijk is ("*rolling MAC address*") zal het, wanneer opnieuw verbinding wordt gemaakt met een bekende wifi, een formaat aannemen dat reeds eerder werd gebruikt, waardoor de autoriteiten de informatie kunnen natrekken om tot een identificatie te komen.

La “nomadicité” croissante des services de téléphonie nécessite également d’inclure l’adresse MAC (*Media Access Control*) parmi les données d’identification des équipements terminaux.

En effet, un numéro de téléphone (fixe ou mobile) n’est plus uniquement utilisé sur un équipement téléphonique classique (appareil téléphonique classique, fixe ou mobile), mais peut également être rendu “nomade” au sens de l’arrêté royal du 27 avril 2007 relatif à la gestion de l’espace de numérotation national et à l’attribution et au retrait des droits d’utilisation de numéros (“arrêté royal numérotation”). Ceci signifie qu’une communication téléphonique peut être passée avec ce numéro par l’intermédiaire de différents types de logiciels ou d’équipements, en ce compris par un ordinateur habituellement identifié par son adresse MAC.

L’exploitation par les autorités de l’adresse MAC est une solution de dernier recours, dans le cas où l’opérateur n’arrive pas à identifier l’utilisateur d’un de ses services de communication à l’aide d’un autre identifiant (par exemple l’IMEI ou le PEI). Dans certains cas (par exemple si les enquêteurs ne disposent que de l’adresse MAC), l’adresse MAC sera la seule manière pour les enquêteurs d’identifier l’utilisateur final.

La conservation de l’adresse MAC se justifie également par le fait que l’IMEI ou le PEI peut ne pas apparaître ou ne pas être disponible en fonction de la technologie utilisée ou d’un problème technique sur le réseau. Une personne, qui veut se soustraire à des poursuites judiciaires, peut également modifier les identifiants de son appareillage.

Les opérateurs business sont dispensés de conserver l’adresse MAC, étant donné que la conservation d’une telle donnée ne représente pas d’utilité pratique pour les autorités.

Suite à la consultation publique relative aux projets d’amendements, il parait utile de préciser que lorsque l’opérateur ne traite pas ou ne génère pas l’identifiant de l’équipement terminal de l’utilisateur final, il y a lieu de conserver, à défaut, “l’identifiant de l’équipement qui est le plus proche de l’équipement terminal”. Il est bien entendu qu’en toute hypothèse (même dans ce dernier cas), il ne doit s’agir que d’équipements utilisés pour la fourniture du réseau ou du service de communication électronique concerné (p.ex. l’adresse MAC d’un ordinateur utilisé comme serveur proxy). Il ne s’agit évidemment pas d’identifier d’autres équipements proches de l’utilisateur final (équipements d’un autre abonné) et qui n’ont aucun lien avec la fourniture du réseau ou du service de communication électronique concerné.

Door de toenemende “nomadiciteit” van de telefoniediensten, dient het MAC-adres (*Media Access Control*) eveneens te worden opgenomen als identificatiegegeven van de eindapparatuur.

Een (vast of mobiel) telefoonnummer wordt immers niet langer enkel voor een klassiek telefoontoestel gebruikt (vast of mobiel klassiek telefoontoestel), maar kan ook “nomadisch” gemaakt worden in de zin van het koninklijk besluit van 27 april 2007 betreffende het beheer van de nationale nummeringsruimte en de toekenning en intrekking van gebruiksrechten voor nummers (“nummerings-KB)”. Dat betekent dat een telefonische communicatie via verschillende soorten van software of apparatuur tot stand kan worden gebracht met datzelfde nummer, inclusief via een computer die doorgaans aan de hand van zijn MAC-adres wordt geïdentificeerd.

Het gebruik van het MAC-adres door de autoriteiten is een laatste redmiddel, in het geval dat de operator er niet in slaagt de gebruiker van één van zijn communicatiediensten aan de hand van een andere identifier (bijvoorbeeld de IMEI of de PEI) te identificeren. In sommige gevallen (bijvoorbeeld als de onderzoekers alleen het MAC-adres hebben) is het MAC-adres voor de onderzoekers de enige manier om de eindgebruiker te identificeren.

De bewaring van het MAC-adres wordt ook verantwoord door het feit dat het kan gebeuren dat de IMEI of de PEI niet te zien zijn of niet beschikbaar zijn afhankelijk van de toegepaste technologie of door een technisch probleem op het netwerk. Een persoon die zich aan gerechtelijke vervolging wil onttrekken, kan ook de identifier van zijn apparatuur wijzigen.

Zakelijke operatoren zijn ervan vrijgesteld om het MAC-adres te bewaren, aangezien het bewaren van zo’n gegeven geen praktisch nut heeft voor de veiligheidsdiensten.

Naar aanleiding van de openbare raadpleging over de ontwerpen van amendement, lijkt het nuttig om te preciseren dat wanneer de operator de identifier van de eindapparatuur van de eindgebruiker niet verwerkt of genereert, er reden is om, bij gebrek, “de identificatiecode van de apparatuur die zich het dichtst bij die eindapparatuur bevindt” te bewaren. Vast staat dat in elk geval (zelfs in dat laatste geval) het enkel mag gaan over apparatuur die gebruikt is voor het aanbieden van het netwerk of de dienst voor elektronische communicatie in kwestie (bijv. het MAC-adres van een computer die als proxyserver is gebruikt). Het gaat vanzelfsprekend niet erom andere apparatuur in de buurt van de eindgebruiker (apparatuur van een andere abonnee) te identificeren, die geen enkele link heeft met de levering van het netwerk of de dienst voor elektronische communicatie in kwestie.

Les autres identifiants ajoutés par arrêté royal (17°)

La possibilité pour le Roi d'imposer aux opérateurs de conserver d'autres données a été prévue au cas où il serait nécessaire d'imposer de manière urgente la conservation de cette donnée, sans devoir attendre la modification de la loi. Ainsi, il pourrait apparaitre que l'absence de conservation de certaines données constitue un problème opérationnel majeur pour les autorités. Dans ce cas, il sera nécessaire d'adapter au plus vite un arrêté royal qui prévoit la conservation des données manquantes. La même explication vaut mutatis mutandis en ce qui concerne l'article 126/2, § 2, alinéa 1er, 10°.

Durée de conservation (paragraphe 2)

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 que l'opérateur doit conserver afin de pouvoir vérifier l'identité de l'abonné (conservation jusqu'à 12 mois après la fin du contrat). Les 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.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

De andere identifiers toegevoegd bij koninklijk besluit (17°)

Er is voorzien in de mogelijkheid voor de Koning om de operatoren te verplichten andere gegevens te bewaren, in het geval dat het noodzakelijk zou zijn om dringend de bewaring van dat gegeven op te leggen zonder te moeten wachten op de wetswijziging. Zo zou kunnen blijken dat de afwezigheid van bewaring van sommige gegevens een groot operationeel probleem vormt voor de veiligheidsdiensten. In dat geval zal het nodig zijn om zo snel mogelijk een koninklijk besluit aan te nemen dat in de bewaring van de ontbrekende gegevens voorziet. Dezelfde uitleg geldt mutatis mutandis wat betreft het ontworpen artikel 126/2, § 2, eerste lid, 10°.

Bewaringstermijn (paragraaf 2)

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 operator moet worden bewaard om de identiteit van de abonnee te kunnen verifiëren (bewaring tot 12 maanden na het einde van het contract). De 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 eindapparaat 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

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 2 **DU GOUVERNEMENT**

Art. 9

Dans l'article 126/1 proposé, apporter les modifications suivantes:

1° remplacer le paragraphe 2 par ce qui suit:

*"§ 2. Les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'applique l'obligation de conservation visée au paragraphe 1er sont énumérées à l'article 126/2."***;**

2° dans le paragraphe 4, alinéa 4, remplacer les mots "dans l'arrêté royal visé au paragraphe 2, alinéa 2" **par les mots** *"à l'article 126/2"***.**

JUSTIFICATION

Les présentes modifications effectuées à l'article 9, qui insère un article 126/1 dans la loi du 13 juin 2005 relative aux communications électroniques, sont une conséquence de l'insertion d'un nouvel article 126/2 dans la même loi, qui énumère les données qui doivent être conservées sur base de l'article 126/1. En effet, il a été décidé, suite à l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour Constitutionnelle, d'énumérer les métadonnées qui doivent être conservées dans la loi plutôt que dans un arrêté royal. Par conséquent, la délégation au Roi qui était prévue à l'article 126/1, § 2, n'a plus de raison d'être.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Nr. 2 **VAN DE REGERING**

Art. 9

In het voorgestelde artikel 126/1 de volgende wijzigingen aanbrengen:

1° paragraaf 2 vervangen als volgt:

*"§ 2. De elektronische-communicatiemetagegevens, met inbegrip van de metagegevens voor de oproeppogingen zonder resultaat, waarop de in paragraaf 1 bedoelde bewaarplicht van toepassing is, worden opgesomd in artikel 126/2."***;**

2° In paragraaf 4, vierde lid, de woorden "in het koninklijk besluit bedoeld in paragraaf 2, tweede lid" **vervangen door de woorden** *"in artikel 126/2"***.**

VERANTWOORDING

De huidige wijzigingen van artikel 9, dat een artikel 126/1 invoegt in de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn een gevolg van de invoeging van een nieuw artikel 126/2 in diezelfde wet, waarin de gegevens worden opgesomd die op grond van artikel 126/1 moeten worden bewaard. Naar aanleiding van arrest nr. 158/2021 van het Grondwettelijk Hof van 18 november 2021 is inderdaad besloten de metagegevens die moeten worden bewaard, in de wet op te nemen in plaats van in een koninklijk besluit. Bijgevolg is de in artikel 126/1, § 2, bedoelde delegatie aan de Koning niet langer nodig.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 3 **DU GOUVERNEMENT**

Art. 9/1 *(nouveau)*

Insérer un article 9/1, rédigé comme suit:

"Art. 9/1. Dans la même loi, un article 126/2 est inséré, rédigé comme suit:

"Art. 126/2. § 1er. Pour l'application du présent article, il y a lieu d'entendre par:

"Communication": toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit.

§ 2. Les données visées à l'article 126/1, § 2, qui doivent être conservées en exécution de l'article 126/1 par les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que par les opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, sont les suivantes:

1° la description et les caractéristiques techniques du service de communications électroniques utilisé lors de la communication;

2° les données d'identification visées à l'article 126, § 1er, 2°, 10° à 14° et 16°, du destinataire de la communication;

3° pour les services de communications électroniques à l'exception des services d'accès à Internet, l'adresse IP utilisée par le destinataire de la communication, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués;

Nr. 3 **VAN DE REGERING**

Art. 9/1 *(nieuw)*

Een artikel 9/1 invoegen, luidende:

"Art. 9/1. In dezelfde wet wordt een artikel 126/2 ingevoegd, luidende:

"Art. 126/2. § 1. Voor de toepassing van dit artikel wordt verstaan onder:

"Communicatie": informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een publiek beschikbare elektronischecommunicatiedienst. Dit omvat niet de informatie die via een openbare omroepdienst over een elektronischecommunicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gelinkt aan de identificeerbare abonnee of gebruiker die deze informatie ontvangt.

§ 2. De gegevens bedoeld in artikel 126/1, § 2, die in uitvoering van artikel 126/1 bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische- communicatiediensten aanbieden, alsook door de operatoren die elektronische-communicatienetwerken aanbieden die het aanbieden van die diensten mogelijk maken, zijn de volgende:

1° de beschrijving en de technische karakteristieken van de elektronische-communicatiedienst die werd aangewend tijdens de communicatie;

2° de identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14° en 16°, van de geadresseerde van de communicatie;

3° voor de elektronische-communicatiediensten met uitzondering van de internettoegangsdiensten, het IP-adres dat gebruikt is door de geadresseerde van de communicatie, het tijdstempel alsook, in geval van gedeeld gebruik van een IP-adres van de geadresseerde, de poorten die aan hem zijn toegewezen;

4° 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;

5° la date et l'heure exacte du début et de la fin de la session du service de communication électronique concerné, en ce compris la date et l'heure exacte du début et de la fin de l'appel;

6° les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile, qui ont été utilisé(e)s pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations;

7° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session;

8° pour ce qui concerne les services de communications électroniques mobiles, la date et l'heure 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;

9° pour ce qui concerne les services de communications électroniques mobiles, la localisation de l'équipement terminal et la date et l'heure de cette localisation chaque fois que l'opérateur cherche à connaître quels équipements terminaux sont connectés au réseau;

10° les autres identifiants relatifs au destinataire de la communication électronique, à son équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, après avis de l'Autorité de protection des données et de l'Institut, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

4° in geval van een groepsgesprek, oproepdoorschakeling of –doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

5° de datum en het exacte tijdstip van de aanvang en het einde van de sessie van de betrokken elektronische-communicatiedienst, waaronder de datum en het exacte tijdstip van de aanvang en het einde van de oproep;

6° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie, alsook de exacte data en tijdstippen van deze verschillende locaties;

7° het tijdens de duur van de sessie geüploade en gedownloade volume van gegevens;

8° voor wat betreft de mobiele elektronische-communicatiediensten, de datum en het tijdstip van de verbinding van de eindapparatuur met het netwerk wegens van het opstarten van die apparatuur, en het moment waarop de verbinding van deze eindapparatuur met het netwerk wordt verbroken wegens het uitschakelen van die apparatuur;

9° voor wat betreft de mobiele elektronische-communicatiediensten, de locatie van de eindapparatuur en de datum en het tijdstip van deze locatie telkens wanneer de operator wil weten welke eindapparatuur is verbonden met zijn netwerk;

10° de andere identifiers met betrekking tot de geadresseerde van de elektronische communicatie, tot zijn eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, na advies van de Gegevensbeschermingsautoriteit en het Instituut, op voorwaarde dat dit besluit door de wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

Par dérogation à l'article 126/1, la durée de conservation de la donnée visée à l'alinéa 1er, 8°, est de 6 mois après avoir été générée ou traitée.

L'arrêté royal visé au paragraphe 1er, 10°, ne porte pas sur le contenu des communications électroniques.

Le Roi peut, après avis de l'Autorité de protection des données et de l'Institut, préciser les données visées à l'alinéa 1er.

§ 3. La combinaison des données conservées en exécution de l'article 126 et du présent article doit permettre d'établir la relation entre l'origine de la communication et sa destination.

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 en matière de précision et de fiabilité auxquelles les données visées au présent article doivent répondre."."

In afwijking van artikel 126/1 bedraagt de bewaartermijn van het gegeven bedoeld in het eerste lid, 8°, 6 maanden nadat het is gegenereerd of verwerkt.

Het koninklijk besluit bedoeld in paragraaf 1, 10°, slaat niet op de inhoud van de elektronische communicatie.

De Koning kan, na advies van de Gegevensbeschermingsautoriteit en het Instituut, de gegevens bedoeld in eerste lid, preciseren.

§ 3. De combinatie van de gegevens bewaard in uitvoering van artikel 126 en van dit artikel moet het mogelijk maken om de relatie te leggen tussen de bron en de bestemming van de communicatie.

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 inzake nauwkeurigheid en betrouwbaarheid bepalen waaraan de gegevens bedoeld in dit artikel moeten beantwoorden."."

JUSTIFICATION

Nécessité du présent amendement à la suite de l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle

Le présent amendement vise à introduire un nouvel article 9/1 dans le projet de loi, qui lui-même introduit un nouvel article 126/2 dans la loi relative aux communications électroniques.

Le 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 (ci-après le projet de loi "conservation des données") a pour objet, entre autres, d'introduire un nouvel article 126/1 dans la loi relative aux communications électroniques, concernant la conservation des données sur base d'un critère géographique.

VERANTWOORDING

Noodzaak van dit amendement ingevolge arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof

Dit amendement wenst een nieuw artikel 9/1 in te voeren in het wetsontwerp, dat op zich een nieuw artikel 126/2 invoert in de wet betreffende de elektronische communicatie.

Het 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 (hierna het wetsontwerp "gegevensbewaring") beoogt, onder meer, de invoering van een nieuw artikel 126/1 in de wet betreffende de elektronische communicatie, aangaande de bewaring van gegevens op basis van een geografisch criterium.

Dans un arrêt n° 158/2021 du 18 novembre 2021, la Cour constitutionnelle a annulé l'article 2 de la loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, au motif que cet article ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération.

Selon la Cour, de tels éléments essentiels d'un traitement de données à caractère personnel ne sauraient être couverts par l'habilitation vague conférée par l'article 127, § 1er, alinéa 1er, de la loi du 13 juin 2005 et qui consiste à prendre les "mesures techniques et administratives" nécessaires en vue de rendre l'utilisateur final identifiable.

Même si l'annulation de l'article 2 précité ne porte pas sur les métadonnées à conserver dans le cadre de l'article 126/1, et que cet article contient une délégation explicite et spécifique au Roi pour fixer les métadonnées de communications électroniques qui sont visées par l'article 126/1, le législateur estime, par souci de cohérence, qu'il est préférable d'énumérer l'ensemble des données à conserver dans la loi. Ainsi, à l'instar des données d'identification reprises à l'article 126, les données visées aux paragraphes 2 des articles 3 à 6 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 ont été déplacées vers ce nouvel article 126/2.

Considérations générales sur l'article 126/2

À l'instar des données d'identification énumérées à l'article 126, le présent article 126/2, § 2, reprend et adapte les données précédemment listées aux paragraphes 2 des articles 3 à 6 de l'arrêté royal du 19 septembre 2013 non plus au moyen de listes de données distinctes par type de service de communications électroniques (téléphone fixe, téléphonie mobile, service d'accès à internet, service de courrier électronique et service de téléphonie par internet), mais au moyen d'une seule liste de données commune pour l'ensemble de ces services. Une liste commune se justifie compte tenu de la convergence croissante des services de communications électroniques et de l'extension de cette dernière notion, ainsi que de la notion d'opérateur aux acteurs OTT, à la suite de la transposition dans la loi télécom 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). Il incombe dès lors à l'opérateur

In arrest nr. 158/2021 van 18 november 2021 heeft het Grondwettelijk Hof artikel 2 van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst nietig verklaard, op grond van het feit dat dit artikel niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking worden genomen.

Dergelijke essentiële elementen van een verwerking van persoonsgegevens kunnen volgens het Hof niet worden begrepen onder de vage machtiging in artikel 127, § 1, eerste lid, van de wet van 13 juni 2005 om de nodige "technische en administratieve maatregelen" te nemen met het oog op de identificeerbaarheid van de eindgebruiker.

Ook al heeft de vernietiging van het voormelde artikel 2 geen betrekking op de metagegevens die in het kader van artikel 126/1 moeten worden bewaard, en bevat dit artikel een uitdrukkelijke en specifieke delegatie aan de Koning om de in artikel 126/1 bedoelde elektronische-communicatiemetagegevens te bepalen, toch is de wetgever van oordeel dat het ter wille van de coherentie de voorkeur verdient alle gegevens die moeten worden bewaard, in de wet op te sommen. Zo zijn, naar het voorbeeld van de identificatiegegevens opgenomen in artikel 126, de gegevens bedoeld in de paragrafen 2 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, verplaatst naar dit nieuwe artikel 126/2.

Algemene overwegingen betreffende artikel 126/2

Naar het voorbeeld van de identificatiegegevens opgesomd in artikel 126, neemt onderhavig artikel 126/2, § 2, de gegevens over die voordien zijn opgesomd in de paragrafen 2 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013 en past deze aan, niet langer door middel van afzonderlijke lijsten van gegevens per type van elektronische-communicatiediensten (vaste telefonie, mobiele telefonie, internettoegangsdienst, e-maildienst via internet en een internettelefoniedienst), maar door middel van een enkele gemeenschappelijke lijst van gegevens voor al die diensten. Een gemeenschappelijke lijst is gerechtvaardigd rekening houdend met de toenemende convergentie van de elektronische-communicatiediensten en met de uitbreiding van dat laatste begrip, alsook van het begrip operator naar de OTT-spelers naar aanleiding van de omzetting in de telecomwet van het Europees wetboek voor elektronische communicatie (Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling

de vérifier quelles données de cette liste sont traitées ou générées par lui dans le cadre des services ou réseaux qu'il offre. Cette vérification doit être effectuée pour chaque type de service offert par l'opérateur, de sorte que l'ensemble des données pertinentes soient conservées pour chaque service et pour chaque utilisateur final.

Certaines adaptations techniques sont, par ailleurs, justifiées par la spécificité de la technologie 5G. Il s'agit, en particulier de l'ajout, pour les besoins de cette technologie, du "*Subscription Permanent Identifier*" ou "SUPI", du "*Subscription Concealed Identifier*" ou "SUCI" et du "*Permanent Equipment Identifier*" ou "PEI" parmi les "données d'identification visées à l'article 126, § 1er, 2°, 10° à 14 et 16°, du destinataire de la communication" visées au paragraphe 2, 2°.

Le paragraphe 2, 11°, du nouvel article 126/2 prévoit également la possibilité de conserver une donnée ayant une fonction équivalente lorsqu'une donnée reprise dans ces paragraphes n'est pas disponible. Cette possibilité permet:

— à la loi de résister au temps. Il est important que la loi ne soit pas immédiatement dépassée par les rapides évolutions technologiques dans le secteur des communications électroniques (ex. 5G);

— de s'assurer que la loi est adaptée à tous les opérateurs. Il convient à cet égard de rappeler que la notion d'opérateur couvre des entreprises pouvant être très différentes (opérateur de réseau classique vs opérateur qui fournit des services de communications interpersonnelles qui ne sont pas basés sur la numérotation);

— de s'assurer que la loi est technologiquement neutre.

Paragraphe 1er

Le premier paragraphe reprend la définition de "communication" qui se trouve à l'article 2, d), de la directive "vie privée et communications électroniques" (directive 2002/58/CE) et qui est nécessaire à la bonne compréhension de cet article. Cette définition est très large, dès lors qu'elle vise tout type d'informations (signes, signaux, écrits, images, sons ou données de toute nature) et dès lors qu'une partie à la communication peut être une machine (Internet des objets).

van het Europees wetboek voor elektronische communicatie). Het is dus de verantwoordelijkheid van de operator om te verifiëren welke gegevens van die lijst verwerkt of gegenereerd zijn door hem in het kader van de diensten of netwerken die hij aanbiedt. Die verificatie moet worden uitgevoerd voor elk type van dienst die door de operator aangeboden wordt, zodat alle relevante gegevens bewaard worden voor elke dienst en voor elke eindgebruiker.

Een aantal technische aanpassingen worden gerechtvaardigd door de specificiteit van de 5G-technologie. Het gaat in het bijzonder om de toevoeging, ten behoeve van die technologie, van de "*Subscription Permanent Identifier*" of "SUPI", van de "*Subscription Concealed Identifier*" of "SUCI" en van de "*Permanent Equipment Identifier*" of "PEI" aan de "identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14° en 16°, van de geadresseerde van de communicatie" bedoeld in paragraaf 2, 2°.

Paragraaf 2, 11°, van het nieuwe artikel 126/2 voorziet ook in de mogelijkheid dat, wanneer een in die paragrafen vermeld gegeven niet beschikbaar is, een gegeven met een gelijkwaardige functie bewaard wordt. Deze mogelijkheid maakt het mogelijk:

— voor de wet om tijdsbestendig te zijn. Het is belangrijk dat de wet niet onmiddellijk achterhaald raakt door snelle technologische ontwikkelingen in de elektronische-communicatiesector (bijv. 5G);

— om zich ervan te vergewissen dat de wet aangepast is aan alle operatoren. Wat dat betreft dient te worden herhaald dat het begrip van operator ondernemingen dekt die sterk verschillend kunnen zijn (klassieke netwerkoperator versus een operator die nummeronafhankelijke interpersoonlijke communicatiediensten aanbiedt);

— om zich ervan te vergewissen dat de wet technologisch neutraal is.

Paragraaf 1

De eerste paragraaf neemt de definitie van "communicatie" over die te vinden is in artikel 2, d), van de richtlijn "betreffende privacy en elektronische communicatie" (Richtlijn 2002/58/EG) en die noodzakelijk is voor het goede begrip van dit artikel. Deze definitie is erg ruim daar ze elk type van informatie beoogt (tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard) en daar een machine een bij de communicatie betrokken partij kan zijn (internet der dingen).

Paragraphe 2

Le deuxième paragraphe énumère les données visées à l'article 126/1, § 2, qui doivent être conservées en exécution de l'article 126/1 par 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.

La description et les caractéristiques techniques du service de communications électroniques utilisé lors de la communication (1°)

Il s'agit d'une donnée déjà prévue par l'arrêté royal du 19 septembre 2013 pour l'ensemble des services, à l'exception de l'accès à Internet. Cette donnée doit donc désormais être conservée pour tout service de communication électronique offert.

Dans le cadre d'une enquête judiciaire, les caractéristiques du service de communications électroniques utilisé par le sujet de l'enquête permettent de déterminer son profil de communication. Cela pourra permettre de déterminer si celui-ci correspond au profil de l'auteur des faits. Un autre exemple est celui d'un GSM qui n'aurait activé que le service "Voice" et le service "SMS" et quasi pas de "Data". L'utilisateur du GSM sera, grâce à cette information, immédiatement écarté d'une enquête de hacking où l'appareillage utilisé aurait dû activer des volumes importants de data.

Les données d'identification visées à l'article 126, § 1er, 2°, 10° à 14 et 16°, du destinataire de la communication (2°)

De façon parallèle à la conservation des données d'identification de l'utilisateur final d'un service de communication prévue par l'article 126, § 1er, il s'agit ici de conserver les données d'identification similaires concernant le destinataire de la communication, à savoir:

— l'alias éventuel du destinataire (art. 126, § 1er, 2°);

— son adresse de messagerie principale et les adresses de messagerie employées comme alias (art. 126, § 1er, 11°);

— son numéro de téléphone attribué pour les besoins du service (art. 126, § 1er, 10°);

— son IMSI (art. 126, § 1er, 12°);

Paragraaf 2

De tweede paragraaf somt de gegevens op bedoeld in artikel 126/1, § 2, die bewaard moeten worden in uitvoering van artikel 126/1 door de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden alsook de operatoren die elektronische-communicatienetwerken aanbieden die het aanbieden van die diensten mogelijk maken.

De beschrijving en de technische karakteristieken van de elektronische-communicatiedienst aangewend tijdens de communicatie (1°)

Het gaat om een gegeven waarin het koninklijk besluit van 19 september 2013 reeds voor alle diensten voorziet, met uitzondering van de internettoegang. Dat gegeven moet dus voortaan bewaard worden voor elke elektronische-communicatiedienst die aangeboden wordt.

In het kader van een gerechtelijk onderzoek kan aan de hand van de kenmerken van de elektronische-communicatiedienst gebruikt door de persoon die het voorwerp uitmaakt van het onderzoek, diens communicatieprofiel worden bepaald. Dat zal het mogelijk maken om te bepalen of dat laatste overeenstemt met het profiel van de dader van de feiten. Een ander voorbeeld is dat van een gsm waarop enkel de spraakdienst en de sms-dienst zouden geactiveerd zijn en bijna geen data. De gebruiker van de gsm zal dankzij die informatie onmiddellijk kunnen worden uitgesloten in het onderzoek naar hacking waarbij het gebruikte toestel grote volumes data zou moeten geactiveerd hebben.

De identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14° en 16°, van de geadresseerde van de communicatie (2°)

Parallel met de in artikel 126, § 1 bepaalde bewaring van de identificatiegegevens van de eindgebruiker van een communicatiedienst, gaat het hier om het bewaren van de gelijkaardige identificatiegegevens betreffende de geadresseerde van de communicatie, met name:

— de eventuele alias van de geadresseerde (art. 126, § 1, 2°);

— zijn voornaamste e-mailadres en de e-mailadressen die worden gebruikt als alias (art. 126, § 1, 11°);

— zijn telefoonnummer dat toegewezen is ten behoeve van de dienst (art. 126, § 1, 10°);

— zijn IMSI (art. 126, § 1, 12°);

— son SUPI (art. 126, § 1er, 13°);

— son SUCI (art. 126, § 1er, 14°);

— l'identifiant de l'équipement terminal du destinataire, ou lorsque l'opérateur ne le traite pas ou ne le génère pas, l'identifiant de l'équipement qui est le plus proche de cet équipement terminal, à savoir notamment l'IMEI, le PEI ou l'adresse MAC (art. 126, § 1er, 16°).

Les données d'identification du destinataire sont indispensables pour mener une enquête approfondie, que ce soit en cas d'enquête judiciaire ou dans le cadre des missions des services de renseignement. Ces données permettent d'identifier les contacts (ponctuels ou récurrents) de la personne faisant l'objet d'une enquête et de cartographier son réseau de contacts. Étant donné que les auteurs d'infractions tentent en général de brouiller les pistes des autorités en utilisant, par exemple, des numéros de téléphone au nom d'une autre personne, toutes les données d'identification visées à l'article 126, § 1er, 2°, 10° à 14° et 16°, sont nécessaires pour identifier correctement le véritable destinataire des appels. Les exemples et explications fournis à cet égard concernant l'utilisateur qui est à l'origine de l'appel valent également pour ce qui concerne les mêmes données d'identification du destinataire de l'appel.

L'adresse IP du destinataire, l'horodatage et le port attribué en cas d'utilisation partagée (3°)

Cette donnée est conservée pour ce qui concerne les services de communications électroniques autres que les services d'accès à internet. En effet, comme l'a rappelé l'Autorité de protection des données dans son avis n° 108/2021 du 28 juin 2021, 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. Pour ce motif, la conservation de l'adresse IP de destination est exclue pour les services d'accès à internet. Cependant, pour les services de téléphonie en *Voice-over-IP*, la conservation de l'adresse IP utilisée par le destinataire était déjà précédemment prévue par l'article 6, § 2, 2°, b) de l'arrêté royal du 19 septembre 2013. Cette obligation est maintenue.

Néanmoins, il semble utile de clarifier que l'adresse IP de destination ne contient pas de contenu de communication et ne permet pas de déduire l'URL (par exemple *https://fr.airbnb.be/rooms/*) consultée, ou à tout le moins pas de façon aussi précise (au maximum le nom de domaine du site visite, par exemple *fr.airbnb.be*) que pour l'identification de l'appelant

— zijn SUPI (art. 126, § 1, 13°);

— zijn SUCI (art. 126, § 1, 14°);

— de identifier van de eindapparatuur van de geadresseerde, of indien de operator dit niet verwerkt of genereert, de identifier van de apparatuur die zich het dichtst bij die eindapparatuur bevindt, met name de IMEI, de PEI of het MAC-adres (art. 126, § 1, 16°).

De identificatiegegevens van de ontvanger zijn essentieel om een grondig onderzoek uit te voeren, zowel in het kader van een gerechtelijk onderzoek als in het kader van de opdrachten van de inlichtingendiensten. Deze gegevens maken het mogelijk de (punctuele of recurrente) contacten van de persoon tegen wie een onderzoek loopt te identificeren en zijn netwerk van contacten in kaart te brengen. Aangezien de daders van inbreuken doorgaans trachten de autoriteiten in verwarring te brengen door bijvoorbeeld telefoonnummers te gebruiken op naam van een andere persoon, zijn alle in artikel 126, § 1, 2°, 10° tot 14° en 16°, bedoelde identificatiegegevens nodig om de werkelijke ontvanger van de oproepen correct te identificeren. De voorbeelden en toelichtingen over de gebruiker die de oproep heeft gedaan, gelden ook voor dezelfde identificatiegegevens van de ontvanger van de oproep.

Het IP-adres van de geadresseerde, het tijdstempel en de toegewezen poort in geval van het gedeelde gebruik (3°)

Dit gegeven wordt bewaard wat betreft andere elektronische-communicatiediensten dan de internettoegangsdiensten. In haar advies nr. 108/2021 van 28 juni 2021 benadrukt de Gegevensbeschermingsautoriteit immers dat de bewaring van de verkeersgegevens geen specifieke URL van de door de betrokken personen bezochte websites mogen bevatten, of het niet mogelijk mag maken om dergelijke URL's af te leiden. Om die reden, is de bewaring van het IP-adres van bestemming uitgesloten voor de internettoegangsdiensten. Voor de *Voice-over-IP*-telefoniediensten was er echter in de bewaring van het IP-adres dat gebruikt wordt door de geadresseerde reeds voorzien door artikel 6, § 2, 2°, b), van het koninklijk besluit van 19 september 2013. Die verplichting wordt behouden.

Niettemin lijkt het nuttig om duidelijk te maken dat het IP-adres van bestemming geen communicatie-inhoud bevat en het niet mogelijk maakt de geraadpleegde URL (bijvoorbeeld *https://fr.airbnb.be/rooms/*) af te leiden, of op zijn minst niet zo nauwkeurig (hoogstens de domeinnaam van de bezochte site, bijvoorbeeld *fr.airbnb.be*) als voor de identificatie van

et l'appelé dans le cadre d'un appel téléphonique (classique ou *Voice-over-IP*).

En effet, avec une adresse IP (fixe ou dynamique), il est possible d'identifier le détenteur de cette adresse IP au moment de la recherche. Cependant avec une adresse IP dynamique, la même adresse IP conduira au moment X vers le site web et au moment Y vers le site web B. L'historique de l'attribution des adresses IP aux sites web n'est pas conservé par les DNS, de sorte qu'il ne sera pas possible de retrouver à quelle URL était attribuée telle adresse IP dans le passé, sauf à interroger l'ensemble des entités (en règle générale, hébergeurs de contenus) ayant utilisé cette adresse IP pendant la période donnée.

En outre, deuxièmement, une fois que l'hébergeur est identifié (par exemple, Microsoft, Amazon, OVH, …), il faut encore pouvoir identifier l'URL visitée. Or, l'hébergeur ne conserve pas de registre historique de quelle URL s'est vue attribuée quelle adresse IP au moment X. Les hébergeurs donnent accès à une multitudes de sites web divers et variés qui peuvent aussi bien être commerciaux, politiques, religieux ou d'information. En règle générale, toute déduction est donc fort peu certaine.

Par contre en "téléphonie classique", lorsque l'utilisateur A téléphone, par exemple, à l'hôtel B, il peut être déduire que l'utilisateur A à l'intention de séjourner dans l'hôtel B. En matière d'adresses IP de pages web, rien n'est moins vrai: il se peut également que l'ordinateur de l'utilisateur A se connecte automatiquement, à chaque ouverture de session, au serveur de "AirBNB" car son navigateur a enregistré ce site comme page d'accueil, sans que cela ne signifie que l'utilisateur souhaite immédiatement contacter un hôtel.

Et même dans l'hypothèse où un utilisateur visite explicitement le serveur de Airbnb, contrairement à la "téléphonie classique", disposer de l'adresse IP de destination, et pouvoir déterminer qu'il s'agit du serveur de Airbnb, n'offrira jamais la possibilité aux autorités judiciaires de déterminer l'intérêt du suspect pour l'hôtel B.

Pour obtenir cette information, il conviendrait que les autorités judiciaires compétentes transmettent une requête, via le service désigné par le Roi, auprès de Airbnb, ou par commission rogatoire internationale, pour tenter d'obtenir cette information.

C'est donc bien ce très grand nombre d'adresses IP de destination généré par l'utilisation de l'internet, couplé à l'impossibilité d'en déduire une information directement utilisable

de oproeper en de opgebelde persoon in het kader van een telefoongesprek (klassiek of *Voice-over-IP*).

Met een IP-adres (vast of dynamisch) is het immers mogelijk om de houder van dat IP-adres te identificeren op het moment van de opzoeking. Met een dynamisch IP-adres zal hetzelfde IP-adres echter op tijdstip X naar website A leiden en op tijdstip Y naar website B leiden. De geschiedenis van de toewijzing van IP-adressen aan websites wordt niet door de DNS bewaard. Het zal dus niet mogelijk zijn om te achterhalen welke URL in het verleden aan welk IP-adres was toegewezen, tenzij alle entiteiten (gewoonlijk content hosts) die dat IP-adres in de gegeven periode hebben gebruikt, worden opgevraagd.

Ten tweede, zodra de host geïdentificeerd is (b.v. Microsoft, Amazon, OVH, ...), moet men nog de bezochte URL kunnen identificeren. De host houdt echter geen historisch overzicht bij van welke URL op tijdstip X welk IP-adres kreeg toegewezen. Hostingbedrijven bieden toegang tot een veelheid aan diverse en gevarieerde websites die commercieel, politiek, religieus of informatief kunnen zijn. In het algemeen is elke afleiding hoogst onzeker.

In het kader van de "klassieke telefonie" daarentegen, wanneer gebruiker A bijvoorbeeld hotel B telefoneert, kan daaruit worden afgeleid dat gebruiker A van plan is in hotel B te overnachten. In het geval van IP-adressen van webpagina's is niets minder waar: het kan ook zijn dat de computer van gebruiker A zich automatisch aanmeldt bij de "Airbnb"-server telkens wanneer hij inlogt, omdat zijn browser deze site als startpagina heeft geregistreerd, zonder dat dit betekent dat de gebruiker onmiddellijk contact met een hotel wil opnemen.

Zelfs als een gebruiker de Airbnb server expliciet bezoekt, in tegenstelling tot "klassieke telefonie", zal het feit dat men het IP-adres van de bestemming heeft, en kan vaststellen dat het de Airbnb server is, de gerechtelijke autoriteiten nooit de mogelijkheid bieden om de interesse van de verdachte in hotel B vast te stellen.

Om deze informatie te verkrijgen dienen de bevoegde gerechtelijke autoriteiten via de door de Koning aangewezen dienst een verzoek te sturen naar Airbnb, of via een internationale rogatoire commissie, om te proberen deze informatie te verkrijgen.

Daarom maakt dit zeer grote aantal door het gebruik van Internet gegenereerde IP-adressen van bestemmingen, gekoppeld aan de onmogelijkheid om er voor de gerechtelijke

pour les autorités judiciaires, qui rend déraisonnable et non souhaitable leur conservation par les opérateurs.

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 conservation de cette donnée était déjà prévue dans le cadre de la téléphonie classique fixe et mobile, mais peut être étendue à tout service de téléphonie (classique ou en *Voice-over-IP*), dès lors que l'appel multiple, la déviation et le renvoi d'appel sont des possibilités existantes également pour ce type de services.

Dans le cadre d'une enquête judiciaire ou des services de renseignements, l'identification de tous les participants à un appel groupé permet de cartographier le réseau de contacts de la personne ciblée et également de révéler les relations entre les contacts. Le fait que des personnes différentes participent à la même conversation peut indiquer qu'elles se connaissent et ont un point commun.

Si un appel est transféré vers une autre ligne, il est nécessaire de pouvoir identifier toutes les lignes utilisées. Par exemple, une personne ciblée peut utiliser un deuxième numéro de téléphone qui n'est pas enregistré à son nom. Si la personne ciblée par une enquête judiciaire ou de renseignement redirige ses appels entrants vers une deuxième ligne pour laquelle elle est correctement identifiée, il sera possible de l'identifier au moyen de cette deuxième ligne.

La date et l'heure exacte du début et de la fin de la session du service de communication électronique concerné (5°)

La conservation de ces données était déjà prévue pour l'ensemble des services visés par l'arrêté royal du 19 septembre 2013. La terminologie a cependant été adaptée de manière à faire référence uniquement à la notion de "session", étant entendu qu'un appel téléphonique, que ce soit classique ou en *Voice-over-IP*, doit être considéré comme une session.

La conservation des dates et heures de début et fin de session (en ce compris d'un appel) est une donnée essentielle pour encadrer toutes les autres informations. Sans une date ou une heure concrète, il est presque impossible d'interpréter les autres informations, comme par exemple:

autoriteiten rechtstreeks bruikbare informatie uit af te leiden, het voor de operatoren dan ook onredelijk en ongewenst om ze te bewaren.

In geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid (4°)

In de bewaring van dit gegeven was reeds voorzien in het kader van de klassieke vaste en mobiele telefonie, maar die kan worden uitgebreid tot elke telefoniedienst (klassiek of *Voice-over-IP*), aangezien het groepsgesprek, de oproepdoorschakeling of –doorverbinding ook voor dat type van diensten bestaande mogelijkheden zijn.

In het kader van de gerechtelijke onderzoeken of een onderzoek van de inlichtingendiensten maakt de identificatie van alle deelnemers aan een groepsoproep het mogelijk het netwerk van contacten van het doelwit in kaart te brengen. Op deze wijze kunnen de relaties tussen de contacten ook onthuld worden. Het feit dat verschillende mensen aan hetzelfde gesprek deelnemen, kan erop wijzen dat zij elkaar kennen en iets gemeen hebben.

Als een oproep naar een andere lijn wordt doorgeschakeld, is het nodig om alle gebruikte lijnen te kunnen identificeren. Bv. kan een betrokken persoon een tweede telefoonnummer gebruiken dat niet op zijn naam wordt geregistreerd. Als de persoon tegen wie een gerechtelijk of inlichtingenonderzoek loopt oproepen doorschakelt naar een tweede lijn waarvoor hij correct is geïdentificeerd, zal het mogelijk zijn hem via deze tweede lijn te identificeren.

De datum en het juiste tijdstip van aanvang en einde van de sessie van de betrokken elektronische-communicatiedienst (5°)

In de bewaring van die gegevens was reeds voorzien voor alle diensten bedoeld door het koninklijk besluit van 19 september 2013. De terminologie is echter zodanig aangepast om uitsluitend te verwijzen naar het begrip van "sessie", met dien verstande dat een telefonische oproep, of het nu om een klassieke of een *Voice-over-IP*-oproep gaat, moet worden beschouwd als een sessie.

De bewaring van de datum en het juiste tijdstip van aanvang en einde van de sessie (oproep inbegrepen) is essentieel voor de omkadering van alle andere informatie. Zonder een concrete datum of tijdstip is het bijna onmogelijk om andere informatie te interpreteren, zoals:

— détecter une activité accrue d'une personne ciblée juste avant ou après une réunion du groupe extrémiste auquel elle peut appartenir;

— en combinaison avec la localisation, les dates et heures de communications passées permettent de retracer l'itinéraire parcouru sur une carte;
— le début et la fin d'une session indiquent la durée d'une communication. Cela permet notamment d'évaluer l'importance de certains contacts.

L'identification et la localisation des cellules ou autres points de terminaison du réseau utilisés pendant la communication et les dates et heures y afférentes (6°)

Il convient de conserver "les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau, qui ont été utilisé(e)s pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations". La localisation des cellules s'effectue en se référant à leur identifiant cellulaire ("*global cell ID*").

Cette disposition reprend et adapte les données précédemment prévues au paragraphe 2, 6° et 7° de l'article 4 et au paragraphe 2, 3°, 4° et 6° de l'article 5 de l'arrêté royal du 19 septembre 2013.

Elle précise les données de localisation à conserver dans le cadre d'une communication (tout appel ou SMS ou autre type de message entrant ou sortant). Dans le cadre du service d'accès à internet, la communication est toute donnée reçue par l'utilisateur final (ex. toute information reçue dès que la 4G est activée) ou information envoyée (par exemple visite d'un site internet).

Une nouvelle exigence est ajoutée par rapport l'arrêté royal de 2013: les opérateurs doivent désormais conserver la localisation des cellules et autres points de terminaison du réseau tout au long de la communication (par exemple, les mâts intermédiaires, ou les routeurs Wifi dans le cadre de services nomades) et pas uniquement leur localisation au début et à la fin de la communication. Une telle exigence prend tout son sens lorsque l'utilisateur final se déplace. Une telle information est capitale pour les autorités. Les données de localisation que les opérateurs doivent conserver en dehors de toute communication sont prévues au paragraphe 2, 10°.

L'article 5, § 2, 3° de l'AR de 2013 ne mentionnait l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final qu'au début et à la fin d'une

— het opsporen van een verhoogde activiteit van een betrokken persoon net voor of na een ontmoeting met de extremistische groep waartoe hij mogelijk behoort;

— in combinatie met de locatie kan aan de hand van de data en tijdstippen van vroegere communicaties de afgelegde route op een kaart worden weergegeven;
— de aanvang en het einde van een sessie geven de duur van een communicatie aan. Dit maakt het mogelijk het belang van bepaalde contacten te beoordelen.

Het identificeren en het lokaliseren van de cellen of andere netwerkaansluitpunten gebruikt tijdens de communicatie en de data en de tijdstippen die ermee verband houden (6°)

De "gegevens voor het identificeren en het lokaliseren van de cellen of andere netwerkaansluitpunten, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie alsook de exacte data en tijdstippen van deze verschillende locaties" moeten worden bewaard. Het lokaliseren van cellen gebeurt door te refereren aan hun celidentiteit ("*global cell ID*").

Deze bepaling neemt de gegevens over waarin voordien in paragraaf 2, 6° en 7°, van artikel 4, en in paragraaf 2, 3°, 4° en 6°, van artikel 5, van het koninklijk besluit van 19 september 2013 voorzien was en past deze aan.

Ze preciseert de locatiegegevens die moeten worden bewaard in het kader van een communicatie (elke oproep of sms of ander type van binnenkomend of uitgaand bericht). In het kader van de internettoegangsdienst bestaat de communicatie in elk gegeven ontvangen door de eindgebruiker (bijv. alle ontvangen informatie zodra 4G is geactiveerd) of verzonden informatie (bijv. bezoek aan een website).

Een nieuwe vereiste wordt toegevoegd ten opzichte van het koninklijk besluit van 2013: de operatoren moeten voortaan de locatie van de cellen en andere netwerkaansluitpunten bewaren gedurende de communicatie (bijvoorbeeld de tussenliggende masten, of de wifirouters in het kader van nomadische diensten) en niet uitsluitend hun locatie bij aanvang en einde van de communicatie. Het nut van een dergelijke vereiste wordt volledig duidelijk wanneer de eindgebruiker zich verplaatst. Dergelijke informatie is van cruciaal belang voor de autoriteiten. De locatiegegevens die de operatoren moeten bewaren buiten elke communicatie worden bepaald in paragraaf 2, 10°.

Artikel 5, § 2, 3°, van het KB van 2013 vermeldde de identificatie en de lokalisering van het netwerkaansluitpunt gebruikt door de eindgebruiker enkel bij de aanvang en op het einde

connexion. Dans le cadre de la technologie 2G et 3G, ceci permettait effectivement de localiser la communication réalisée au départ de cette technologie.

Ce type d'utilisation est devenu obsolète depuis la généralisation des smartphones avec connexion de données permanente puisqu'avec cette technologie, une session data peut durer de nombreuses heures (parfois supérieure à 12 heures). Cela a pour conséquence qu'un utilisateur pourrait erronément être localisé à un endroit alors qu'il ne s'y trouve plus depuis de nombreuses heures.

Cette localisation erronée risque d'emporter des conséquences, à charge ou à décharge, des citoyens.

Dans le cas d'une connexion de données mobile ou sans fil, il est également important de connaître les points de terminaison du réseau utilisés par l'utilisateur final pendant la communication.

Ces données sont disponibles auprès de l'opérateur étant donné que le réseau de télécommunications a besoin de connaître à tout moment la localisation de l'équipement de l'utilisateur final, et pour cela il s'appuie sur les données fournies par les antennes au moment de la fourniture d'une communication.

Au début d'une connexion à l'antenne A, d'un transfert de la connexion mobile (le "*handover*") à l'antenne B et à la fin de la connexion à l'antenne C, les données de localisation des trois antennes doivent être enregistrées à la suite de cette modification, alors qu'auparavant, seules les positions de l'antenne au début et à la fin étaient enregistrées.

Dans la pratique, cela apporte une valeur ajoutée opérationnelle cruciale. Cette adaptation reflète l'utilisation moderne et continue des télécommunications mobiles.

Dans son avis sur l'amendement, le Conseil d'État indique ce qui suit:

"S'agissant de la donnée reprise à l'article 126/2, § 2, alinéa 1er, 7° en projet, la justification de l'amendement explique ce qui suit:

"Elle précise les données de localisation à conserver dans le cadre d'une communication (tout appel ou SMS ou autre type de message entrant ou sortant). Dans le cadre du service d'accès à internet, la communication est toute donnée reçue par l'utilisateur final (ex. toute information reçue dès que la 4G est activée) ou information envoyée (par exemple visite d'un site internet)".

van de verbinding. In het kader van de 2G- en 3G-technologie maakte dit het inderdaad mogelijk om de met deze technologie uitgevoerde communicatie te lokaliseren.

Dit type van gebruik is voorbijgestreefd sinds het wijdverspreide gebruik van smartphones met permanente dataverbinding, omdat met deze technologie een datasessie vele uren kan duren (soms meer dan 12 uur). Het gevolg daarvan is dat een gebruiker verkeerdelijk gelokaliseerd zou kunnen worden op een plek, terwijl hij zich daar al ettelijke uren niet meer bevindt.

Deze foutieve plaatsbepaling riskeert gevolgen à charge of à décharge voor de burgers met zich te brengen.

In geval van een mobiele of draadloze dataverbinding, is het belangrijk ook de netwerkaansluitpunten die door de eindgebruiker worden gebruikt gedurende de communicatie te kennen.

Deze gegevens zijn beschikbaar bij de operator, want het telecommunicatienetwerk dient te allen tijde de locatie van de eindgebruikersapparatuur te kennen, en hiervoor valt het terug op de gegevens die de antennes aanleveren bij het aanbieden van een communicatie.

Bij de start van een verbinding op antenne A, een overdracht van de mobiele verbinding (de "*handover*") naar antenne B en het afsluiten van de verbinding op antenne C, moeten naar aanleiding van deze wijziging de locatiegegevens van de drie antennes worden bewaard, terwijl voorheen enkel de antenneposities bij aanvang en einde werden bewaard.

In de praktijk biedt dit een cruciale operationele meerwaarde. Deze aanpassing weerspiegelt het moderne en continue gebruik van mobiele telecommunicatiemiddelen.

In het advies betreffende het amendement vermeldt de Raad van State het volgende:

"*S'agissant de la donnée reprise à l'article 126/2, § 2, alinéa 1er, 7° en projet, la justification de l'amendement explique ce qui suit:*

"Elle précise les données de localisation à conserver dans le cadre d'une communication (tout appel ou SMS ou autre type de message entrant" ou sortant). Dans le cadre du service d'accès à internet, la communication est toute donnée reçue par l'utilisateur final (ex. toute information reçue dès que la 4G est activée) ou information envoyée (par exemple visite d'un site internet)".

Cette explication ne permet pas de comprendre quels sont les éléments permettant de s'assurer que la conservation de cette donnée se concilie avec les réserves que l'Autorité de protection des données a émises dans son avis n° 108/2021 selon lesquelles "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".

Le point 6° porte sur la localisation de la personne sur le territoire belge lorsqu'elle fait usage d'un service fourni par le réseau mobile d'un opérateur (appel téléphonique ou surf sur internet). Ce point 6° ne porte donc pas sur les pages internet visitées.

Le volume de données envoyées et téléchargées pendant la durée de la session (7°)

Cette obligation, qui était déjà prévue par l'arrêté royal du 19 septembre 2013 pour les services d'accès à internet (art. 5, § 2, 5°), est maintenue.

Le volume de données permet à une autorité de déterminer entre autres si cela vaut la peine d'adresser une demande vers un opérateur, par exemple s'il n'y a pas de donnée échangée à l'aide du service de communications électroniques souscrit.

De façon similaire à ce qui a été dit précédemment concernant la durée d'un appel, le volume de données utilisé permet d'attribuer une certaine importance à une communication (ex: une communication de moins de X secondes aura, en principe, une importance limitée). De plus, grâce à la corrélation, la nature de la communication peut être estimée en fonction du volume qu'elle engendre (message texte, image, lien vidéo, etc.).

Dates et heures du démarrage et de l'extinction de l'équipement terminal (8°)

Alors que les articles 4, § 2, 6°, et 5, § 2, 3°, de l'arrêté royal de 2013 contenaient une obligation large pour les opérateurs en matière de conservation de données de connexion, le nouveau paragraphe 2, 9°, de l'article 126/2 en projet prévoit la conservation de certaines données de connexion indépendantes d'une communication, à savoir les données de (dé) connexion qui sont générées par l'allumage ou l'extinction du téléphone mobile.

La donnée relative au statut ouvert ou éteint du téléphone est bien entendu utile au niveau tactique pour repérer une personne qui va passer à l'acte. Ainsi, une personne soupçonnée

Cette explication ne permet pas de comprendre quels sont les éléments permettant de s'assurer que la conservation de cette donnée se concilie avec les réserves que l'Autorité de protection des données a émises dans son avis n° 108/2021 selon lesquelles "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".

Punt 6° slaat op de locatie van de persoon op Belgisch grondgebied wanneer die gebruikmaakt van een dienst die aangeboden wordt via het mobiele netwerk van een operator (telefonische oproep of surfen op het internet). Dat punt 6° heeft dus geen betrekking op de bezochte internetpagina's.

Het tijdens de sessie geüploade en gedownloade volume van gegevens (78°)

Deze verplichting, waarin reeds voorzien werd door het koninklijk besluit van 19 september 2013 voor de internettoegangsdiensten (art. 5, § 2, 5°), wordt behouden.

Met het volume van gegevens kan een autoriteit onder meer bepalen of het de moeite loont een operator te vragen bijvoorbeeld of er gegevens worden uitgewisseld via de elektronische-communicatiedienst waarop de betrokkene intekent.

Op gelijkaardige wijze als hierboven over de duur van een oproep maakt het gebruikte volume van gegevens het mogelijk een bepaald belang toe te kennen aan een communicatie (bijvoorbeeld een communicatie van minder dan X seconden zal in beginsel een beperkt belang hebben). Dankzij de correlatie kan de aard van de communicatie ook worden geraamd in functie van het gegenereerde volume (tekstbericht, afbeelding, videoverbinding, enz.).

Data en tijdstippen van de inschakeling en uitschakeling van de eindapparatuur (8°)

Terwijl de artikelen 4, § 2, 6°, en 5, § 2, 3°, van het koninklijk besluit van 2013 een brede verplichting omhelsden voor de operatoren inzake bewaring van verbindingsgegevens, schrijft de nieuwe paragraaf 2, 9°, van het ontworpen artikel 126/2 de bewaring voor van bepaalde verbindingsgegevens los van een communicatie, namelijk de verbindings-/afschakelgegevens die worden gegenereerd bij het aan- of uitzetten van de mobiele telefoon.

Het gegeven in verband met de open of uitgedoofde status van de telefoon is uiteraard nuttig op tactisch niveau om een persoon te vinden die zijn plan tot uitvoering zal brengen. Zo

de vouloir faire un holdup par exemple sur une bijouterie, sachant que la justice peut demander les métadonnées de communication, peut couper son GSM à l'approche de la bijouterie, ce qui donne une indication au juge d'instruction sur l'endroit où il compte mettre son plan à l'exécution.

À l'identique, lorsque l'ensemble des membres d'une organisation criminelle coupe simultanément son GSM, cela donne une indication aux enquêteurs qu'il est possible qu'ils soient ensemble et comptent passer à l'acte. Le moment et le lieu où le GSM est coupé constitue donc une indication précieuse dans le cadre des enquêtes.

Pouvoir déterminer l'heure à laquelle un appareillage s'est connecté pour la première fois sur le réseau suite à l'événement "Le mobile vient d'être allumé" apporte des éléments extrêmement importants dans une enquête criminelle. Cela permet de qualifier toute une série de situations essentielles dans le cadre de l'exécution des missions de police dans les dossiers les plus complexes. Prenons l'exemple du phénomène de l'enlèvement de personnes. Dans ce cas, les services de police remarquent quasi systématiquement que lorsque les auteurs demandent une rançon, ils éteignent leur GSM dès que la négociation avec la famille se termine et ce afin d'éviter d'être localisés. Recevoir de l'opérateur l'information que le GSM se rallume permet aux enquêteurs de prendre une attitude proactive et de gagner du temps. Ceci permettra aux services de police de localiser plus facilement les auteurs et surtout l'endroit où la victime est détenue.

En cas de disparition inquiétante, pouvoir déterminer le moment où la personne qui veut mettre fin à ses jours a éteint son GSM est une information cruciale.

Cette information est également essentielle lors du suivi d'un groupe d'auteurs qui systématiquement avant de passer à l'acte de "*Home-Jacking*" coupent leur GSM.

Cette donnée peut également s'avérer utile pour déterminer la situation d'une personne. Par exemple, un équipement terminal qui se déconnecte du réseau sans raison apparente peut indiquer que cet équipement a été endommagé et qu'une personne portée disparue a peut-être été victime d'un accident. Un autre exemple est celui d'une personne ciblée dont on sait qu'elle s'apprête à prendre un avion. En cas d'extinction de l'équipement terminal, il est permis de penser que l'avion a décollé, et au moment du rallumage du même équipement terminal, que l'avion a atterri.

kan een persoon die ervan verdacht wordt een overval te willen plegen op bijvoorbeeld een juwelierswinkel, wetende dat justitie de communicatiemetagegevens kan vragen, zijn gsm uitschakelen bij het naderen van de juwelierswinkel, hetgeen de onderzoeksrechter een aanwijzing geeft over de plaats waar hij zijn plan tot uitvoering wil brengen.

Op exact dezelfde wijze geeft, wanneer alle leden van een criminele organisatie hun gsm tegelijk uitschakelen, dit een aanwijzing aan de onderzoekers dat zij mogelijk tezamen zijn en hun plan willen uitvoeren. Het ogenblik en de plaats waar de gsm is uitgeschakeld, vormt dus een waardevolle indicatie in het kader van het onderzoek.

Het tijdstip kunnen bepalen waarop een toestel voor de eerste keer de verbinding met het netwerk heeft gemaakt na de gebeurtenis "Het mobiele toestel is zonet ingeschakeld" levert elementen op die uiterst belangrijk zijn bij een crimineel onderzoek. Zo kan een hele reeks van situaties bestempeld worden als essentieel in het kader van de uitvoering van de politionele taken in de meest ingewikkelde dossiers. Nemen we het voorbeeld van het fenomeen ontvoering van personen. In dat geval merken de politiediensten bijna systematisch op dat wanneer de daders losgeld vragen, zij hun gsm uitschakelen zodra de onderhandeling met de familie afgelopen is en dat om te vermijden dat ze gelokaliseerd kunnen worden. Als men van de operator de informatie kan ontvangen dat de gsm opnieuw aangezet wordt, biedt dit de onderzoekers de mogelijkheid om een proactieve houding aan te nemen en tijd te winnen. Daardoor zullen de politiediensten de daders makkelijker kunnen lokaliseren en vooral de plaats vinden waar het slachtoffer wordt vastgehouden.

In geval van een onrustwekkende verdwijning is het kunnen bepalen van het moment waarop de persoon die zijn leven wil beëindigen zijn gsm heeft uitgeschakeld, cruciale informatie.

Deze informatie is ook van essentieel belang bij het volgen van een groep daders die voordat zij tot homejacking over zullen gaan, systematisch hun gsm uitzetten.

Dit gegeven kan ook nuttig zijn om de situatie van een persoon te bepalen. Zo kan een eindapparatuur die zonder duidelijke reden de verbinding met het netwerk verbreekt, erop wijzen dat de apparatuur beschadigd is en dat een vermiste persoon betrokken kan zijn geweest bij een ongeval. Een ander voorbeeld is een persoon van wie men weet dat hij op het punt staat aan boord van een vliegtuig te gaan. Bij het uitschakelen van de eindapparatuur kan worden aangenomen dat het vliegtuig is opgestegen, en bij het inschakelen van dezelfde eindapparatuur dat het vliegtuig is geland.

La durée de conservation de cette donnée est limitée à 6 mois, dès lors que cette durée est suffisante pour les autorités et que les opérateurs ont indiqué que la conservation de cette donnée représente une quantité importante de données à conserver.

Localisation de l'équipement terminal en dehors de toute communication (9°)

De même, le nouveau paragraphe 2, 9° de l'article 126/2 en projet prévoit la conservation de la localisation de l'équipement terminal en dehors de toute communication, dans le cadre des opérations que fait l'opérateur régulièrement pour connaitre la présence des équipements terminaux sur son réseau. Ceci est techniquement nécessaire pour en conserver la performance, pour maintenir un niveau de service élevé, assurer le transit rapide des appels et des communications qu'ils doivent traiter, etc. Pour ce faire, diverses méthodes sont utilisées. Il peut par exemple s'agir de "LBS" ("*Localisation Base Services*") ou de "*paging*". La fréquence et la méthode de ces opérations est variable. Elle dépend des nécessités techniques propres au réseau de l'opérateur, telles que le type de technologie utilisée (2G, 3G, 4G, etc.) ou la densité d'utilisateurs présents sur une partie du réseau.

Savoir où le téléphone d'une personne se trouvait à un moment donné est une donnée capitale dans une enquête. Cela permet d'écarter certaines personnes de l'enquête ou par contre de confirmer les soupçons par rapport à une personne. Cela peut également être utile en cas de disparition d'une personne. Par ailleurs, le fait de pouvoir disposer d'informations de localisation en dehors de toute communication de contenu permet aux autorités de disposer de données de localisation des personnes recherchées même si ces dernières s'abstiennent délibérément de communiquer (par exemple, pendant une réunion visant à organiser des activités illégales).

Chez certains opérateurs, le "*paging*" se fait toutes les 6 heures et pour d'autres tous les 4 heures. La fréquence du paging peut aussi dépendre du nombre de personnes connectées au réseau (si ce nombre est très élevé, un paging plus fréquent peut être nécessaire). Dans ces conditions, si un téléphone mobile est sous mesure d'observation ou si sa position est requise par l'autorité judiciaire compétente, cette autorité obtiendra de l'opérateur une localisation de l'appareillage au minimum de 4 fois sur une journée. L'information reçue ne sera donc pas importante en termes de nombre, ni extrêmement précise (zone couverte par un pylône). Par contre, cette donnée peut se révéler, dans de très nombreuses

De bewaringstermijn van dit gegeven is beperkt tot 6 maanden, omdat die duur voldoende is voor de autoriteiten en omdat de operatoren hebben aangegeven dat de bewaring van dit gegeven een grote hoeveelheid te bewaren gegevens vertegenwoordigt.

Locatie van de eindapparatuur buiten elke communicatie (9°)

Zo bepaalt de nieuwe paragraaf 2, 9°, van het ontworpen artikel 126/2 de bewaring van de locatie van de eindapparatuur buiten elke communicatie, in het kader van de handelingen die de operator regelmatig uitvoert om te weten welke eindapparatuur zich op zijn netwerk bevindt. Dat is technisch noodzakelijk om de goede werking ervan te behouden, om een hoog niveau van dienstverlening te behouden, om de oproepen en communicatie die ze moeten behandelen, snel te verwerken, enz. Daartoe worden verscheidene methodes gebruikt. Het kan bijvoorbeeld gaan om "LBS" ("*Localisation Base Services*") of "*paging*". De frequentie en de methode van deze handelingen verschillen. Ze hangen af van de technische vereisten die inherent zijn aan het netwerk van de operator, zoals het type technologie dat wordt gehanteerd (2G, 3G, 4G, enz.) of de dichtheid van de gebruikers op een deel van het netwerk.

Weten waar de telefoon van een persoon zich op een gegeven ogenblik bevond, is een heel belangrijk gegeven in een onderzoek. Zo kunnen bepaalde personen uitgesloten worden van het onderzoek of integendeel de vermoedens over een persoon bevestigd worden. Dit kan ook nuttig zijn in geval van de verdwijning van een persoon. Bovendien stelt het feit van over locatiegegevens te kunnen beschikken zonder enige inhoudelijke communicatie, de autoriteiten in staat om over locatiegegevens van de gezochte personen te beschikken, ook wanneer die laatsten opzettelijk alle communicatie achterwege laten (bijvoorbeeld tijdens een ontmoeting met het oog op illegale activiteiten).

Bij bepaalde operatoren vindt de *paging* plaats om de 6 uur en bij anderen om de 4 uur. De frequentie van de paging kan ook afhangen van het aantal personen dat op het netwerk is aangesloten (als het aantal zeer hoog is, kan het nodig zijn vaker een paging uit te voeren). Onder deze omstandigheden, als een mobiele telefoon onder observatie staat of als de locatie ervan door de bevoegde rechterlijke autoriteit wordt verzocht, zal deze autoriteit van de operator ten minste viermaal op één dag een locatie van de apparatuur verkrijgen. De ontvangen informatie zal dus niet aanzienlijk zijn in termen van aantallen, noch uiterst nauwkeurig (dekkingszone van een pyloon). Daarentegen kan dit gegeven in het kader

enquêtes, être essentielles pour le travail des autorités: dans quelle région se trouvait un suspect au moment où des crimes ont été perpétrés, quelle est la dernière localisation connue d'une personne connue ou enlevée, etc.

Paragraphe 3

Le troisième paragraphe reprend et adapte l'article 7, § 1er, alinéa 2, de l'arrêté royal du 19 septembre 2013, afin de veiller à ce que les données conservées en exécution de l'article 126 et du présent article puissent être combinées de manière à permettre d'établir la relation entre l'origine de la communication et sa destination.

Enfin, le troisième paragraphe prévoit une délégation au Roi dans le cas où il s'avérerait nécessaire de spécifier les exigences auxquelles ces données doivent répondre.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

van vele onderzoeken essentieel zijn voor het werk van de autoriteiten: waar bevond een verdachte zich op het moment van het gepleegde misdrijf, wat is de laatst bekende locatie van een bekende of ontvoerde persoon, enz.

Paragraaf 3

De derde paragraaf neemt artikel 7, § 1, tweede lid, van het koninklijk besluit van 19 september 2013 over en past deze aan, om ervoor te zorgen dat de bewaarde gegevens in uitvoering van artikel 126 en dit artikel gecombineerd kunnen worden om de relatie te kunnen leggen tussen de bron en de bestemming van de communicatie.

Tot slot voorziet de derde paragraaf in een delegatie aan de Koning voor het geval dat het noodzakelijk zou zijn de vereisten te specifiëren waaraan deze gegevens moeten beantwoorden.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 4 **DU GOUVERNEMENT**

Art. 14

Dans le 1°, dans le paragraphe 1er proposé, remplacer les mots "126, 126/1"**," par les mots** *"126 à 126/2"***.**

JUSTIFICATION

Vu qu'un nouvel article 126/2 est inséré dans la loi télécom par l'amendement n° 3, il est nécessaire d'adapter l'article 145 de cette même loi, de sorte que le non-respect de l'arrêté royal d'exécution de l'article 126/2 soit puni par l'amende pénale prévue à l'article 145.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Nr. 4 **VAN DE REGERING**

Art. 14

In de bepaling onder 1°, in de voorgestelde paragraaf 1, de woorden "126, 126/1" **vervangen door de woorden** *"126 tot 126/2"***.**

VERANTWOORDING

Aangezien door amendement nr. 3 een nieuw artikel 126/2 wordt ingevoegd in de telecomwet, is het noodzakelijk om artikel 145 van dezelfde wet aan te passen, zodat de niet-naleving van het koninklijk besluit ter uitvoering van artikel 126/2 bestraft wordt met de geldboete waarin artikel 145 voorziet.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 5 **DU GOUVERNEMENT**

Art. 39 *(nouveau)*

Insérer un article 39, rédigé comme suit:

"Art. 39. Les opérateurs conservent les données suivantes au plus tard le premier jour qui suit l'expiration d'un délai de deux ans prenant cours le jour de la publication de la présente loi au Moniteur belge:

1° l'adresse MAC (Media Access Control), visée aux articles 126 et 126/2 de la loi du 13 juin 2005 relative aux communications électroniques;

2° les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile, qui ont été utilisé(e)s au cours de la communication, visées à l'article 126/2, § 2, 6°, de la loi du 13 juin 2005 relative aux communications électroniques;

3° les données visées à l'article 126/2, § 2, 8° et 9°, de la loi du 13 juin 2005 relative aux communications électroniques."

JUSTIFICATION

Les opérateurs disposent d'une période de transition de deux ans pour mettre en œuvre la conservation des nouvelles données, à savoir des données visées dans les articles 126 et 126/2 de la loi télécom et qui ne sont pas prévues 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.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Nr. 5 **VAN DE REGERING**

Art. 39 *(nieuw)*

Een artikel 39 invoegen, luidende:

"Art. 39. Uiterlijk op de eerste dag die volgt op de afloop van een termijn van twee jaar die ingaat op de dag waarop deze wet wordt bekendgemaakt in het Belgisch Staatsblad, bewaren de operatoren de volgende gegevens:

1° het MAC-adres (Media Access Control), bedoeld in de artikelen 126 en 126/2 van de wet van 13 juni 2005 betreffende de elektronische communicatie;

2° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt tijdens de communicatie, waarvan sprake in artikel 126/2, § 2, 6°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

3° de gegevens bedoeld in artikel 126/2, § 2, 8° en 9°, van de wet van 13 juni 2005 betreffende de elektronische communicatie."

VERANTWOORDING

De operatoren beschikken over een overgangsperiode van twee jaar om de bewaring van de nieuwe gegevens aan te wenden, namelijk gegevens bedoeld in de artikelen 126 en 126/2 van de telecomwet en waarin het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie niet voorziet.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 6 **DU GOUVERNEMENT**

Art. 10

Remplacer cet article par ce qui suit:

"Art. 10. L'article 127 de la même loi est remplacé par ce qui suit:

"Art. 127. § 1er. Le présent article s'applique aux opérateurs qui fournissent en Belgique, aux utilisateurs finaux, un service de communications électroniques.

Il est interdit de distribuer en Belgique, en ce compris par internet, aux utilisateurs finaux, sans l'accord de l'entreprise étrangère qui fournit le service de communications électroniques accessible au public:

— des cartes prépayées ou des abonnements de cette entreprise qui leur permettent d'y utiliser un service de communications électroniques;

— des objets connectés dans lesquels un produit de cette entreprise est intégré et qui leur permettent d'y utiliser un service d'accès à internet ou un service de communication interpersonnelle d'un opérateur.

La personne qui distribue en Belgique ces cartes prépayées, ces abonnements ou ces objets connectés fournit aux officiers de police judiciaire de l'Institut, à leur demande, la preuve de cet accord.

En cas d'accord de l'entreprise, cette dernière est opérateur et se conforme à l'article 9, § 1er.

§ 2. Pour l'application du présent article, il faut entendre par:

1° service de communications électroniques payant: le service de communications électroniques pour lequel un paiement de l'abonné à l'opérateur est nécessaire pour utiliser le service ou continuer à l'utiliser, ainsi que tout service de communications électroniques offert

Nr. 6 **VAN DE REGERING**

Art. 10

Dit artikel vervangen als volgt:

"Art. 10. Artikel 127 van dezelfde wet wordt vervangen als volgt:

"Art. 127. § 1. Dit artikel is van toepassing op de operatoren die in België een elektronische-communicatiedienst aanbieden aan eindgebruikers.

Het is verboden om in België, inclusief via het internet, zonder het akkoord van de buitenlandse onderneming die de voor het publiek beschikbare elektronische-communicatiedienst verstrekt, het volgende aan te bieden aan de eindgebruikers:

— voorafbetaalde kaarten of abonnementen van die onderneming die hen in staat stellen om er een elektronische-communicatiedienst te gebruiken;

— geconnecteerde voorwerpen waarin een product van die onderneming is geïntegreerd en die hen in staat stellen om er een internettoegangsdienst of een interpersoonlijke communicatiedienst van een operator te gebruiken.

De persoon die deze voorafbetaalde kaarten, deze abonnementen of deze geconnecteerde voorwerpen aanbiedt in België, verstrekt aan de officieren van gerechtelijke politie van het Instituut, wanneer zij daarom verzoeken, het bewijs van dat akkoord.

Indien de onderneming akkoord gaat, is zij de operator en schikt zij zich naar artikel 9, § 1.

§ 2. Voor de toepassing van dit artikel wordt verstaan onder:

1° elektronische-communicatiebetaaldienst: een elektronische-communicatiedienst waarbij de abonnee moet betalen aan de operator om de dienst te gebruiken of te blijven gebruiken, evenals elke elektronische-communicatiedienst die samen met deze dienst zonder

sans surcoût par l'opérateur à l'abonné conjointement à ce service;

2° service de communications électroniques gratuit: le service de communications électroniques offert par l'opérateur à l'abonné autre que le service de communications électroniques payant;

3° méthode d'identification directe: méthode par laquelle l'opérateur collecte et conserve pour les besoins des autorités visées à l'article 127/1, § 3, alinéa 1er:

— des données fiables relatives à l'identité civile d'une personne physique, qui est son abonné ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir l'obligation d'identification de la personne morale et, le cas échéant;

— une copie du document d'identification de cette personne physique;

4° méthode d'identification indirecte: méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés.

5° point de vente: point de vente physique de cartes prépayées ou d'abonnements d'un opérateur.

L'opérateur qui fournit un service de communications électroniques payant identifie ses abonnés au moyen d'une méthode d'identification directe ou indirecte, à l'exception des méthodes d'identification indirecte visées au paragraphe 9, alinéa 1er, 1° et 2°.

Par dérogation à l'alinéa 2, l'opérateur visé à cet alinéa peut également identifier l'abonné au moyen de la méthode d'identification indirecte visée au paragraphe 9, alinéa 1er, 2°, lorsqu'il offre un service de communications électroniques pour lequel les méthodes d'identification directe et indirecte autorisées par l'alinéa 2 impliquent des contraintes importantes pour les abonnés et l'opérateur, à savoir:

meerkosten door de operator wordt aangeboden aan de abonnee;

2° gratis elektronische-communicatiedienst: de elektronische-communicatiedienst aangeboden door de operator aan de abonnee die geen elektronische-communicatiebetaaldienst is;

3° directe identificatiemethode: methode waarbij de operator voor de behoeften van de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid:

— betrouwbare gegevens verzamelt en bewaart met betrekking tot de burgerlijke identiteit van een natuurlijke persoon, die zijn abonnee is of die optreedt voor rekening van een rechtspersoon die abonnee is van de operator om de verplichtingen inzake identificatie van de rechtspersoon te vervullen en, in voorkomend geval;

— een kopie van het identificatiedocument van deze natuurlijke persoon verzamelt en bewaart;

4° indirecte identificatiemethode: methode waarbij de operator gegevens verzamelt en bewaart aan de hand waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen.

5° verkooppunt: fysiek verkooppunt van voorafbetaalde kaarten of abonnementen van een operator.

De operator die een elektronische-communicatiebetaaldienst verstrekt, identificeert zijn abonnees door middel van een directe of indirecte identificatiemethode, met uitzondering van de indirecte identificatiemethodes bedoeld in paragraaf 9, eerste lid, 1° en 2°.

In afwijking van het tweede lid mag de in dat lid bedoelde operator de abonnee ook identificeren aan de hand van de indirecte identificatiemethode bedoeld in paragraaf 9, eerste lid, 2°, wanneer hij elektronische-communicatiediensten aanbiedt waarvoor de directe en indirecte identificatiemethodes bedoeld in het tweede lid belangrijke lasten met zich meebrengen voor de abonnees en de operatoren, namelijk:

— les services fixes d'accès à internet utilisés par des personnes physiques en dehors de leur lieu de résidence et du lieu où elles exercent une activité professionnelle, tels que les services de communications électroniques offerts à l'aide de bornes WiFi des opérateurs;

— les autres services déterminés par le Roi.

L"opérateur qui fournit un service de communications électroniques gratuit identifie ses abonnés au moyen d"une méthode d'identification indirecte visée au paragraphe 9.

§ 3. Il est interdit aux points de vente de conserver des données d'identification ou des copies de documents d'identification ou d'en faire un usage quelconque autre que l'identification de l'abonné.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées pour la mise en œuvre de l'interdiction visée à l'alinéa 1er, en ce compris en permettant aux points de vente d'introduire directement les données d'identification et les copies de documents d'identification dans leurs systèmes informatiques.

Si une introduction directe dans les systèmes informatiques de l'opérateur n'est temporairement plus possible en raison d'une défaillance de ces systèmes, les données d'identification et les copies de documents d'identification gardées par le point de vente lors de cette défaillance sont détruites au plus tard après l'activation du service de communications électroniques.

Sauf disposition légale contraire, les données d'identification et les copies de document d'identification collectées en vertu du présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la fin du service de communications électroniques.

§ 4. L'opérateur met tout en œuvre pour assurer la fiabilité de l'identification de l'abonné qui est une personne physique.

— de vaste internettoegangsdiensten die worden gebruikt door natuurlijke personen buiten hun verblijfplaats en de plaats waar ze een beroepsactiviteit uitoefenen, zoals de elektronische-communicatiediensten die worden verstrekt door middel van WiFi hotspots van de operatoren;

— de andere diensten bepaald door de Koning.

Een operator die een gratis elektronische-communicatiedienst verstrekt, identificeert zijn abonnees aan de hand van een indirecte identificatiemethode zoals bedoeld in paragraaf 9.

§ 3. Het is verboden voor de verkooppunten om identificatiegegevens of kopieën van identiteitsdocumenten te bewaren, of deze voor enig ander doeleinde te gebruiken dan de identificatie van de abonnee.

De operatoren nemen de gepaste en evenredige technische en organisatorische maatregelen voor de tenuitvoerlegging van het in het eerste lid bedoelde verbod, door onder andere de verkooppunten toe te staan om de identificatiegegevens en de kopieën van identificatiedocumenten rechtstreeks in te voeren in hun computersystemen.

Indien een rechtstreekse invoer in de computersystemen van de operator tijdelijk niet mogelijk is door een storing in deze systemen, worden de identificatiegegevens en de kopieën van identificatiedocumenten die het verkooppunt op het moment van de storing heeft bewaard, vernietigd, uiterlijk na de activering van de elektronische-communicatiedienst.

Behoudens andersluidende wettelijke bepaling, worden de identificatiegegevens en de kopieën van identificatiedocumenten vergaard krachtens dit artikel bewaard vanaf de datum van activering van de dienst tot twaalf maanden na de stopzetting van de elektronische-communicatiedienst.

§ 4. De operator stelt alles in het werk om de betrouwbaarheid van de identificatie van de abonnee die een natuurlijke persoon is te garanderen.

Lorsque l'opérateur identifie l'abonné à l'aide d'un document d'identification, il s'assure:

— que les données d'identification collectées correspondent aux données sur ce document;

— que la date de validité de ce document n'est pas dépassée au moment de l'identification de l'abonné.

Lorsque l'opérateur identifie l'abonné à l'aide d'un document d'identification, il met tout en œuvre pour vérifier:

— que ce document est l'original, lisible et apparence d'authenticité;

— que ce document est relatif à la personne identifiée.

Afin d'assurer la fiabilité visée à l'alinéa 1er et d'éviter les fraudes à l'identité, l'opérateur ou le point de vente peut réaliser de manière automatique une comparaison entre les paramètres biométriques sur la photo du document d'identification de l'abonné et ceux de son visage, aux conditions suivantes:

1° l'outil de comparaison a été autorisé par le ministre et le ministre de la Justice, après vérification que cet outil assure la fiabilité de l'identification de l'abonné pour les besoins des autorités, en tenant compte en particulier du risque de fraude à l'identité de la part de la personne qui s'identifie;

2° l'opérateur offre à l'abonné au moins une manière alternative de s'identifier;

3° l'abonné a donné son consentement explicite au sens de l'article 4 du RGPD, ce qui implique notamment que l'abonné soit informé des finalités pour lesquelles ces données seront récoltées, à savoir la mise en œuvre de l'obligation légale d'identification de l'abonné de manière fiable et la lutte contre la fraude à l'identité;

Wanneer de operator de abonnee identificeert aan de hand van een identificatiedocument, vergewist hij zich ervan:

— dat de vergaarde identificatiegegevens overeenstemmen met de gegevens op het document;

— dat de geldigheidsdatum van dat document niet overschreden is op het ogenblik van de identificatie van de abonnee.

Wanneer de operator de abonnee identificeert aan de hand van een identificatiedocument, stelt hij alles in het werk om te controleren:

— of het document het origineel is, leesbaar is en de indruk geeft van authenticiteit;

— dat dit document betrekking heeft op de geïdentificeerde persoon.

Teneinde de betrouwbaarheid bedoeld in het eerste lid te garanderen en identiteitsfraudes te vermijden, kan de operator of het verkooppunt automatisch een vergelijking uitvoeren tussen de biometrische gegevens op de foto van het identificatiedocument van de abonnee en deze van zijn gezicht, volgens deze voorwaarden:

1° de vergelijkingstool werd toegestaan door de minister en de minister van Justitie, na verificatie dat deze tool de betrouwbaarheid van de identificatie van de abonnee voor de behoeften van de autoriteiten garandeert, in het bijzonder rekening houdende met het risico van identiteitsfraude vanwege de persoon die zich identificeert;

2° de operator biedt de abonnee minstens een alternatieve manier aan om zich te identificeren;

3° de abonnee heeft zijn uitdrukkelijke instemming gegeven in de zin van artikel 4 van de AVG, wat met name inhoudt dat de abonnee op de hoogte is van de doeleinden waarvoor deze gegevens zullen worden verzameld, met name de tenuitvoerbrenging van de wettelijke verplichting tot identificatie van de abonnee op betrouwbare wijze en de strijd tegen identiteitsfraude;

4° l'opérateur et le point de vente ne peuvent communiquer ces données biométriques à un tiers au sens de l'article 4, 10), du RGPD et ne peuvent les traiter que dans les limites nécessaires en vue d'accomplir les finalités de comparaison faciale visée à l'alinéa 4;

5° il est interdit de conserver ces données biométriques au-delà de cette comparaison.

Lorsque l'abonné s'identifie à l'aide d'une carte d'identité électronique belge et que l'opérateur n'a pas mis en œuvre la méthode de comparaison faciale visée à l'alinéa 4, l'opérateur peut demander à l'abonné l'introduction du code PIN.

§ 5. Les documents d'identification qui sont admis pour identifier l'abonné qui est une personne physique sont les suivants:

1° la carte d'identité électronique belge;

2° le passeport belge;

3° le certificat d'inscription au registre des étrangers – séjour temporaire, délivré avant le 11 octobre 2021, en cours de validité (carte A);

4° le titre de séjour limité (carte A);

5° le certificat d'inscription au registre des étrangers, délivré avant le 11 octobre 2021, en cours de validité (carte B);

6° le titre de séjour illimité (carte B);

7° la carte d'identité d'étranger, délivrée avant le 11 octobre 2021, en cours de validité (carte C);

8° le titre d'établissement (carte K);

9° le titre de séjour de résident de longue durée – UE, délivré avant le 11 octobre 2021, en cours de validité (carte D);

4° de operator en het verkooppunt mogen deze biometrische gegevens niet meedelen aan een derde als bedoeld in artikel 4, 10), van de AVG en zij mogen deze maar verwerken binnen de limieten die nodig zijn om het in het vierde lid beoogde doelen van gezichtsvergelijking te verwezenlijken;

5° het is verboden om deze biometrische gegevens te bewaren na die vergelijking.

Wanneer de abonnee zich aan de hand van een Belgische elektronische identiteitskaart identificeert en de operator de in het vierde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast, kan de operator aan de abonnee vragen om de pincode in te tikken.

§ 5. De toegestane identificatiedocumenten ter identificatie van de abonnee die een natuurlijke persoon is, zijn de volgende:

1° de Belgische elektronische identiteitskaart;

2° het Belgisch paspoort;

3° het bewijs van inschrijving in het vreemdelingenregister – tijdelijk verblijf, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (A-kaart);

4° de beperkte verblijfstitel (A-kaart);

5° het bewijs van inschrijving in het vreemdelingenregister, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (B-kaart);

6° de onbeperkte verblijfstitel (B-kaart);

7° de identiteitskaart voor vreemdelingen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (C-kaart);

8° de vestigingsvergunning (K-kaart);

9° de EU-verblijfstitel voor langdurig ingezetenen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (D-kaart);

10° le titre de séjour de résident de longue durée – UE (carte L);

11° l'attestation d'enregistrement, délivrée avant le 10 mai 2021, en cours de validité (carte E);

12° le document d'enregistrement "Art 8 DIR 2004/38/CE" E (carte EU);

13° le document attestant de la permanence de séjour, délivré avant le 10 mai 2021, en cours de validité (carte E+);

14° le document de séjour permanent "Art 19 DIR 2004/38/CE" (carte EU+);

15° la carte de séjour de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F);

16° la carte de séjour de membre de la famille d'un citoyen de l'Union "membre famille UE – Art 10 DIR 2004/38/CE" (carte F);

17° la carte de séjour permanent de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F+);

18° la carte de séjour la carte de séjour permanent de membre de la famille d'un citoyen de l'Union "membre famille UE – Art 20 DIR 2004/38/CE" (carte F+);

19° la carte bleue européenne (carte H);

20° le permis pour personne faisant l'objet d'un transfert temporaire intragroupe "ICT" (carte I);

21° le permis pour mobilité de longue durée "mobile ICT"I (carte J);

22° la carte de séjour pour bénéficiaires de l'accord de retrait "Art. 50 TUE" (carte M);

10° de EU-verblijfstitel voor langdurig ingezetenen (L-kaart);

11° de verklaring van inschrijving, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E-kaart);

12° het document van inschrijving "Art 8 RL 2004/38/EG" E (EU-kaart);

13° het document ter staving van duurzaam verblijf, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E+-kaart);

14° het document van duurzaam verblijf "Art 19 RL 2004/38/EG" (EU+-kaart);

15° de verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F-kaart);

16° de verblijfskaart van een familielid van een burger van de Unie "familielid EU – Art 10 RL 2004/38/EG"(F-kaart);

17° de duurzame verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F-+ kaart);

18° de duurzame verblijfskaart van een familielid van een burger van de Unie "Familielid EU – Art 20 RL 2004/38/EG" (F+-kaart);

19° de Europese blauwe kaart (H-kaart);

20° de vergunning voor een binnen een onderneming overgeplaatste persoon "ICT" (I-kaart);

21° de vergunning voor lange-termijnmobiliteit "mobiele ICT" (J-kaart);

22° de verblijfskaart voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU" (M-kaart);

23° la carte de séjour permanent pour bénéficiaires de l'accord de retrait "Art. 50 TUE" (carte M);

24° la carte pour petit trafic frontalier pour bénéficiaires de l'accord de retrait "Art. 50 TUE – Travailleur frontalier" (carte N);

25° l'acte de notoriété;

26° l'annexe 12 délivrée en application de l'article 6 de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité ou en application de l'article 36bis de l'arrêté royal du 8 octobre 1981 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers;

27° l'attestation d'immatriculation (carte orange);

28° la carte d'identité étrangère, lorsqu'un passeport international n'est pas nécessaire pour séjourner en Belgique;

29° les cartes d'identité spéciales délivrées aux catégories de personnel actives dans les missions diplomatiques et consulaires et aux membres de leur famille, en vertu des Conventions de Vienne de 1961 et 1963 et de l'arrêté royal du 30 octobre 1991 relatif aux documents de séjour en Belgique de certains étrangers;

30° la carte d'identité délivrée conformément aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux;

31° le passeport étranger;

32° tout autre document déterminé par le Roi, pour autant que l'arrêté royal soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Les opérateurs qui disposent de points de vente permettent à leurs abonnés de s'identifier à l'aide de

23° de duurzame verblijfskaart voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU" (M-kaart);

24° de kaart voor klein grensverkeer voor begunstigden van het terugtrekkingsakkoord "Artikel 50 VEU – grensarbeider" (N-kaart);

25° de akte van bekendheid;

26° bijlage 12 verstrekt krachtens artikel 6 van het koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten of krachtens artikel 36bis van het koninklijk besluit van 8 oktober 1981 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

27° het attest van immatriculatie (oranje kaart);

28° de buitenlandse identiteitskaart, wanneer een internationaal paspoort niet nodig is om in België te verblijven;

29° de bijzondere identiteitskaarten verstrekt aan de categorieën van personeel dat actief is in diplomatieke en consulaire zendingen en aan hun familieleden, krachtens de Verdragen van Wenen van 1961 en 1963 en het koninklijk besluit van 30 oktober 1991 betreffende de documenten voor het verblijf in België van bepaalde vreemdelingen;

30° de identiteitskaart verstrekt conform de Conventies van Genève van 12 augustus 1949 inzake de bescherming van de slachtoffers van internationale gewapende conflicten;

31° het buitenlands paspoort;

32° elk ander document bepaald door de Koning, op voorwaarde dat het koninklijk besluit door de wet wordt bekrachtigd binnen twaalf maanden na de bekendmaking van dit besluit.

De operatoren die over fysieke verkooppunten beschikken, maken het voor hun abonnees mogelijk om

n'importe lequel des documents d'identification visés à l'alinéa 1er, dans le cadre d'au moins une méthode d'identification de leur choix.

Par dérogation à l'alinéa 2, un opérateur peut refuser d'identifier un abonné sur base d'un document d'identification visé à l'alinéa 1er autre que la carte d'identité électronique belge s'il lui offre la possibilité de s'identifier selon une des manières alternatives visées à l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée et pour autant que l'abonné soit en mesure de mettre en œuvre cette alternative.

Lorsqu'un opérateur identifie l'abonné à partir d'un document d'identification, il conserve une copie de ce document, sauf lorsqu'il s'agit de la carte d'identité électronique belge.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées pour empêcher que les points de vente ou des tiers ne prennent une copie de la carte d'identité électronique belge, sans préjudice du paragraphe 3, alinéa 3.

§ 6. Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné qui est une personne physique à partir de sa carte d'identité électronique belge, il conserve son numéro de registre national, son nom et son prénom.

Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné à partir d'un autre document que la carte d'identité électronique belge ou au moyen d'une autre méthode d'identification directe que la présentation d'un document d'identification, il conserve parmi les données suivantes celles qui se trouvent sur le document d'identification présenté ou qui sont traitées lors de la mise en œuvre de la méthode d'identification directe:

zich te identificeren aan de hand van om het even welke van de in het eerste lid bedoelde identificatiedocumenten, in het kader van minstens één identificatiemethode van hun keuze.

In afwijking van het tweede lid kan een operator weigeren om een abonnee te identificeren op basis van een ander identificatiedocument dat is vermeld in het eerste lid dan de Belgische elektronische identiteitskaart indien hij hem de mogelijkheid biedt zich te identificeren op een van de alternatieve wijzen vermeld in het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart en voor zover de abonnee in staat is die alternatieve wijze te gebruiken.

Wanneer de operator een abonnee identificeert uitgaande van een identificatiedocument, bewaart hij een kopie van dat document, behalve als het gaat om de Belgische elektronische identiteitskaart.

De operatoren nemen de passende en evenredige maatregelen van technische en organisatorische aard teneinde te verhinderen dat de verkooppunten of derden een kopie nemen van de Belgische elektronische identiteitskaart, zulks onverminderd paragraaf 3, derde lid.

§ 6. Onverminderd artikel 126, bewaart de operator het rijksregisternummer, de naam en voornaam van zijn abonnee die een natuurlijke persoon is, wanneer hij die abonnee identificeert aan de hand van zijn Belgische elektronische identiteitskaart.

Onverminderd artikel 126 bewaart de operator, bij het identificeren van de abonnee via een ander document dan de Belgische elektronische identiteitskaart of aan de hand van een andere directe identificatiemethode dan de overlegging van een identificatiedocument, tussen de volgende gegevens diegene die op het voorgelegde identificatiedocument staan of diegene die worden verwerkt tijdens de toepassing van de directe identificatiemethode:

1° le nom et le prénom;

2° la nationalité;

3° la date de naissance;

4° l'adresse du domicile, l'adresse e-mail et le numéro de téléphone;

5° le numéro du document d'identification et le pays d'émission du document lorsqu'il s'agit d'un document étranger;

6° le lien entre le nouveau service de communications électroniques auquel l'abonné souscrit et le service pour lequel il a déjà été identifié.

§ 7. Lorsqu'un opérateur fournit à un abonné qui est une personne morale un service de communications électroniques mobile sur la base d'une carte prépayée et qu'il l'identifie par le biais d'une méthode d'identification directe, il collecte et conserve, en respectant les exigences prévues aux paragraphes 3 à 6, l'identité civile d'une personne physique qui agit pour le compte de la personne morale.

§ 8. Pour ce qui concerne les méthodes d'identification directe, le Roi peut:

1° déterminer les seules méthodes que les opérateurs peuvent utiliser;

2° prévoir, par méthode, les conditions à respecter, en ce compris soumettre une méthode d'identification proposée par une entreprise à une autorisation préalable du ministre et du ministre de la Justice;

3° imposer des obligations aux opérateurs, aux points de vente, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 9. L'opérateur permet aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'identifier ses

1° de naam en voornaam;

2° de nationaliteit;

3° de geboortedatum;

4° het adres van de woonplaats, het e-mailadres en het telefoonnummer;

5° het nummer van het identificatiedocument en het land van uitgifte van het document wanneer het een buitenlands document betreft;

6° het verband tussen de nieuwe elektronische-communicatiedienst waarop de abonnee intekent en de dienst waarvoor hij reeds werd geïdentificeerd.

§ 7. Wanneer een operator op basis van een voorafbetaalde kaart een mobiele elektronische-communicatiedienst aanbiedt aan een abonnee die een rechtspersoon is en die hij identificeert aan de hand van een directe identificatiemethode, vergaart en bewaart hij de burgerlijke identiteit van een natuurlijke persoon die handelt voor rekening van de rechtspersoon, conform de vereisten vastgelegd in de paragrafen 3 tot 6.

§ 8. Wat de directe identificatiemethodes betreft, kan de Koning:

1° de enige methodes vastleggen die de operatoren mogen gebruiken;

2° per methode te bepalen aan welke voorwaarden moet worden voldaan, onder meer door een door een onderneming voorgestelde identificatiemethode te onderwerpen aan een voorafgaande machtiging van de minister en van de minister van Justitie;

3° verplichtingen opleggen aan de operatoren, aan de verkooppunten, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 9. De operator maakt het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, mogelijk

abonnés par le biais d'une méthode d'identification indirecte:

1° en conservant, en exécution de l'article 126 et pendant les délais prévus par cet article, l'adresse IP ayant servi à la souscription au service de communications électroniques ou à son activation, l'adresse IP à la source de la connexion et les données qui doivent être conservées avec ces adresses, ou;

2° en collectant et conservant le numéro de téléphone de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné conformément au présent article, ou;

3° en cas de paiement en ligne spécifique à la souscription d'un service de communications électroniques, en collectant et conservant:

— la référence de l'opération de paiement, et;

— le nom, le prénom, l'adresse du domicile et la date de naissance déclarés par la personne physique qui est l'abonné de l'opérateur ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir son obligation en matière d'identification, ou;

4° en cas de carte SIM ("subscriber identity/identification module") ou toute autre carte équivalente intégrée dans un véhicule, en collectant et conservant le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte;

5° en cas de souscription d'un abonné qui réside dans un centre fermé ou un lieu d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers à un service de communications électroniques mobile fourni au moyen d'une carte prépayée, en collectant et conservant le nom et le prénom de l'abonné, son numéro de sécurité publique, à savoir le numéro de dossier attribué par l'Office des

om zijn abonnees te identificeren via een indirecte identificatiemethode:

1° door de bewaring, overeenkomstig artikel 126 en gedurende de in dat artikel bepaalde termijnen, van het IP-adres dat werd gebruikt om zich op de elektronische- communicatiedienst in te tekenen of om deze dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij bewaard moeten worden, of;

2° door de vergaring en bewaring van het telefoonnummer van de abonnee dat werd toegewezen in het kader van een elektronische-communicatiebetaaldienst waarvoor een operator de abonnee moet identificeren krachtens onderhavig artikel, of;

3° in geval van een onlinebetaling specifiek voor de intekening op een elektronische-communicatiedienst, door de vergaring en bewaring van:

— het kenmerk van de betalingsverrichting, en;

— de naam, de voornaam, het verblijfadres en de geboortedatum opgegeven door de natuurlijke persoon die de abonnee van de operator is of die handelt voor rekening van een rechtspersoon die de abonnee van de operator is, teneinde zijn verplichtingen inzake identificatie te vervullen, of;

4° in geval van een simkaart ("subscriber identity/identification module") of andere gelijkwaardige kaart die in een voertuig wordt ingebouwd, door de vergaring en bewaring van het chassisnummer van het voertuig en van de link tussen het chassisnummer en het nummer van de kaart;

5° in geval van een intekening van een abonnee die in een gesloten centrum of woonunit verblijft in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op een mobiele elektronische-communicatiedienst verstrekt door middel van een voorafbetaalde kaart, door de vergaring en bewaring van de naam en de voornaam van de

Étrangers et les coordonnées du centre ou du lieu d'hébergement où la souscription a eu lieu, ou;

6° en cas de souscription à un service de communications électroniques par une personne morale au nom et pour le compte d'une personne physique qui rencontre des difficultés à effectuer cette souscription, en collectant et conservant la dénomination précise de cette personne morale et, pour ce qui concerne cette personne physique, au minimum son nom, son prénom, son adresse de résidence, lorsqu'elle en dispose, sa date de naissance et le numéro par lequel elle est identifiée, tel un numéro de registre national, ces informations lui étant transmises par cette personne morale.

Pour l'application de l'alinéa 1er, 6°, la personne morale:

1° doit, avant de pouvoir souscrire à un service de communications électroniques pour la personne physique, obtenir un agrément, délivré par le ministre et le ministre de la Justice, et ayant pour objet de vérifier qu'elle respecte les valeurs démocratiques inscrites dans la Constitution ainsi que le présent article;

2° s'identifie auprès de l'opérateur conformément au présent article;

3° identifie les abonnés à l'aide d'un des documents d'identification visés au paragraphe 5, conformément aux exigences de fiabilité visées au paragraphe 4, ou à l'aide d'une autre méthode autorisée dans l'agrément visé au 1°;

4° conserve une copie du document d'identification des abonnés autre que la carte d'identité électronique belge, sauf dérogation accordée dans l'agrément visé au 1°;

5° conserve une liste actualisée permettant de faire le lien entre le service de communications électroniques et les abonnés, comprenant au minimum le nom, le

abonnee, zijn openbaar veiligheidsnummer, zijnde het door Vreemdelingenzaken toegekende dossiernummer, en de contactgegevens van het centrum of de woonunit waar de intekening heeft plaatsgevonden, of:

6° in geval van intekening op een elektronische-communicatiedienst door een rechtspersoon namens en voor rekening van een natuurlijke persoon die moeilijkheden heeft om die intekening te verrichten, door de vergaring en bewaring van de precieze benaming van de rechtspersoon en, wat de natuurlijke persoon in kwestie betreft, minimaal zijn naam, zijn voornaam, zijn verblijfadres als hij dat heeft, zijn geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals een rijksregisternummer, welke hem wordt meegedeeld door de rechtspersoon.

Voor de toepassing van het eerste lid, 6°:

1° moet de rechtspersoon, alvorens te kunnen intekenen op een elektronische-communicatiedienst voor de natuurlijke persoon, een erkenning verkrijgen, verstrekt door de minister en de minister van Justitie, en met als voorwerp om na te gaan dat de persoon de democratische waarden vastgelegd in de Grondwet alsook dit artikel nakomt;

2° identificeert de rechtspersoon zich bij de operator overeenkomstig dit artikel;

3° identificeert de rechtspersoon de abonnees aan de hand van een van de identificatiedocumenten bedoeld in paragraaf 5, conform de vereisten inzake betrouwbaarheid bedoeld in paragraaf 4, of aan de hand van een andere methode die toegestaan is in de in 1° bedoelde erkenning;

4° bewaart de rechtspersoon een kopie van het andere identificatiedocument van de abonnees dan de Belgische elektronische identiteitskaart, behoudens afwijking toegestaan in de in 1° bedoelde erkenning;

5° bewaart de rechtspersoon een geactualiseerde lijst aan de hand waarvan het verband kan worden vastgesteld tussen de elektronische-communicatiedienst

prénom, l'adresse de la résidence, lorsque la personne en dispose, la date de naissance et le numéro par lequel elle est identifiée, tel le numéro de registre national.

Le Roi peut:

1° prévoir par méthode visée à l'alinéa 1er les conditions à respecter, une condition pouvant être l'obtention d'une autorisation préalable du ministre et du ministre de la Justice;

2° imposer des obligations aux opérateurs, aux personnes morales visées à l'alinéa 1er, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 10. Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Pour les services de communications électroniques mobiles fournis au moyen d'une carte prépayée, le Roi:

1° restreint la possibilité pour l'abonné de permettre à des tiers de bénéficier du service;

2° impose des obligations aux abonnés qui sont des personnes morales afin de déterminer les utilisateurs habituels du service.

L'opérateur qui offre une carte SIM ou toute carte équivalente, destinée à être intégrée dans un véhicule, conserve le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte. À la demande d'une autorité, l'opérateur ne lui communique que ce numéro de châssis ou le numéro de cette carte.

Le Roi peut fixer les modalités de l'obligation visée à l'alinéa 3 et peut imposer aux entreprises qui disposent

en de abonnees, met daarin ten minste de naam, de voornaam, het verblijfadres als de persoon dat heeft, de geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals het rijksregisternummer.

De Koning kan:

1° per in het eerste lid vermelde methode de voorwaarden vastleggen die moeten worden nageleefd, waarbij een voorwaarde het verkrijgen van een voorafgaande machtiging van de minister en van de minister van Justitie kan zijn;

2° verplichtingen opleggen aan de operatoren, aan de in het eerste lid bedoelde rechtspersonen, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 10. Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

De Koning, voor de mobiele elektronische-communicatiediensten verstrekt op basis van een voorafbetaalde kaart:

1° beperkt de mogelijkheid voor de abonnee om derden gebruik te laten maken van de dienst;

2° legt verplichtingen aan de abonnees die rechtspersonen zijn op om de gewoonlijke gebruikers van de dienst te identificeren.

De operator die een simkaart of een gelijkwaardige kaart aanbiedt die bestemd is om in een voertuig te worden ingebouwd, bewaart het chassisnummer van dat voertuig, evenals de link tussen het chassisnummer en het nummer van deze kaart. Op verzoek van een autoriteit deelt de operator haar enkel dat chassisnummer of het nummer van deze kaart mee.

De Koning kan de nadere bepalingen van de verplichting bedoeld in het derde lid vastleggen en

du numéro de châssis de le transmettre aux opérateurs.

§ 11. 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.

L'arrêté royal visé dans le présent article est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres."."

kan de ondernemingen die over het chassisnummer beschikken, verplichten om dat door te geven aan de operatoren.

§ 11. 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.

Het koninklijk besluit bedoeld in dit artikel wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad."."

JUSTIFICATION

Adaptation de l'article 127 de la loi télécom à la suite de l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle

Introduction

Le présent amendement a pour objectif de réparer la loi télécom à la suite de l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle. Par cet arrêt, la Cour constitutionnelle:

"— annule l'article 2 de la loi du 1er septembre 2016 "portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité", uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération;

— maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces

VERANTWOORDING

Aanpassing van artikel 127 van de telecomwet naar aanleiding van arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof

Inleiding

Dit amendement heeft tot doel de telecomwet te repareren naar aanleiding van arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof. Met dat arrest doet het Grondwettelijk Hof het volgende. Het:

"— vernietigt artikel 2 van de wet van 1 september 2016 "tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst", zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen;

— handhaaft de gevolgen van de vernietigde bepaling tot de inwerkingtreding van een wetskrachtige norm waarin die

données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus;

— rejette le recours pour le surplus, sous réserve des interprétations mentionnées en B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 et B.30.4." (dispositif de l'arrêt).

Les avis rendus par le Conseil d'État et l'Autorité de protection des données sur l'avant-projet de loi qui est devenu la loi du 1er septembre 2016 et sur l'avant-projet de loi "conservation des données"

Dans son arrêt précité, la Cour constitutionnelle estime que les avis de la Commission de la protection de la vie privée (actuellement l'Autorité de protection des données) et du Conseil d'État qui ont été rendus sur l'avant-projet de loi qui est devenu la loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après la loi du 1er septembre 2016) ont seulement été partiellement suivis, dès lors que cette loi ne reprend pas les données d'identification qui peuvent être collectées et traitées et les documents d'identification qui entrent en considération.

Cependant, des modifications à l'article 127 de la loi télécom étaient prévues dans le 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 leur fourniture aux autorités (ci-après le projet de loi "conservation des données"). À la suite de l'arrêt du 18 novembre 2021 de la Cour constitutionnelle, ces modifications ont été retirées de cet projet.

Dans le point 105 de son avis n° 108/2021 du 28 juin 202 sur l'avant-projet de loi "conservation des données", l'Autorité de protection des données a indiqué ce qui suit:

"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."

Il en ressort que selon l'Autorité de protection des données, la loi ne doit pas obligatoirement déterminer les données

identificatiegegevens en identificatiedocumenten worden opgesomd en uiterlijk tot en met 31 december 2022;

— verwerpt het beroep voor het overige, onder voorbehoud van de in B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 en B.30.4 vermelde interpretaties." (dictum van het arrest).

De adviezen die zijn verstrekt door de Raad van State en door de Gegevensbeschermingsautoriteit over het voorontwerp van wet dat de wet van 1 september 2016 is geworden en over het voorontwerp van wet "gegevensbewaring"

In zijn voormelde arrest is het Grondwettelijk Hof van oordeel dat de adviezen van de Commissie voor de bescherming van de persoonlijke levenssfeer (tegenwoordig de Gegevensbeschermingsautoriteit) en van de Raad van State die verstrekt zijn over het voorontwerp van wet dat de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten is geworden (hierna de wet van 1 september 2016) slechts gedeeltelijk zijn gevolgd, omdat deze wet niet bepaalt welke identificatiegegevens verzameld en verwerkt mogen worden en welke identificatiedocumenten in aanmerking komen.

In dat 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 (hierna het wetsontwerp "gegevensbewaring") waren evenwel wijzigingen in artikel 127 van de telecomwet vastgesteld. Naar aanleiding van het arrest van 18 november 2021 van het Grondwettelijk Hof zijn die wijzigingen uit dat ontwerp verwijderd.

In punt 105 van haar advies nr. 108/2021 van 28 juni 2021 over het voorontwerp van de wet "gegevensbewaring" heeft de Gegevensbeschermingsautoriteit het volgende aangegeven:

"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."

Daaruit vloeit voort dat volgens de Gegevensbeschermingsautoriteit, de wet niet verplicht de

d'identification et les copies du document d'identification à collecter et à conserver par l'opérateur, étant donné que cela peut être fait par arrêté royal.

Dans son avis n° 69 381/4 du 28 juin 2021 sur ce même avant-projet de loi, le Conseil d'État a fait des remarques sur les modifications à l'article 127 de la loi télécom mais n'a pas fait de remarque sur l'article 127, § 3, alinéa 1er, 3°, en projet, qui permettait au Roi de "déterminer les données et documents d'identification à collecter et à conserver par l'opérateur".

L'exigence de fixer dans la loi les éléments essentiels du traitement de données et les motifs qui peuvent justifier que certaines règles se trouvent dans un arrêté royal

Dans l'arrêt du 18 novembre 2021, la Cour constitutionnelle rappelle ce qui suit:

— "B.6. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout justiciable qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

— Une délégation au pouvoir exécutif n'est toutefois pas contraire au principe de la légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.";

— "B.8.4.2. […] la délégation d'éléments essentiels d'une matière réservée par le Constituant au pouvoir législatif n'est possible que si le respect de la procédure parlementaire ne permet pas au législateur de réaliser un objectif d'intérêt général et à condition qu'il détermine explicitement et sans équivoque l'objet de cette habilitation et que les mesures prises par le Roi soient examinées par le pouvoir législatif, en vue de leur confirmation, dans un délai relativement court, fixé dans la loi d'habilitation."

La Cour estime que la loi du 1er septembre 2016 ne répond pas à ces exigences, dès lors qu'elle considère que les données d'identification qui sont collectées et traitées et les

identificatiegegevens en de kopieën van identificatiedocumenten die door de operator verzameld en bewaard moeten worden, moet bepalen, aangezien dat via koninklijk besluit kan gebeuren.

In zijn advies nr. 69 381/4 van 28 juni 2021 over datzelfde voorontwerp van wet heeft de Raad van State opmerkingen gemaakt over de wijzigingen in artikel 127 van de telecomwet, maar heeft hij geen opmerking gemaakt over het ontworpen artikel 127, § 3, eerste lid, 3°, dat de Koning in staat zou stellen om "de door de operator te verzamelen en bewaren identificatiegegevens en –documenten [te] bepalen".

De eis om in de wet de essentiële elementen van de gegevensverwerking vast te stellen en de redenen die kunnen rechtvaardigen waarom sommige regels zich in een koninklijk besluit bevinden

In het arrest van 18 november 2021 herinnert het Grondwettelijk Hof aan het volgende:

— "B.6. Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

— Een delegatie aan de uitvoerende macht is evenwel niet in strijd met het wettigheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld.";

— "B.8.4.2. […] Een delegatie van essentiële elementen van een door de Grondwetgever aan de formele wetgever voorbehouden aangelegenheid is immers slechts mogelijk indien de inachtneming van de parlementaire procedure de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken, en op voorwaarde dat hij het onderwerp van die machtiging uitdrukkelijk en ondubbelzinnig vaststelt en dat de door de Koning genomen maatregelen door de wetgevende macht worden onderzocht met het oog op hun bekrachtiging binnen een relatief korte termijn, vastgesteld in de machtigingswet."

Het hof is van oordeel dat de wet van 1 september 2016 niet aan die eisen voldoet, omdat het ervan uitgaat dat de identificatiegegevens die worden verzameld en verwerkt en de

documents d'identification qui entrent en considération constituent des "éléments essentiels d'un traitement de données à caractère personnel" (point B.8.4.2. de l'arrêt), qui doivent dès lors être déterminés dans la loi, ce qui n'est pas le cas pour ce qui concerne la loi du 1er septembre 2016.

Cependant, dans son avis n° 68 936/AG du 7 avril 2021 sur un avant-projet de loi "relative aux mesures de police administrative lors d'une situation d'urgence épidémique", le Conseil d'État a considéré ce qui suit:

"101. Conformément à l'article 22 de la Constitution, tout traitement de données à caractère personnel et, plus généralement, toute atteinte au droit à la vie privée, sont soumis au respect d'un principe de légalité formelle.

En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les "éléments essentiels" sont fixés préalablement par le législateur. Par conséquent, les "éléments essentiels" des traitements de données à caractère personnel doivent être fixés dans la loi elle-même. À cet égard, la section de législation considère que, quelle que soit la matière concernée, constituent, en principe, des "éléments essentiels" les éléments suivants: 1°) les catégories de données traitées; 2°) les catégories de personnes concernées; 3°) la finalité poursuivie par le traitement; 4°) les catégories de personnes ayant accès aux données traitées; et 5°) le délai maximal de conservation des données." (c'est nous qui soulignons)

Il en ressort que le Conseil d'État n'exige pas que la loi fasse une liste des données traitées mais seulement qu'elle reprenne les catégories de données traitées.

Dans son arrêt précité, la Cour constitutionnelle rappelle que la loi du 1er septembre 2016 ne fixe pas de liste de données d'identification ou de documents d'identité, à part la carte d'identité électronique belge et le numéro de registre national et que la méthode de travail consistait à permettre

identificatiedocumenten die in aanmerking komen, "essentiele elementen van een verwerking van persoonsgegevens" vormen (punt B.8.4.2. van het arrest), die daarom in de wet moeten worden bepaald, hetgeen niet het geval is wat de wet van 1 september 2016 betreft.

In zijn advies nr. 68 936/AG van 7 april 2021 over een voorontwerp van wet "betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie" heeft de Raad van State evenwel het volgende geoordeeld:

"101. Krachtens artikel 22 van de Grondwet geldt voor elke verwerking van persoonsgegevens en, meer in het algemeen, voor elke schending van het recht op het privéleven, dat het formeel legaliteitsbeginsel dient te worden nageleefd.

Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de "essentiële elementen" voorafgaandelijk door de wetgever vastgesteld zijn. Bijgevolg moeten de "essentiële elementen" van de verwerking van persoonsgegevens in de wet zelf worden vastgelegd. In dat verband is de afdeling Wetgeving van oordeel dat ongeacht de aard van de betrokken aangelegenheid, de volgende elementen in beginsel "essentiële elementen" uitmaken: 1°) de categorie van verwerkte gegevens; 2°) de categorie van betrokken personen; 3°) de met de verwerking nagestreefde doelstelling; 4°) de categorie van personen die toegang hebben tot de verwerkte gegevens; en 5°) de maximumtermijn voor het bewaren van de gegevens." (wij onderlijnen)

Daaruit blijkt dat de Raad van State niet eist dat de wet een lijst van de verwerkte gegevens opstelt, maar enkel dat daarin de categorieën van verwerkte gegevens moeten worden vermeld.

In zijn voormelde arrest herinnert het Grondwettelijk Hof eraan dat de wet van 1 september 2016 geen lijst van identificatiegegevens of –documenten vaststelt, behalve de Belgische elektronische identiteitskaart en het rijksregisternummer, en dat de werkwijze erin bestond om het aan de Koning toe te

au Roi de les déterminer, ce choix étant justifié comme suit dans l'exposé des motifs:

"B.8.4.3. Lors des travaux préparatoires, le législateur justifie cette méthode de travail par le caractère technique des données d'identification et des documents d'identification, la nécessité de pouvoir en adapter l'énumération en fonction de nouveaux enseignements et le fait que, dans le cadre de la conservation des données, ces données n'étaient pas non plus énumérées dans l'article 126 de la loi du 13 juin 2005 lui-même annulé par l'arrêt de la Cour n° 57/2021 du 22 avril 2021.

Indépendamment du fait que ces arguments ne sauraient expliquer l'absence d'une habilitation explicite et sans équivoque, le caractère technique des données d'identification et des documents d'identification et l'adaptabilité d'une telle énumération ne suffisent pas pour conclure que le fait d'ancrer de tels éléments dans une norme législative ne permettrait pas au législateur de réaliser un objectif d'intérêt général. En effet, même une norme législative peut être modifiée. Le Conseil des ministres ne démontre pas qu'une modification de ces données d'identification peut être urgente au point de ne pas pouvoir suivre le cours normal de la procédure législative. De même, une énumération des données d'identification et des documents d'identification n'est pas complexe au point de ne pas pouvoir être inscrite dans une norme législative. Enfin, le législateur ne saurait justifier une violation de la Constitution en renvoyant à une autre disposition législative qui comportait peut-être la même inconstitutionnalité."

Les différents sujets traités par l'article 127 de la loi télécom

Dans le cadre de l'avant-projet de loi "conservation des données", il était prévu de revoir l'article 127 de la loi télécom pour rendre cette loi plus lisible.

En effet, l'ancien article 127 mélangeait différentes matières que sont:

— l'identification de l'abonné et de l'utilisateur habituel du service de communications électroniques (dorénavant reprise à l'article 127);

— des délégations au Roi pour fixer la collaboration des opérateurs entre autres avec les autorités judiciaires (dorénavant reprises à l'article 127/3 inséré par le projet de loi "conservation des données");

staan om die te bepalen, waarbij die keuze als volgt in de memorie van toelichting werd gerechtvaardigd:

"B.8.4.3. In de parlementaire voorbereiding verantwoordt de wetgever die manier van werken door te verwijzen naar de technische aard van de identificatiegegevens en identificatiedocumenten, de noodzaak om de oplijsting daarvan te kunnen aanpassen in het licht van gewijzigde inzichten, en het feit dat ook in het kader van de dataretentie die gegevens niet in het bij het arrest van het Hof nr. 57/2021 van 22 april 2021 vernietigde artikel 126 van de wet van 13 juni 2005 zelf werden opgesomd.

Nog afgezien van het feit dat die argumenten de afwezigheid van een uitdrukkelijke en ondubbelzinnige machtiging niet kunnen verklaren, volstaan de technische aard van identificatiegegevens en identificatiedocumenten en de aanpasbaarheid van een dergelijke oplijsting niet om te besluiten dat een verankering ervan in een wetskrachtige norm de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken. Ook een wetskrachtige norm kan immers worden gewijzigd. De Ministerraad toont niet aan dat een wijziging van die identificatiegegevens zo dringend kan zijn dat het normale verloop van de wetgevende procedure niet kan worden gevolgd. Een oplijsting van identificatiegegevens en identificatiedocumenten is ook niet dermate complex dat zij niet in een wetskrachtige norm kan worden opgenomen. Tot slot kan de wetgever een schending van de Grondwet niet rechtvaardigen door te verwijzen naar een andere wetsbepaling die mogelijk dezelfde ongrondwettigheid bevatte."

De verschillende onderwerpen die door artikel 127 van de telecomwet worden behandeld

In het kader van het voorontwerp van wet "gegevensbewaring" was het de bedoeling om artikel 127 van de telecomwet te herzien, teneinde die wet leesbaarder te maken.

Het oude artikel 127 vormde immers een mengeling van verschillende materies, namelijk:

— de identificatie van de abonnee en van de gewoonlijke gebruiker van de elektronische-communicatiedienst (voortaan opgenomen in artikel 127);

— delegaties aan de Koning om de medewerking van de operatoren vast te stellen onder andere met de gerechtelijke autoriteiten (voortaan opgenomen in artikel 127/3 ingevoegd door het wetsontwerp "gegevensbewaring");

— les règles en matière de système d'encryptage (dorénavant reprises à l'article 107/5 remplacé par le projet de loi "conservation des données").

La disposition au sein du paragraphe 1er de l'article 127 qui indiquait que l'opérateur est le responsable du traitement a été déplacée vers un article commun à plusieurs dispositions (voir art. 127/3 inséré par le projet de loi "conservation des données").

Le paragraphe 3 de l'article 127 a été supprimé, étant donné que la loi du 1er septembre 2016 a mis fin à l'anonymat pour les cartes prépayées.

Renforcement de l'obligation d'identification de l'abonné

Dans son avis sur les amendements, l'Autorité de protection des données indique que les éléments suivants rendent plus strict l'obligation pour les opérateurs d'identifier leurs abonnés et augmentent donc l'ingérence de la loi dans les droits et libertés des individus.

Au point 40 de son avis, l'Autorité de protection des données indique à juste titre que l'obligation pour un opérateur d'identifier ses abonnés est étendue, étant donné que la notion d'opérateur au sens de la loi télécom a été élargie par la loi du 21 décembre 2021 loi portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques. À la suite de cette loi, les entreprises qui fournissent au public des services de communications interpersonnelles non fondés sur la numérotation (les fournisseurs de services "over the top" ou "OTT") sont considérés comme des opérateurs au sens de la loi télécom.

De l'avis du gouvernement, cette extension de l'obligation d'identification aux OTT est pleinement justifiée vu l'utilisation par les "criminels" de leurs services, qui sont en pleine croissance. En ce sens, la loi suit les évolutions techniques et économiques. Par ailleurs, il ne serait pas acceptable que les opérateurs "traditionnels" belges aient des obligations strictes en matière d'identification de leurs abonnés, alors que les opérateurs OTT n'aient aucune obligation en la matière. Par ailleurs, ne pas obliger les OTT à conserver des données qui permettent aux autorités d'identifier leurs abonnés fragiliserait aussi très fortement l'obligation d'identification, dès lors qu'il suffirait pour un criminel d'utiliser un service d'OTT pour échapper à toute identification.

— de regels inzake versleutelingssysteem (voortaan opgenomen in artikel 107/5 vervangen door het wetsontwerp "gegevensbewaring").

De bepaling binnen paragraaf 1 van artikel 127 die aangaf dat de operator verantwoordelijk is voor de verwerking, is verplaatst naar een gemeenschappelijk artikel met verscheidene bepalingen (zie art. 127/3 ingevoegd door het wetsontwerp "gegevensbewaring").

Paragraaf 3 van artikel 127 werd geschrapt aangezien de wet van 1 september 2016 een einde heeft gemaakt aan de anonimiteit van de vooraf betaalde kaarten.

Uitbreiding van de verplichting tot identificatie van de abonnee

De Gegevensbeschermingsautoriteit wijst er in haar advies over de amendementen op dat de volgende elementen de verplichting voor de operatoren om hun abonnees te identificeren strenger maken en derhalve leiden tot een aanzienlijke toename van de inmenging van de wet in de rechten en vrijheden van het individu.

De Gegevensbeschermingsautoriteit merkt in punt 40 van haar advies terecht op dat de verplichting voor een operator om zijn abonnees te identificeren wordt uitgebreid, aangezien het begrip "operator" in de zin van de telecomwet werd uitgebreid bij de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie. Ingevolge die wet worden de ondernemingen die aan het publiek interpersoonlijke communicatiediensten aanbieden die nummeronafhankelijk zijn (de aanbieders van "over the top"-diensten of "OTT's"), beschouwd als operatoren in de zin van de telecomwet.

De regering is de mening toegedaan dat deze uitbreiding van de identificatieplicht met de OTT's geheel gerechtvaardigd is, gelet op het gebruik dat de "criminelen" maken van hun diensten, die in volle groei zijn. In die zin volgt de wet de technische en economische evoluties. Voorts zou het niet aanvaardbaar zijn dat er voor de "traditionele" Belgische operatoren strenge verplichtingen zouden gelden op vlak van de identificatie van hun abonnees, terwijl er voor de operatoren van de OTT's ter zake geen enkele verplichting zou gelden. De OTT's niet verplichten om gegevens te bewaren die het voor de autoriteiten mogelijk maken om hun abonnees te identificeren, zou daarnaast ook de identificatieplicht heel erg verzwakken, aangezien het voor een crimineel zou volstaan om een OTT-dienst te gebruiken om aan enige identificatie te ontsnappen.

Contrairement à ce que l'Autorité de protection des données indique dans son avis, la notion de services de communications électroniques au sens de la loi télécom incluait déjà avant la loi du 21 décembre 2021 précitée les "services consistant entièrement ou principalement en la transmission de signaux" (ce qui incluait déjà les services de transmission utilisés pour la fourniture de services de machine à machine). Par ailleurs, cette Autorité déduit de l'article 1er de l'arrêté royal "cartes prépayées" (AR du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée) que "dans le contexte normatif actuel, les détenteurs d'une carte SIM utilisée uniquement dans le cadre d'une communication "M2M" ne sont pas soumis à une obligation d'identification". Il est correct que l'article 1er de cet arrêté royal exclut de son champ d'application les "cartes prépayées permettant exclusivement la technologie M2M". Par contre, il n'est pas correct que les opérateurs ne doivent pas identifier les abonnés de ce type de cartes prépayées. Une obligation d'identification résulte de l'article 127 de la loi télécom mais les modalités de cette obligation d'identification ne sont pas réglées par cet arrêté.

Au point 40 de son avis, l'Autorité de protection des données considère que "les autorités qui pourront avoir accès aux données d'identification des abonnés aux services de communications électroniques seront plus nombreuses que celles qui peuvent avoir accès à ces données dans la version actuelle des articles 126 et 127." Or, de l'avis du gouvernement, l'article 127/1 en projet de la loi télécom n'étend pas la liste des autorités qui peuvent demander des données d'identification aux opérateurs. Il ne fait qu'établir un cadre commun que doivent respecter les lois organiques / sectorielles propres à chaque autorité. Ce sont in fine ces dernières lois qui déterminent le nombre d'autorités qui peuvent obtenir des données d'identification des opérateurs. Par ailleurs, le fait qu'un certain nombre d'autorités aient besoin d'obtenir des opérateurs des données d'identification pour remplir leurs missions montre l'importance de l'obligation des opérateurs d'identifier leurs abonnés ou de rendre possible cette identification.

Au point 40 de son avis, l'Autorité de protection des données cite un passage de la justification de l'amendement: "l'ancien article 127, § 2, contenait une interdiction pour les opérateurs de rendre difficile ou impossible l'identification des utilisateurs finaux. Le nouvel article 127 comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés (méthode d'identification directe) ou à tout le moins de rendre cette identification possible (méthode

In tegenstelling tot wat de Gegevensbeschermingsautoriteit beweert in haar advies, omvatte het begrip "elektronischecommunicatiediensten" in de zin van de telecomwet reeds vóór de voor voornoemde wet van 21 december 2022 de "diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen" (wat de transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt reeds omvatte). Voorts leidt de Gegevensbeschermingsautoriteit uit artikel 1 van het koninklijk besluit "voorafbetaalde kaarten" (KB van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronischecommunicatiediensten die worden geleverd op basis van een voorafbetaalde kaart) dat "[...] in de huidige normatieve context voor houders van een SIM-kaart die uitsluitend voor "M2M communicatie" wordt gebruikt, geen identificatieplicht [geldt]." Het klopt dat in artikel 1 van het koninklijk besluit in kwestie de "voorafbetaalde kaarten waarmee enkel de M2M-technologie kan worden gebruikt" worden uitgesloten van het toepassingsgebied ervan. Het klopt echter niet dat de operatoren de abonnees van die soort voorafbetaalde kaarten niet moeten identificeren. Uit artikel 127 van de telecomwet vloeit een identificatieplicht voort, maar die identificatieplicht is niet nader geregeld in het bedoelde koninklijk besluit.

De Gegevensbeschermingsautoriteit stelt in punt 40 van haar advies dat "[m]eer autoriteiten toegang [zullen] kunnen krijgen tot de identificatiegegevens van abonnees van elektronische-communicatiediensten dan op grond van de huidige versie van de artikelen 126 en 127 het geval is."De regering is evenwel van mening dat het ontworpen artikel 127/1 van de telecomwet de lijst van de autoriteiten die identificatiegegevens kunnen opvragen bij de operatoren niet uitbreidt. Het voorziet enkel in een gemeenschappelijk kader dat in acht moet worden genomen in de specifieke organieke/sectoriële wetten voor de verschillende autoriteiten. In fine zijn het die wetten die bepalend zijn voor het aantal autoriteiten die identificatiegegevens kunnen verkrijgen van de operatoren. Voorts wijst het gegeven dat een aantal autoriteiten identificatiegegevens van de operatoren moeten krijgen om hun opdrachten te kunnen vervullen op het belang van de verplichting voor de operatoren om hun abonnees te identificeren of om die identificatie mogelijk te maken.

De Gegevensbeschermingsautoriteit citeert in punt 40 van haar advies een passage uit de verantwoording van het amendement: "Het oude artikel 127, § 2, bevatte een verbod voor de operatoren om de identificatie van de eindgebruikers te bemoeilijken of onmogelijk te maken. Het nieuwe artikel 127 bevat nu een positieve verplichting voor de operatoren om hun abonnees te identificeren (directe identificatiemethode) of op zijn minst deze identificatie mogelijk te maken (indirecte

d'identification indirecte)". De l'avis du gouvernement, cette modification rend la loi plus claire.

Au point 40 de son avis, l'Autorité de protection des données indique à juste titre ce qui suit: "le nouvel article 127 § 1er interdit, sous peine de sanction pénale, de distribuer en Belgique des cartes prépayées ou des abonnements qui permettent aux utilisateurs finaux d'y utiliser un service de communications électroniques ou encore des objets connectés qui permettent l'utilisation d'un service d'accès à Internet ou d'un service de communication interpersonnelle, sans avoir obtenu l'accord de l'entreprise qui fournit ce service de communications électroniques accessible au public. L'entreprise qui donne son accord doit être considérée comme un opérateur tenu au respect de l'obligation imposée par ce nouvel article 127. Cette interdiction vise à empêcher tout contournement de l'obligation qui pèse sur les opérateurs d'identifier les utilisateurs finaux des services de communications électroniques qu'ils fournissent."

Concernant l'ingérence qu'entraine l'identification des abonnés des opérateurs, il convient de noter que dans son arrêt Quadrature du Net du 6/10/2020 (aff. Jointes C-511/18, La Quadrature du Net e.a.; C-512/18, French Data Network e.a.; C-520/18, OBFG e.a.), la Cour de Justice de l'Union européenne a indiqué que la conservation des données relatives à l'identité civile constitue une ingérence non grave dans les droits repris dans la Charte des droits fondamentaux de l'Union européenne (en particulier le droit à la vie privée et le droit à la protection des données à caractère personnel).

En effet, ces données ne donnent pas d'information sur la communication, ni sur la localisation de l'utilisateur final.

Finalement, cette ingérence est nécessaire pour que les différentes autorités qui peuvent obtenir des données d'identification de l'opérateur puissent remplir leurs missions.

L'anonymat des correspondances et la liberté d'expression

Dans son avis sur les amendements, l'Autorité de protection des données indique que le renforcement de l'obligation d'identification de l'abonné au vu des éléments repris ci-dessus:

— "aboutit à rendre impossible – ou en tout cas très difficile – toute correspondance anonyme sur Internet" (point 24), alors que la CJUE a indiqué "dans l'arrêt du 6 octobre 2020: "[…] les internautes disposent, conformément à ce qui a été

identificatiemethode)." De regering is van mening dat die wijziging de wet duidelijker maakt.

De Gegevensbeschermingsautoriteit wijst in punt 40 van haar advies terecht op het volgende: "[...] het nieuwe artikel 127, § 1, verbiedt, op straffe van strafrechtelijke sancties, de distributie in België van voorafbetaalde kaarten of abonnementen waarmee eindgebruikers een elektronische-communicatiedienst kunnen gebruiken, of van daarmee verbonden voorwerpen die het gebruik van een internettoegangsdienst of een interpersoonlijke-communicatiedienst mogelijk maken, zonder de toestemming te hebben verkregen van de onderneming die deze openbare elektronische-communicatiedienst aanbiedt. De onderneming die haar toestemming geeft, moet worden beschouwd als een operator die gebonden is door opgelegde verplichting krachtens dit nieuwe artikel 127. Dit verbod is bedoeld om te voorkomen dat de verplichting van de operatoren om de eindgebruikers van de door hen aangeboden elektronische-communicatiediensten, te identificeren, wordt omzeild."

Met betrekking tot de inmenging waartoe de identificatie van de abonnees van de operatoren leidt, dient te worden opgemerkt dat in zijn arrest-Quadrature du Net van 6/10/2020 (gevoegde zaken C-511/18, La Quadrature du Net e.a.; C-512/18, French Data Network e.a.; C-520/18, OBFG e.a.), het Europees Hof van Justitie heeft aangegeven dat de bewaring van gegevens met betrekking tot de burgerlijke identiteit, een niet-ernstige inmenging vormt in de rechten vervat in het Handvest van de grondrechten van de Europese Unie (in het bijzonder het recht op de persoonlijke levenssfeer en het recht op de bescherming van de persoonsgebonden gegevens).

Deze gegevens onthullen immers geen informatie over de communicatie, noch over de locatie van de eindgebruiker.

Uiteindelijk is deze inmenging noodzakelijk opdat de verschillende autoriteiten die identificatiegegevens van de operator kunnen verkrijgen hun opdrachten kunnen vervullen.

Anonimiteit van de correspondentie en vrije meningsuiting

De Gegevensbeschermingsautoriteit merkt in haar advies over de amendementen op dat de uitbreiding van de verplichting om de abonnee te identificeren in het licht van de bovenstaande elementen:

— "[...] onmogelijk – of op zijn minst zeer moeilijk – [maakt] om anoniem te corresponderen op het internet" (punt 24), terwijl het HJEU in zijn arrest van 6 oktober 2020 stelde dat "[…] internetgebruikers, zoals in punt 109 van het

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 […]" (point 155 de l'arrêt et note de bas de page n° 8 de l'avis de l'Autorité de protection des données);

— "pourrait avoir un "effet dissuasif" ou "effet inhibiteur" sur l'exercice du droit à la liberté d'expression par le biais de moyens de communications électroniques." (note de bas de page n° 9).

Tout d'abord, l'Autorité de protection des données fait référence au point 155 de l'arrêt du 6 octobre 2020 (arrêt La Quadrature du Net), qui renvoie lui-même vers le point 109 du même arrêt. Dans ce dernier point la CJUE indique qu'en adoptant la directive "e-privacy" (directive 2002/58), "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."

Le fait que "les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications […]restent […] anonymes" n'implique pas que les utilisateurs auraient un droit à l'anonymat. En effet, le principe mentionné par la CJUE connait une exception, à savoir le cas où l'autorité peut légalement identifier une ou plusieurs parties à la communication.

L'article 5.1 de la directive e-privacy prévoit ce qui suit:

"1. 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."

Il convient de rappeler que les données de trafic qui permettent la transmission des communications ne sont pas confidentielles par rapport à l'opérateur, dès lors qu'il les traite ou génère. La confidentialité de ces données de trafic signifie que les opérateurs ne peuvent en principe pas les communiquer à des tiers. Ce principe connait cependant des exceptions, dès lors que les autorités peuvent dans certains cas exiger d'un opérateur certaines données de trafic.

onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop [moeten] kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld […]" (punt 155 van het arrest en voetnoot nr. 8 van het advies van de Gegevensbeschermingsautoriteit);

— "een [...] "afschrikkend effect" of een "remmend effect" [...] zou kunnen hebben op de uitoefening van het recht op vrije meningsuiting via elektronische-communicatiemedia." (voetnoot nr. 9).

De Gegevensbeschermingsautoriteit verwijst in de eerste plaats naar punt 155 van het arrest van 6 oktober 2020 (arrest-La Quadrature du Net), waarin wordt verwezen naar punt 109 van hetzelfde arrest. In dat punt 109 wijst het HJEU erop dat, met de vaststelling van de "e-privacy"-richtlijn (Richtlijn 2002/58), "de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten [heeft] 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."

Het gegeven dat "de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie [...] anoniem [blijft]" houdt niet in dat de gebruikers een recht op anonimiteit hebben. Op het beginsel dat het HJEU vermeldt, bestaat er immers een uitzondering, namelijk het geval waarin de overheid een of meerdere partijen bij de communicatie wettelijk mag identificeren.

In artikel 5.1 van de e-privacy-richtlijn is het volgende bepaald:

"1. De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische-communicatiediensten."

Er moet worden opgemerkt dat de verkeersgegevens die het overbrengen van communicatie mogelijk maken niet vertrouwelijk zijn wat de operator betreft, aangezien hij ze verwerkt of genereert. De vertrouwelijkheid van deze verkeersgegevens houdt in dat de operatoren ze in beginsel niet mogen meedelen aan derden. Op dat beginsel zijn er evenwel uitzonderingen, aangezien de autoriteiten in een aantal gevallen van een operator kunnen eisen om bepaalde verkeersgegevens mee te delen.

Il ressort de la définition de données de trafic au sens de l'article 2 de la directive e-privacy que les données de trafic comprennent également les données traitées en vue de la facturation d'un service de communications électroniques. Ces données de facturation comprennent l'identité civile de l'abonné, dès lors que l'opérateur doit pouvoir adresser la facture à une personne déterminée et doit disposer des informations lui permettant d'introduire une procédure en justice pour récupérer le montant des factures impayées. Ces données d'identité civile ne sont pas des informations confidentielles par rapport à l'opérateur, qui les traite. La confidentialité de ces données d'identité civile signifie que les opérateurs ne peuvent en principe pas les communiquer à des tiers. Ce principe connait cependant des exceptions, dès lors que les autorités peuvent dans certains cas exiger d'un opérateur de leur fournir l'identité de l'abonné.

Il en résulte que la directive e-privacy ne consacre pas un droit à l'anonymat.

Dans son arrêt du 5 avril 2022 (affaire C-140/20, G.D.), la CJUE a indiqué ce qui suit: "la directive 2002/58 ne s'oppose pas, aux fins de la lutte contre la criminalité en général, à la conservation généralisée des données relatives à l'identité civile. Dans ces conditions, il y a lieu de préciser que ni cette directive ni aucun autre acte du droit de l'Union ne s'opposent à une législation nationale, ayant pour objet la lutte contre la criminalité grave, en vertu de laquelle l'acquisition d'un moyen de communication électronique, tel qu'une carte SIM prépayée, est subordonnée à la vérification de documents officiels établissant l'identité de l'acheteur et à l'enregistrement, par le vendeur, des informations en résultant, le vendeur étant le cas échéant tenu de donner accès à ces informations aux autorités nationales compétentes" (point 72).

Par ailleurs, la Cour constitutionnelle, dans son arrêt n° 158/2021 du 18 novembre 2021 rendu dans le cadre du recours en annulation de la loi du 1er septembre 2016 "portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité" (loi "cartes prépayées") n'a pas annulé la loi "cartes prépayées" au motif que les abonnés auraient un droit à l'anonymat.

Dans cet arrêt, la Cour constitutionnelle a indiqué ce qui suit:

"B. 22. Un tel lien indirect entre la suppression, attaquée, de l'anonymat des cartes de téléphonie mobile prépayées et

Uit de definitie van verkeersgegevens in de zin van artikel 2 van de e-privacy-richtlijn blijkt dat de verkeersgegevens ook de gegevens omvatten die worden verwerkt met het oog op de facturatie van een elektronische-communicatiedienst. Die facturatiegegevens omvatten de burgerlijke identiteit van de abonnee, aangezien de operator de factuur moet kunnen versturen naar een bepaalde persoon en moet kunnen beschikken over de gegevens die hem in staat stellen een gerechtelijke procedure te starten om het bedrag van de onbetaalde facturen te vorderen. Deze burgerlijke-identiteitsgegevens zijn geen vertrouwelijke gegevens voor de operator, die ze verwerkt. De vertrouwelijkheid van deze burgerlijke-identiteitsgegevens houdt in dat de operatoren ze in beginsel niet mogen meedelen aan derden. Op dat beginsel zijn er evenwel uitzonderingen, aangezien de autoriteiten in een aantal gevallen van een operator kunnen eisen om hun de identiteit van de abonnee mee te delen.

Daaruit volgt dat e-privacy-richtlijn geen recht op anonimiteit inhoudt.

Het HJEU stelde in zijn arrest van 5 april 2022 (zaak C-140/20, G.D.) het volgende: "[...] Richtlijn 2002/58 [staat] er niet aan in de weg dat met het oog op de algemene bestrijding van criminaliteit gegevens over de burgerlijke identiteit algemeen worden bewaard. Daarbij moet worden gepreciseerd dat noch deze richtlijn noch enige andere handeling van Unierecht zich verzet tegen nationale wetgeving die tot doel heeft zware criminaliteit te bestrijden en die de toekenning van een elektronisch communicatiemiddel, zoals een vooraf betaalde simkaart, afhankelijk stelt van de verificatie van officiële documenten waaruit de identiteit van de koper blijkt, en van de registratie door de verkoper van de daarin vervatte informatie, waarbij de verkoper in voorkomend geval gehouden is de bevoegde nationale autoriteiten toegang tot deze informatie te geven." (punt 72).

Voorts heeft het Grondwettelijk Hof in zijn arrest nr. 158/2021 van 18 november 2021, gewezen in het kader van het beroep tot vernietiging van de wet van 1 september 2016 "tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten" (wet "voorafbetaalde kaarten"), die wet niet vernietigd om de reden dat de abonnees een recht op anonimiteit zouden hebben.

In dit arrest wijst het Grondwettelijk Hof op het volgende:

"B. 22. [...] Een dergelijk onrechtstreeks verband tussen de bestreden afschaffing van de anonimiteit van vooraf betaalde

le contenu des communications effectuées ne suffit pas pour considérer que la loi attaquée limite la liberté d'expression. La simple collecte de données d'identification de tous les utilisateurs finaux d'un réseau de communications électroniques ne saurait justifier la crainte, dans un État de droit démocratique, que toutes les communications menées sur ce réseau seront supervisées par les pouvoirs publics. La loi attaquée ne saurait dès lors avoir pour effet, par elle-même, de dissuader des personnes d'exprimer leur opinion ou de partager des informations avec des journalistes ou avec des personnalités politiques."

Un principe essentiel est qu'une personne doit rendre compte de ses actes, tant sur le plan civil que pénal. L'anonymat met en péril ce principe. La possibilité d'identifier l'abonné permet de le mettre en œuvre. Il est également essentiel qu'il soit possible pour les autorités (autorités judiciaires, services de renseignement et de sécurité et autres autorités qui peuvent demander des données de trafic ou d'identification aux opérateurs) de pouvoir retrouver l'identité de l'abonné.

Mais il est correct que l'identité de l'abonné doit être protégée, ce qui est le cas en Belgique entre autres par les mesures suivantes:

— l'identité de l'abonné collectée par les opérateurs pour les besoins des autorités ne peut être utilisée par les opérateurs pour leurs propres besoins ni être transférée à autre personne qu'une autorité, ce qui n'empêche pas les opérateurs de collecter également cette identité pour leurs propres besoins, conformément aux dispositions applicables (voir article 127/2, § 2, 3° en projet de la loi télécom);

— lorsque l'opérateur offre un service gratuit, il ne peut pas mettre en œuvre une méthode d'identification directe (cf. *infra*).

L'efficacité de la mesure d'identification de l'abonné et les possibilités de contourner la mesure

Dans son avis sur les amendements, l'Autorité de protection des données remet aussi en cause l'efficacité de l'obligation d'identification:

— "les "criminels" qui souhaitent échapper à la surveillance des moyens de communications électroniques par les autorités trouveront d'autres moyens de communication qui leur permettront de préserver leur anonymat" (point 41);

belkaarten en de inhoud van gevoerde communicaties volstaat niet om de bestreden wet als een beperking op de vrijheid van meningsuiting aan te merken. De loutere verzameling van identificatiegegevens van alle eindgebruikers van een elektronischecommunicatienetwerk kan in een democratische rechtsstaat niet de vrees rechtvaardigen dat alle communicatie over dat netwerk door de overheid zal worden gemonitord. De bestreden wet kan er bijgevolg op zich niet toe leiden dat personen worden ontmoedigd om hun mening te uiten of om informatie te delen met journalisten of politici."

Het is een wezenlijk beginsel dat een persoon rekenschap moet afleggen van zijn daden, zowel op burgerrechtelijk als op strafrechtelijk vlak. De anonimiteit brengt dat beginsel in gevaar. De mogelijkheid om de abonnee te identificeren staat toe om het ten uitvoer te leggen. Het is ook van essentieel belang dat het voor de autoriteiten (gerechtelijke autoriteiten, inlichtingen- en veiligheidsdiensten en andere autoriteiten die bij de operatoren verkeers- of identificatiegegevens kunnen opvragen) mogelijk is om de identiteit van de abonnee te kunnen achterhalen.

Het is echter wel zo dat de identiteit van de abonnee moet worden beschermd, wat in België het geval is, onder andere door de volgende maatregelen:

— de identiteit van de abonnee die de operatoren vergaren voor de behoeften van de autoriteiten, mag door de operatoren niet worden gebruikt voor hun eigen behoeften, noch aan iemand anders dan een autoriteit worden doorgegeven. Dat belet de operatoren niet om die identiteit ook te vergaren voor hun eigen behoeften, zulks overeenkomstig de toepasselijke bepalingen (zie het ontworpen artikel 127/2, § 2, 3°, van de telecomwet);

— wanneer de operator een gratis dienst aanbiedt, mag hij geen directe identificatiemethode uitvoeren (cf. *infra*).

Doeltreffendheid van de maatregel inzake de identificatie van de abonnee en mogelijkheden om de maatregel te omzeilen

De Gegevensbeschermingsautoriteit stelt in haar advies over de amendementen ook de doeltreffendheid van de identificatieplicht ter discussie:

— "[...] criminelen die de controle van elektronische communicatiemiddelen door de autoriteiten willen vermijden, [zullen] andere communicatiemiddelen [...] vinden waarmee zij anoniem kunnen blijven" (punt 41);

— identifier l'abonné ne signifie pas encore identifier l'utilisateur effectif du service, en particulier pour les méthodes indirectes (point 42).

Concernant le premier point, la Cour constitutionnelle, dans son arrêt n° 158/2021 du 18 novembre 2021 rendu dans le cadre du recours en annulation de la loi "cartes prépayées" a indiqué ce qui suit:

"B. 16.11.2 De même, l'existence d'autres techniques de communication n'empêche pas le législateur de supprimer l'anonymat des cartes de téléphonie mobile prépayées s'il constate notamment que ces cartes de téléphonie mobile sont utilisées dans des milieux terroristes et criminels et que cet anonymat constitue un problème insurmontable pour les autorités judiciaires et pour les services de renseignement et de sécurité. Au demeurant, si la disposition attaquée a pour effet que les organisations terroristes et criminelles passent à des techniques plus avancées, cela démontre plutôt la pertinence de la mesure attaquée. Il appartient alors au législateur de réguler également l'utilisation de ces techniques, en vue de réaliser les mêmes objectifs."

Pour les autorités, imposer une obligation d'identification est nettement préférable à l'absence d'une telle obligation:

— pour ces autorités, il est préférable d'avoir des traces fiables pour retrouver l'abonné et ensuite, sur base d'une enquête, l'utilisateur effectif du service que de n'avoir aucune information; lorsque les autorités judiciaires et les services de renseignement et de sécurité ne disposent pas de données d'identification de l'abonné, elles n'auront pas d'autres choix que de mettre en œuvre des mesures plus attentatoires à la vie privée (ex. intrusion dans le domicile, saisie de matériel informatique, écoute téléphonique, etc.);

— le fait que les criminels soient amenés à chercher des canaux de communications alternatifs leur complique la tâche et les amène à faire des erreurs.

Il n'existe malheureusement aucune loi qui ne soit incontournable. Ceci est une réalité, quelle que soit la loi concernée. Si l'avis de l'Autorité de protection des données était suivi, aucune loi permettant à la police de faire son travail ne serait adoptée, au motif qu'il existe des moyens d'y échapper.

Données d'identification et copies de documents conservées par l'opérateur pour ses propres besoins

— de identificatie van de abonnee van een elektronischecommunicatiedienst [identificeert] niet noodzakelijkerwijs de daadwerkelijke gebruiker van die dienst (punt 42).

Wat het eerste punt betreft, vermeldt het Grondwettelijk Hof in zijn arrest nr. 158/2021 van 18 november 2022, gewezen in het kader van het beroep tot vernietiging van de wet "voorafbetaalde kaarten", het volgende:

"B. 16.11.2 [...] Ook het bestaan van andere communicatietechnieken verhindert de wetgever niet om de anonimiteit van de vooraf betaalde belkaarten af te schaffen indien hij vaststelt dat met name die belkaarten worden gebruikt in terroristische en criminele milieus en dat die anonimiteit een onoverkomelijk probleem vormt voor de gerechtelijke overheden en voor de inlichtingen- en veiligheidsdiensten. Indien de bestreden bepaling als gevolg heeft dat terroristische en criminele organisaties overstappen naar meer geavanceerde technieken, toont dat overigens veeleer de pertinentie van de bestreden maatregel aan. Het staat dan aan de wetgever om met het oog op dezelfde doelstellingen ook het gebruik van die technieken te reguleren."

Voor de autoriteiten is het opleggen van een identificatieplicht duidelijk te verkiezen boven het ontbreken van een soortgelijke plicht:

— voor deze autoriteiten is het beter om betrouwbare sporen te hebben om de abonnee en vervolgens, via een onderzoek, de daadwerkelijke gebruiker van de dienst terug te kunnen vinden dan helemaal geen gegevens te hebben; wanneer de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten niet over identificatiegegevens van de abonnee beschikken, hebben ze geen andere keuze dan maatregelen te gebruiken die een veel grotere inbreuk maken op de persoonlijke levenssfeer (bijvoorbeeld binnentreden in de woning, inbeslagneming van informaticamateriaal, telefoontap, enz.);

— het gegeven dat de criminelen alternatieve communicatiekanalen moeten zoeken, bemoeilijkt de taak van de autoriteiten, waardoor ze fouten kunnen maken.

Jammer genoeg is er geen enkele wet die niet kan worden omzeild. Dat is een realiteit voor eender welke wet. Als het advies van de Gegevensbeschermingsautoriteit zou worden gevolgd, zou geen enkele wet die de politie in staat stelt haar werk te doen worden aangenomen, om de reden dat het mogelijk is eraan te ontsnappen.

Identificatiegegevens en kopieën van documenten bewaard door de operator voor zijn eigen behoeften

L'article 127 de la loi télécom oblige les opérateurs à identifier leurs abonnés pour les besoins des autorités ou à permettre à ces autorités de pouvoir les identifier. Cependant, l'opérateur peut aussi avoir un intérêt légitime à connaître l'identité correcte de son abonné, entre autres lorsque ce dernier ne remplit pas ses obligations et qu'une procédure en justice en recouvrement de créance est nécessaire.

Par conséquent, la présente loi est sans préjudice des données et documents relatifs à l'abonné que l'opérateur peut conserver pour ses propres besoins conformément au RGPD.

Structure de la nouvelle version de l'article 127

Le paragraphe 1er de l'article 127 est un paragraphe général et décrit son champ d'application (entre autres les opérateurs et services de communications électroniques auxquels il s'applique). Les paragraphes 2 à 9 sont relatifs à l'identification par un opérateur de l'abonné (la personne qui conclut le contrat avec l'opérateur). Le paragraphe 10 est consacré à l'identification de l'utilisateur habituel du service. Le paragraphe 11 est un paragraphe général et décrit les sanctions applicables lorsque les opérateurs ou les abonnés ne respectent pas les obligations qui leur incombent.

Paragraphe 1er: champ d'application

L'article 127 s'applique aux opérateurs qui fournissent en Belgique aux utilisateurs finaux un service de communications électroniques, même si l'opérateur n'y dispose pas d'un réseau.

Un utilisateur final peut être une personne physique ou une personne morale (par exemple une entreprise) mais pas un opérateur. En effet, l'article 2, 13°, de la loi télécom définit un "utilisateur final" comme "un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public" et une personne qui fournit un tel réseau ou un tel service est un opérateur (cf. article 2, 11°, de la loi télécom).

Dans le cadre de la consultation publique sur le présent amendement, certains opérateurs qui offrent des services de communications électroniques aux entreprises ont demandé s'ils étaient dans le champ d'application de l'article 127 de la loi télécom. La réponse à cette question est positive vu la formulation du paragraphe 1er, alinéa 1er, de cet article (la notion d'abonné vise aussi les personnes morales). Cependant, les exigences pour ces opérateurs sont très limitées puisqu'il leur suffit d'identifier leur client selon la méthode de leur choix,

Artikel 127 van de telecomwet verplicht de operatoren om hun abonnees te identificeren voor de behoeften van de autoriteiten of om het voor deze autoriteiten mogelijk te maken om ze te identificeren. De operator kan echter ook een gewettigd belang hebben om de juiste identiteit van zijn abonnee te kennen, onder andere wanneer deze laatste zijn verplichtingen niet nakomt en een gerechtelijke procedure voor de inning van een schuldvordering noodzakelijk is.

Bijgevolg doet deze wet geen afbreuk aan de gegevens en documenten met betrekking tot de abonnee die de operator mag bewaren voor zijn eigen behoeften overeenkomstig de AVG.

Structuur van de nieuwe versie van artikel 127

Paragraaf 1 van artikel 127 is een algemene paragraaf en beschrijft het toepassingsgebied ervan (onder andere de operatoren en elektronische-communicatiediensten waarop het van toepassing is). De paragrafen 2 tot 9 hebben betrekking op de identificatie door een operator van de abonnee (de persoon die het contract met de operator sluit). Paragraaf 10 is gewijd aan de identificatie van de effectieve gebruiker van de dienst. Paragraaf 11 is een algemene paragraaf en beschrijft de toepasselijke sancties wanneer de operatoren of de abonnees hun verplichtingen niet nakomen.

Paragraaf 1: toepassingsgebied

Artikel 127 is van toepassing op de operatoren die in België een elektronische-communicatiedienst aanbieden aan de eindgebruikers, ook wanneer de operator er niet over een netwerk beschikt.

Een eindgebruiker kan een natuurlijke persoon of een rechtspersoon (bijvoorbeeld een onderneming) zijn maar geen operator. Artikel 2, 13°, van de telecomwet definieert een "eindgebruiker" immers als "een gebruiker die geen openbaar elektronische-communicatienetwerk of voor het publiek beschikbare elektronische-communicatiediensten aanbiedt" en een persoon die zo'n netwerk of zo'n dienst aanbiedt is een operator (zie artikel 2, 11°, van de telecomwet).

In het kader van de openbare raadpleging over dit amendement hebben een aantal operatoren die elektronische-communicatiediensten aanbieden aan ondernemingen gevraagd of ze binnen het toepassingsgebied vielen van artikel 127 van de telecomwet. Het antwoord op die vraag is positief gelet op de formulering van paragraaf 1, eerste lid, van dat artikel (het begrip abonnee slaat ook op rechtspersonen). De vereisten voor die operatoren zijn evenwel zeer beperkt, aangezien het voor hen volstaat om hun klanten te identificeren volgens

sauf s'ils leur offrent un service de communications électroniques mobiles fourni sur base d'une carte prépayée. Dans ce dernier cas, ils devront identifier une personne physique qui agit pour le compte de la personne morale comme prévu au paragraphe 7 de l'article 127.

Le type de service de communications électroniques fourni en Belgique importe peu. Ainsi, les services de communications interpersonnelles qui ne sont pas fondés sur la numérotation ("OTT" ou fournisseurs "*Over The Top*") sont inclus, vu l'utilisation croissante de ce type de service dans les milieux criminels. Sont également inclus les services de communications électroniques qui sont offerts pour permettre des applications "M2M ".

La notion d'abonné (ou le client de l'opérateur) doit s'entendre au sens large et couvre également les personnes qui souscrivent aux services de l'opérateur à l'aide d'une carte prépayée ou qui souscrivent à un service d'un opérateur qui fournit des services de communications interpersonnelles non fondés sur la numérotation.

L'interdiction visée à l'aliéna 2 s'explique par le fait que dans le passé des organisations ont distribué en Belgique des cartes prépayées d'opérateurs étrangers, sans que ces opérateurs étrangers ne soient nécessairement informés de ce fait, sans qu'ils ne soient notifiés à l'IBPT comme opérateur et sans aucune forme d'identification des utilisateurs finaux. Cette pratique ne peut pas être admise car elle revient à mettre à néant la volonté du gouvernement et du législateur de mettre fin à l'anonymat pour les cartes prépayées.

La nécessité d'une identification de l'abonné en cas de cartes prépayées d'opérateurs étrangers distribuées en Belgique se retrouve également dans l'article 1er, alinéa 2, de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée (ci-après l'AR "cartes prépayées"), qui prévoit qu'il "s'applique […] aux cartes prépayées des entreprises étrangères qui sont vendues en Belgique."

L'alinéa 2 vise les cartes prépayées (soit le fait de payer avant la fourniture du service de communications électroniques) et les abonnements (le service est offert sans paiement ou le paiement est effectué après la fourniture du service).

L'alinéa 2 vise les objets connectés offerts en Belgique qui permettent d'utiliser un service d'accès à internet ou un service de communications interpersonnelles d'un opérateur

de methode van hun keuze, behalve wanneer zij hun een mobiele elektronische-communicatiedienst aanbieden die verschaft wordt via een voorafbetaalde kaart. In dat laatste geval moeten zij een natuurlijke persoon identificeren die handelt voor rekening van de rechtspersoon, zoals bepaald in paragraaf 7 van artikel 127.

Het soort elektronische-communicatiedienst die in België aangeboden wordt doet er weinig toe. Zo worden nummeronafhankelijke interpersoonlijke communicatiediensten ("OTT's" of "*Over The Top*"-aanbieders) meegerekend, gelet op het toenemende gebruik van dergelijke diensten in criminele kringen. Worden ook meegeteld: elektronische-communicatiediensten die aangeboden worden om "M2M"-toepassingen mogelijk te maken.

Het begrip van abonnee (of de klant van de operator) moet worden verstaan in de ruime zin en dekt ook de personen die intekenen op de diensten van de operator met behulp van een vooraf betaalde kaart of die intekenen op een dienst van een operator die nummeronafhankelijke interpersoonlijke communicatiediensten aanbiedt.

Het in het tweede lid bedoelde verbod wordt verklaard door het feit dat organisaties vroeger in België prepaid kaarten van buitenlandse operatoren hebben verdeeld, zonder dat die buitenlandse operatoren daar per se van op de hoogte waren, zonder dat ze aan het BIPT als operator werd gemeld en zonder enige vorm van identificatie van de eindgebruikers. Deze praktijk kan niet worden toegestaan omdat die de wil van de regering en van de wetgever om een eind te maken aan de anonimiteit van prepaid kaarten eigenlijk tenietdoet.

De noodzaak om de abonnee te identificeren in geval van in België verdeelde prepaid kaarten van buitenlandse operatoren is ook te vinden in artikel 1, tweede lid, van het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart (hierna het KB "prepaid kaarten"), dat bepaalt dat het "van toepassing [is] […] op de voorafbetaalde van de buitenlandse operatoren die worden verkocht in België."

Het tweede lid beoogt de prepaid kaarten (namelijk het feit van te betalen voordat de elektronische-communicatiedienst wordt verstrekt) en de abonnementen (de dienst wordt verstrekt zonder betaling of de betaling wordt verricht na de verstrekking van de dienst).

Het tweede lid beoogt de in België aangeboden geconnecteerde objecten waarmee een internettoegangsdienst of een interpersoonlijke communicatiedienst van een operator

(ex. service de téléphonie, service de courrier électronique, service de messagerie instantanée comme WhatsApp, Messenger, Signal), étant donné que ces objets remplissent la même fonction qu'un téléphone intelligent. Ne sont visés que les objets qui permettent effectivement un accès à Internet ou d'utiliser un service de communications interpersonnelles d'un opérateur. Cela n'est pas le cas pour un objet vendu sans la carte SIM, vu que cette carte est nécessaire pour l'utilisation effective de ces services. Si ce paragraphe n'incluait pas ces objets connectés, l'objectif de la législation pourrait être facilement contourné. En effet, une personne pourrait se faire livrer en Belgique un objet (par exemple une voiture) qui lui permet d'accéder à Internet ou d'utiliser un service de communications interpersonnelles d'un opérateur, sans devoir s'identifier auprès d'un opérateur. Il doit s'agir d'un service de communications interpersonnelles d'un opérateur. Il convient à cet égard de rappeler que la définition de "service de communications interpersonnelles", à l'article 2, 5/2°, de la loi télécom exclut les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service (par exemple la possibilité d'échanger des messages entre joueurs d'un jeu vidéo).

L'interdiction visée au paragraphe 1er s'applique également lorsqu'il est possible de se faire livrer en Belgique, à l'aide d'une commande par Internet, des cartes prépayées ou un abonnement d'un opérateur étranger (par exemple par l'envoi d'une carte SIM) ou un objet connecté qui permet d'utiliser un service d'accès à internet ou un service de communications interpersonnelles d'un opérateur.

L'interdiction visée au paragraphe 1er est applicable que la distribution de ces cartes prépayées, abonnements ou objets connectés se fassent contre paiement ou qu'ils soient offerts gratuitement.

Pour éviter que des cartes prépayées, des abonnements ou des objets connectés ne soient distribués en Belgique à l'insu de l'opérateur étranger, l'article 127 prévoit qu'ils ne peuvent être distribués en Belgique qu'avec l'accord de l'opérateur.

En cas d'accord, l'opérateur étranger sera considéré comme un opérateur au sens de l'article 2, 11°, de la loi télécom (et deviendra donc aussi un opérateur belge) et devra le cas échéant se notifier auprès de l'IBPT conformément à l'article 9, § 1er, de la loi télécom. En effet, cette notification à l'IBPT est obligatoire sauf si l'opérateur offre un service de communications interpersonnelles non fondé sur la numérotation (voir article 9, § 1er, de la loi télécom). En donnant cet

gebruikt kan worden (bijv. telefoniedienst , e-maildienst, instant-messagingdienst zoals WhatsApp, Messenger, Signal), aangezien die voorwerpen dezelfde functie als een smartphone vervullen. Enkel voorwerpen die daadwerkelijk een toegang tot het internet of het gebruik van een interpersoonlijke communicatiedienst van een operator mogelijk maken, worden beoogd. Dat is niet het geval bij een voorwerp dat zonder simkaart verkocht wordt, aangezien die kaart noodzakelijk is voor het daadwerkelijke gebruik van deze diensten. Als die paragraaf zulke geconnecteerde voorwerpen niet zou omvatten, zou het doel van de wetgeving makkelijk omzeild kunnen worden. Een persoon zou immers een voorwerp (zoals een auto) kunnen laten leveren waarmee hij toegang heeft tot het internet of zou gebruik kunnen maken van een interpersoonlijke communicatiedienst van een operator, zonder zich eerst bij een operator te moeten identificeren. Het moet gaan om een interpersoonlijke communicatiedienst van een operator. Daarbij dient eraan herinnerd te worden dat de definitie van "interpersoonlijke communicatiedienst", in artikel 2, 5/2°, van de telecomwet de diensten uitsluit die een interpersoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst (bijvoorbeeld de mogelijkheid om berichten uit te wisselen tussen spelers van een videospel).

Het in paragraaf 1 bedoelde verbod geldt ook wanneer het mogelijk is om via een internetbestelling prepaid kaarten of een abonnement van een buitenlandse operator in België te laten leveren (bijvoorbeeld door het verzenden van een simkaart) ofwel een geconnecteerd voorwerp waarmee een internettoegangsdienst of een interpersoonlijke communicatiedienst van een operator kunnen worden gebruikt.

Het in paragraaf 1 bedoelde verbod geldt ongeacht of die prepaid kaarten, abonnementen of geconnecteerde voorwerpen worden verdeeld tegen betaling of gratis worden aangeboden.

Om te vermijden dat prepaid kaarten, abonnementen of geconnecteerde voorwerpen in België worden verdeeld zonder medeweten van de buitenlandse operator, bepaalt artikel 127 dat ze in België maar mogen worden verdeeld met het akkoord van de operator.

In geval van een akkoord zal de buitenlandse operator worden beschouwd als een operator in de zin van artikel 2, 11°, van de telecomwet (en zal die aldus een Belgische operator worden) en zal hij in voorkomend geval een kennisgeving moeten doen aan het BIPT, overeenkomstig artikel 9, § 1, van de telecomwet. De kennisgeving aan het BIPT is immers verplicht, behalve wanneer de operator een nummeronafhankelijke interpersoonlijke communicatiedienst aanbiedt

accord, l'opérateur dirige la fourniture de ses services vers la Belgique, de sorte que l'article 127, § 1er, alinéa 1er trouve à s'appliquer. L'opérateur sera dans une situation similaire à un MVNO ("*Mobile Virtual Network Operator*"). En effet, il offrira en Belgique des services de communications électroniques sans y disposer d'un réseau. D'un point de vue pratique, il est également important que l'opérateur étranger soit considéré comme un opérateur belge, de manière à ce que l'article 127 de la loi télécom mais aussi par exemple l'article 127/3 (Cellule de coordination) de la même loi lui soient applicables.

S'il apparaît qu'il n'y a pas d'accord de l'opérateur étranger, des poursuites pénales pourront être engagées à l'encontre de la personne qui distribue en Belgique les cartes prépayées, les abonnements ou les objets connectés (le non-respect de l'article 127 est puni par des amendes pénales visées à l'article 145 de la loi télécom). Si l'opérateur étranger n'a pas donné son accord, il ne sera pas considéré comme un opérateur au sens de la loi télécom car on ne peut pas considérer qu'il fournit ses services en Belgique.

Par contre, l'opérateur belge ne devra pas obtenir l'identité civile de l'abonné d'un opérateur étranger qui utilise en Belgique le réseau de l'opérateur belge en exécution d'un accord de roaming entre l'opérateur belge et l'opérateur étranger, lorsque la souscription au service a été faite à l'étranger (ex. touristes utilisant en Belgique la carte SIM de leur pays d'origine).

Il n'est plus nécessaire de faire référence à la notion de fournisseur, étant donné que la notion d'opérateur a été élargie dans le cadre de la transposition du Code des communications électroniques européen dans la loi télécom.

Paragraphe 2: méthode d'identification directe ou indirecte

Définitions

Le paragraphe 2, 1°, fait référence à un service de communications électroniques offert sans surcoût conjointement à un service payant. Il s'agit, par exemple, de la situation dans laquelle un opérateur offre sans surcoût à ses abonnés qui souscrivent un contrat d'accès à internet la possibilité de profiter du Wi-Fi de l'ensemble de ses abonnés.

Un service qui est temporairement gratuit mais qui devient payant à partir d'un moment donné doit être considéré comme un service payant. On peut penser, à titre d'exemple, à un

(zie artikel 9, § 1, van de telecomwet). Door dat akkoord te verlenen, verlegt de operator zijn dienstverlening naar België, waardoor artikel 127, § 1, eerste lid, van toepassing is. De operator zal immers in een soortgelijke situatie bevinden als een MVNO ("*Mobile Virtual Network Operator*"). Hij zal in België immers elektronische-communicatiediensten aanbieden zonder daar over een netwerk te beschikken. Vanuit een praktisch oogpunt is het ook belangrijk dat de buitenlandse operator als een Belgische operator wordt beschouwd, zodat artikel 127 van de telecomwet, maar ook bijvoorbeeld artikel 127/3 (Coördinatiecel) van dezelfde wet op hem van toepassing zijn.

Indien blijkt dat er geen akkoord van de buitenlandse operator is, dan zal tot strafvervolging kunnen worden overgegaan tegen de persoon die in België prepaid kaarten, abonnementen of geconnecteerde voorwerpen verdeelt (de niet-nakoming van artikel 127 wordt bestraft met straffen in de vorm van een geldboete, bedoeld in artikel 145 van de telecomwet). Als de buitenlandse operator geen akkoord heeft verleend, zal hij niet worden beschouwd als een operator in de zin van de telecomwet omdat hij niet kan worden beschouwd als een operator die zijn diensten aanbiedt in België.

De Belgische operator zal daarentegen de burgerlijke identiteit van de abonnee van een buitenlandse operator die in België het netwerk van de Belgische operator gebruikt ter uitvoering van een roamingakkoord tussen de Belgische en de buitenlandse operator, niet moeten verkrijgen, wanneer de intekening op de dienst in het buitenland heeft plaatsgehad (bijv. toeristen die in België de simkaart van hun thuisland gebruiken).

Het is niet langer noodzakelijk om te verwijzen naar het begrip van aanbieder aangezien het begrip van operator werd uitgebreid in het kader van de omzetting van het Europees wetboek voor elektronische communicatie in de telecomwet.

Paragraaf 2: directe of indirecte identificatiemethode

Definities

Paragraaf 2, 1°, verwijst naar een elektronische-communicatiediensten die zonder toeslag samen met een betaaldienst wordt aangeboden. Het gaat bijvoorbeeld om de situatie waarin een operator aan zijn abonnees die intekenen op een contract voor internettoegang, zonder toeslag de mogelijkheid aanbiedt om gebruik te maken van de wifi van al zijn abonnees.

Een dienst die tijdelijk gratis is maar waarvoor vanaf een bepaald moment betaald moet worden, moet als een betaaldienst worden beschouwd. Daarbij denken we bijvoorbeeld

service qui est offert à titre gratuit pendant un certain temps, mais, pour lequel l'opérateur envoie une facture à l'abonné par la suite. Un autre exemple est une carte prépayée avec un certain crédit que l'opérateur offre gratuitement à l'abonné, qui devra cependant payer pour la recharge de cette carte une fois que le crédit offert est épuisé.

Une méthode d'identification directe est par exemple une identification de l'abonné dans un point de vente, via itsme, une identification par laquelle l'opérateur reçoit les données d'identité civile d'une banque ou encore une identification par extension de produit (une personne a déjà été identifiée pour un produit et souhaite souscrire à un autre produit).

Le paragraphe 2, 3°, de l'article 127 vise l'identité civile d'une personne physique qui est l'abonné de l'opérateur pour la raison suivante. Un des arguments des parties requérantes dans le cadre du recours devant la Cour constitutionnelle contre la loi du 1er septembre 2016 est que "la disposition attaquée ne précise pas ce qu'il faut entendre par "données et documents d'identification. Ainsi, l'on n'aperçoit pas clairement s'il peut s'agir de données se rapportant à l'identité physique, physiologique, psychique, économique, culturelle ou sociale de l'utilisateur final." (point A.3.5.2. de l'arrêt). Il est cependant clair que l'article 127 de la loi télécom a toujours porté sur l'identification de l'abonné (déterminer qui est l'abonné), ce qui se traduit par l'identité civile lorsque l'abonné est une personne physique. Le terme "identité civile" n'est cependant pas adapté lorsque l'abonné est une personne morale (dans ce cas, l'opérateur identifie l'abonné qui est une personne morale).

Dans le cadre d'une méthode d'identification directe, l'opérateur peut identifier l'abonné à l'aide d'un document d'identification ou sans un tel document.

La personne doit être identifiée (ou doit pouvoir être identifiée par les autorités) dès le début du contrat, et non pas par exemple lors du paiement de la première facture un mois après la fourniture du service (facture qu'un fraudeur ne paiera pas).

Une méthode d'identification reste indirecte même si l'opérateur collecte des données relatives à l'identité civile de l'abonné, lorsque la fiabilité de ces données n'est pas assurée. Ainsi, par exemple, la méthode d'identification par conservation de la référence de paiement en ligne est une méthode d'identification indirecte, même si l'abonné doit communiquer à l'opérateur son nom et son prénom dans le cadre de cette méthode.

aan een dienst die gratis aangeboden wordt gedurende een zekere periode, maar waarvoor de operator nadien een rekening stuurt naar de abonnee. Een ander voorbeeld is een prepaid kaart met daarop een bepaald beltegoed die door de operator gratis wordt aangeboden aan de abonnee, maar waarbij die laatste nadat het beltegoed is opgebruikt, zal moeten betalen om die kaart te herladen.

Een directe identificatiemethode is bijvoorbeeld een identificatie van de abonnee in een verkooppunt, via itsme, een identificatie waarbij de operator de gegevens van burgerlijke identiteit van een bank ontvangt of ook een identificatie via productuitbreiding (een persoon is al eens geïdentificeerd voor een product en wenst in te tekenen op een ander product).

Paragraaf 2, 3°, van artikel 127 beoogt de burgerlijke identiteit van een natuurlijke persoon die abonnee van de operator is om de volgende reden. Een van de argumenten van de eisende partijen in het beroep voor het Grondwettelijk Hof tegen de wet van 1 september 2016 is dat "de bestreden bepaling niet verduidelijkt wat onder "identificatiegegevens en –documenten" dient te worden verstaan. Zo is niet duidelijk of het kan gaan om gegevens die betrekking hebben op de fysieke, fysiologische, psychische, economische, culturele of sociale identiteit van de eindgebruiker" (punt A.3.5.2. van het arrest). Het is evenwel duidelijk dat artikel 127 van de telecomwet altijd betrekking heeft gehad op de identificatie van de abonnee (bepalen wie de abonnee is), hetgeen vertaald wordt in de burgerlijke identiteit wanneer de abonnee een natuurlijke persoon is. De term "burgerlijke identiteit" wordt echter niet aangepast wanneer de persoon een rechtspersoon is (in dat geval identificeert de operator de abonnee die een rechtspersoon is).

In het kader van een directe identificatiemethode kan de operator de abonnee identificeren aan de hand van een identificatiedocument of zonder een soortgelijk document.

De persoon moet worden geïdentificeerd (of moet kunnen worden geïdentificeerd door de autoriteit) bij het begin van de overeenkomst en niet bijvoorbeeld bij de betaling van de eerste factuur, een maand na de levering van de dienst (factuur die een fraudeur niet zal betalen).

Een identificatiemethode blijft indirect zelfs wanneer de operator gegevens in verband met de burgerlijk identiteit van de abonnee verzamelt, wanneer de betrouwbaarheid van deze gegevens niet gegarandeerd wordt. Zo is bijvoorbeeld de identificatiemethode via bewaring van de referentie van de onlinebetaling een indirecte identificatiemethode, zelfs wanneer de abonnee in het kader van die methode naam en voornaam moet meedelen aan de operator.

Méthode d'identification directe vs méthode d'identification indirecte

L'ancien article 127, § 2, contenait une interdiction pour les opérateurs de rendre difficile ou impossible l'identification des utilisateurs finaux. Le nouvel article 127 comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés (méthode d'identification directe) ou à tout le moins de rendre cette identification possible (méthode d'identification indirecte).

Les principes applicables sont les suivants.

Les opérateurs qui offrent des services de communications électroniques payants peuvent identifier leurs abonnés par une méthode d'identification directe.

Ils peuvent aussi les identifier à l'aide d'une méthode d'identification indirecte à l'exception des méthodes d'identification indirecte visées au paragraphe 9, alinéa 1° (adresse IP) et 2° (numéro de téléphone).

Il existe une exception à cette exception: pour certains services (les hotspot wifi des opérateurs), une identification directe est difficile à mettre en œuvre de sorte que l'opérateur peut recourir à la méthode d'identification indirecte visée au paragraphe 9, alinéa 2° (numéro de téléphone).

Généralement, une personne physique utilisera ce type de service de manière occasionnelle en dehors de sa résidence principale ou secondaire et du lieu où elle exerce une activité professionnelle. Soumettre ce type de service à une méthode directe d'identification créerait une barrière pour l'accès à ce type de service.

Les opérateurs qui offrent des services de communications électroniques gratuits devront permettre aux autorités d'identifier leurs abonnés à l'aide d'une méthode d'identification indirecte. En d'autres termes, ils ne peuvent pas l'identifier via une méthode d'identification directe.

Le raisonnement qui justifie une telle distinction est le suivant.

Lorsque l'abonné souscrit à un service payant qui est facturé après la fourniture du service ("*postpaid*"), l'opérateur disposera généralement des données d'identité civile de l'abonné afin de pouvoir correspondre avec ce dernier (et entre autres lui envoyer les factures), afin d'installer des services fixes à son domicile (par exemple la télévision, l'internet ou la téléphonie) et afin de mener à bien une action en justice

Directe identificatiemethode vs. indirecte identificatiemethode

Het oude artikel 127, § 2, bevatte een verbod voor de operatoren om de identificatie van de eindgebruikers te bemoeilijken of onmogelijk te maken. Het nieuwe artikel 127 bevat nu een positieve verplichting voor de operatoren om hun abonnees te identificeren (directe identificatiemethode) of op zijn minst deze identificatie mogelijk te maken (indirecte identificatiemethode).

De toepasselijke principes zijn de volgende.

De operatoren die elektronische-communicatiebetaaldiensten aanbieden, kunnen hun abonnees identificeren via een directe identificatiemethode.

Ze kunnen ze ook identificeren aan de hand van een indirecte identificatiemethode, met uitzondering van de indirecte identificatiemethoden bedoeld in paragraaf 9, eerste en tweede lid (respectievelijk IP-adres en telefoonnummer).

Er is een uitzondering op die uitzondering: voor bepaalde diensten (wifi-hotspots van de operatoren) waar een directe identificatie moeilijk te realiseren is, waardoor de operator wel mag gebruikmaken van de indirecte identificatiemethode bedoeld in paragraaf 9, tweede lid (telefoonnummer).

Gewoonlijk zal een natuurlijke persoon occasioneel van dergelijke diensten gebruikmaken buiten zijn hoofdverblijf of tweede verblijf en buiten de plaats waar hij zijn beroepsactiviteit uitoefent. Zo'n dienst aan een directe identificatiemethode onderwerpen zou een obstakel opwerpen om toegang te krijgen tot zo'n soort van dienst.

De operatoren die gratis elektronische-communicatiediensten aanbieden, zullen de autoriteiten de mogelijkheid moeten bieden om hun abonnees te identificeren aan de hand van een indirecte identificatiemethode. Zij mogen ze met andere woorden niet identificeren aan de hand van een directe identificatiemethode.

De redenering die dat onderscheid rechtvaardigt, is als volgt.

Wanneer de abonnee intekent op een betaaldienst die aangerekend wordt na de levering van de dienst ("postpaid"), zal de operator doorgaans beschikken over de gegevens van burgerlijke identiteit van de abonnee om met die laatste te kunnen corresponderen (en onder andere facturen toesturen), om bij de persoon thuis vaste diensten te installeren (zoals televisie, internet of telefonie) en om een rechtszaak tegen

contre son abonné (par exemple dans le cadre d'un recouvrement de créances). Il faut aussi rappeler que les opérateurs qui offrent des services de communications électroniques qui doivent permettre à l'utilisateur final d'accéder aux services d'urgence qui offrent de l'aide sur place (généralement des services de communications électroniques payants) doivent pouvoir leur envoyer, lors de l'appel d'urgence, le nom et le prénom de l'appelant, en vertu de l'article 107, § 4, alinéa 1er, de la loi télécom. Pour ce qui concerne les services payants, le législateur ne souhaite pas une diminution de la fiabilité actuelle de l'identification par les opérateurs de leurs abonnés. Il convient d'éviter une trop grande application d'une méthode d'identification indirecte, étant donné que ce type de méthode rend la tâche plus difficile pour les autorités.

Les opérateurs qui offrent des services gratuits sont généralement des opérateurs qui offrent des services de communications interpersonnelles qui ne sont pas basés sur la numérotation (les "OTT"). Ils ne disposent généralement pas des données d'identité civile de leurs abonnés (ou en tous cas pas de données dont la fiabilité a été vérifiée) ni de copie de leurs documents d'identification, vu que cela n'est pas nécessaire pour qu'ils offrent leurs services. Le chiffre d'affaires effectué par ce type d'opérateur provient généralement du traitement des données de l'abonné et de l'envoi de publicités à ce dernier. Le gouvernement souhaite éviter que les opérateurs dont le modèle commercial est basé sur le traitement des données de l'abonné mettent en place une méthode d'identification directe, étant donné que cela impliquerait qu'ils pourraient relier les (parfois nombreuses) données qu'ils détiennent déjà sur l'abonné avec l'identité de ce dernier, ce qui rendrait le traitement de ses données plus sensible. L'identification indirecte est plus appropriée pour les services gratuits, étant donné que cette méthode d'identification avantage que l'opérateur ne connaît pas lui-même l'identité de son abonné lorsqu'il n'est pas nécessaire qu'il la connaisse.

Dans son avis sur les amendements (note de bas de page n° 31), l'Autorité de protection des données "note toutefois que certains opérateurs offrent un service de communications électroniques, comme Signal ou Tor, sans collecter des données de ses abonnés et n'ont pas de but de lucre (ils ne gagnent pas d'argent en envoyant des publicités à leurs abonnés)." De l'avis du gouvernement, Tor n'offre pas un service de communications électroniques accessible au public et n'est donc pas un opérateur. Il ne doit donc pas respecter l'article 127 de la loi télécom (au contraire d'un opérateur comme Signal). Les arguments avancés par l'Autorité de protection des données renforcent le raisonnement derrière la règle applicable aux services de communications

zijn abonnee tot een goed einde te brengen (bijvoorbeeld in het kader van een invordering van schulden). Ook dient eraan te worden herinnerd dat de operatoren die elektronische-communicatiediensten aanbieden die voor de abonnee de toegang mogelijk moeten maken tot de nooddiensten die ter plaatse hulp bieden (doorgaans elektronische-communicatiebetaaldiensten), in geval van een noodoproep, aan die nooddiensten de naam en de voornaam van de beller moeten kunnen sturen, krachtens artikel 107, § 4, eerste lid, van de telecomwet. Wat de betaaldiensten betreft, wenst de wetgever niet dat de huidige betrouwbaarheid van de identificatie van de abonnees door de operatoren vermindert. Er moet vermeden worden dat een indirecte identificatiemethodes te vaak wordt toegepast, aangezien zo'n methode de taak voor de autoriteiten moeilijker maakt.

De operatoren die gratis diensten aanbieden zijn over het algemeen operatoren die interpersoonlijke communicatiediensten aanbieden die nummeronafhankelijk zijn (de "OTT's"). Zij beschikken doorgaans niet over de gegevens van burgerlijke identiteit van hun abonnees (of toch niet over gegevens waarvan de betrouwbaarheid geverifieerd is) noch over een kopie van hun identificatiedocumenten, aangezien dat niet noodzakelijk is om hun diensten te kunnen aanbieden. De omzet die zulke operatoren boeken, komt over het algemeen van de verwerking van de gegevens van de abonnee en het verzenden van reclame naar die laatste. De regering wenst te vermijden dat de operatoren van wie het commerciële model gebaseerd is op de verwerking van de abonneegegevens, een directe identificatiemethode instellen, aangezien dat zou betekenen dat ze de (soms talrijke) gegevens die ze al over de abonnee in handen hebben, zouden kunnen in verband brengen met de identiteit van die abonnee, waardoor de verwerking van zijn gegevens gevoeliger zou worden. De indirecte identificatie is het meest geschikt voor de gratis diensten, aangezien deze identificatiemethode als voordeel heeft dat de operator zelf de identiteit van zijn abonnee niet kent wanneer het niet nodig is dat hij die kent.

De Gegevensbeschermingsautoriteit wijst er in haar advies over de amendementen (voetnoot nr. 31) "[...] echter op dat sommige operatoren een elektronische-communicatiedienst, zoals Signal of Tor, aanbieden zonder gegevens van hun abonnees te verzamelen en dat zij geen winstoogmerk hebben (zij verdienen geen geld met het zenden van advertenties aan hun abonnees)". Volgens de regering biedt Tor geen elektronische-communicatiedienst aan die toegankelijk is voor het publiek en is Tor dus geen operator. Tor moet artikel 127 van de telecomwet dus niet naleven (in tegenstelling tot een operator als Signal). De argumenten die de Gegevensbeschermingsautoriteit aanvoert, versterken de redenering achter de regel die geldt voor de gratis

électroniques gratuits. En effet, si certains OTT ne souhaitent pas traiter les données de l'abonné afin de faire du profit, dans le but de protéger sa vie privée, il est préférable de les obliger à mettre en œuvre une méthode d'identification indirecte plutôt qu'une méthode d'identification directe, étant donné que le premier type de méthode d'identification est moins intrusive dans la vie privé des abonnés.

Alors que les opérateurs qui offrent des services payants ont généralement leur établissement principal en Belgique, les opérateurs qui offrent des services gratuits ont généralement leur établissement principal en dehors de l'Union européenne.

Paragraphe 3: conservation des données d'identification et de copies de documents d'identité par l'opérateur et durée de la conservation

L'alinéa 1er reprend une disposition de l'actuel article 127, § 1er et la renforce. En effet, les points de vente des opérateurs sont le "maillon faible" au niveau de l'identification de l'abonné. Il ressort des procédures d'infraction, que l'IBPT a menées contre certains opérateurs par le passé, que les infractions à la réglementation sont généralement commises à la suite d'identifications incorrectes effectuées par les points de vente, qui n'appliquent pas toujours les processus mis en place par l'opérateur.

L'interdiction pour le point de vente de conserver des données d'identification ou des copies de documents d'identification (une telle copie étant obligatoire pour les autres documents que l'eID en vertu de l'article 127, § 5, de la loi télécom) signifie que le point de vente ne peut pas conserver de données ou de telles copies en dehors des systèmes informatiques de l'opérateur.

Au point 46 de son avis sur l'amendement, l'Autorité de protection des données indique que "Le nouvel article 127 § 3, alinéas 1er et 2, sera modifié afin d'imposer aux points de vente de services de communications électroniques l'introduction des données d'identification de l'abonné directement dans les systèmes informatiques de l'opérateur ou de l'entreprise fournissant un service d'identification et leur interdire toute prise de copie de document d'identité."

Cependant, ce n'est pas aux points de vente mais à l'opérateur de faire en sorte que les points de vente introduisent directement les données d'identification de l'abonné dans les systèmes informatiques de l'opérateur. Pour répondre à la préoccupation de l'Autorité de protection des données, l'interdiction visée à l'alinéa 1er a été renforcée et une obligation à charge de l'opérateur a été introduite à l'alinéa 2. Par

elektronische-communicatiediensten. Als bepaalde OTT's de gegevens van de abonnee niet wensen te verwerken om winst te maken, zulks om de persoonlijke levenssfeer van de abonnee te beschermen, is het immers verkieslijk om ze te verplichten een indirecte identificatiemethode te gebruiken in plaats van een directe identificatiemethode, aangezien het eerstgenoemde soort identificatiemethode minder ingrijpt in de persoonlijke levenssfeer van de abonnees.

Terwijl de operatoren die betaaldiensten aanbieden hun hoofdvestiging doorgaans in België hebben, hebben de operatoren die gratis diensten aanbieden hun hoofdvestiging meestal buiten de Europese Unie.

Paragraaf 3: bewaring van de identificatiegegevens en kopieën van identificatiedocumenten door de operator en duur van de bewaring

Het eerste lid neemt een bepaling over van het huidige artikel 127, § 1 en versterkt die. De verkooppunten van de operatoren zijn immers de "zwakke schakel" op het niveau van de identificatie van de abonnee. Uit de inbreukprocedures die het BIPT in het verleden tegen bepaalde operatoren heeft gevoerd, blijkt dat de inbreuken op de regelgeving meestal worden begaan naar aanleiding van onjuiste identificaties door de verkooppunten, die niet altijd de door de operator ingevoerde procedures toepassen.

Het verbod voor het verkooppunt om identificatiegegevens of kopieën van identiteitsdocumenten te bewaren (waarbij een dergelijke kopie verplicht is voor de andere documenten dan de e-ID krachtens artikel 127, § 5, van de telecomwet) houdt in dat het verkooppunt geen gegevens of dergelijke kopieën mag bewaren buiten de IT-systemen van de operator.

In punt 46 van haar advies over het amendement wijst de Gegevensbeschermingsautoriteit erop dat "Het nieuwe artikel 127, § 3, 1ste en 2de lid zal worden gewijzigd om de verkooppunten van elektronische-communicatiediensten te verplichten de identificatiegegevens van de abonnees rechtstreeks in te voeren in de computersystemen van de operator of onderneming die een identificatiedienst aanbiedt, en hen te verbieden kopieën van identiteitsdocumenten te maken."

Niettemin is het niet aan de verkooppunten maar aan de operator om ervoor te zorgen dat de verkooppunten de identificatiegegevens van de abonnee onmiddellijk invoeren in de computersystemen van de operator. Om tegemoet te komen aan de bezorgdheid van de Gegevensbeschermingsautoriteit werd het in het eerste lid bedoelde verbod versterkt en werd in het tweede lid een verplichting ten laste van de operator

ailleurs, il n'est pas possible d'interdire aux points de vente de faire une copie du document d'identification, étant donné que le gouvernement a opté pour maintenir l'obligation de prendre une copie du document d'identification autre que la carte d'identité électronique belge (cf. *infra*).

Dans certains cas, il reste important que les opérateurs puissent quand même se rabattre sur la prise d'une copie de l'eID. Ainsi, pour des raisons techniques, il peut s'avérer nécessaire d'avoir la possibilité de prendre temporairement des copies en attendant le rétablissement d'un dérangement technique ou opérationnel afin de garantir l'identification.

En note de bas de page n° 32 de son avis, l'Autorité de protection des données "recommande au législateur d'indiquer que la copie de la carte d'identité devrait être barrée et qu'il devrait y être fait mention de son destinataire et de l'usage que peut en faire son destinataire."

Les opérateurs ne sont pas favorables à une telle mesure, qui ne pourrait pas être mise en œuvre de manière manuelle mais qui devrait être mise en œuvre dans leur système IT. Or, une fois que la copie du document se trouve dans le système IT de l'opérateur, il n'y a plus de risque d'abus au niveau du point de vente.

La durée de conservation des données d'identification et des copies de documents d'identité est de 12 mois après la fin du contrat comme dans l'article 127 actuel mais est dorénavant fixée directement dans cet article (et non plus par référence vers l'article 126).

La durée de conservation dans le paragraphe 3 ne s'applique pas en cas de disposition légale contraire. C'est le cas pour ce qui concerne l'article 127, § 9, alinéa 1er, 1° (méthode d'identification indirecte via l'adresse IP). Dans ce cas, la durée de conservation des données est fixée par l'article 126 lui-même.

Paragraphe 4: fiabilité de l'identification

Introduction

Il est essentiel que les opérateurs assurent, dans les limites de leurs moyens, que l'identification de l'abonné qui est une personne physique est fiable.

Méthode de comparaison faciale

Afin de faciliter le respect de l'obligation pour l'opérateur d'assurer la fiabilité de l'identification, l'article 127 vise

ingevoerd. Het is overigens niet mogelijk om de verkooppunten te verbieden om een kopie te maken van het identificatiedocument aangezien de regering ervoor heeft gekozen om de verplichting om een kopie te maken van een ander identificatiedocument dan een Belgische elektronische identiteitskaart, te behouden (cf. *infra*).

Het blijft in bepaalde gevallen belangrijk dat operatoren toch kunnen terugvallen op het nemen van een kopie van de eID. Zo kan er om technische redenen een noodzaak zijn om tijdelijk kopieën te kunnen nemen in afwachting van het herstel van een technische of operationele storing om zo de identificatie te garanderen.

In voetnoot nr. 32 van haar advies adviseert de Gegevensbeschermingsautoriteit "de wetgever aan te geven dat de kopie van de identiteitskaart moet worden doorgehaald en dat op de kaart moet worden vermeld wie de ontvanger is en welk gebruik de ontvanger ervan mag maken."

De operatoren zijn geen voorstander van een dergelijke maatregel, die niet handmatig zou kunnen worden uitgevoerd, maar die in hun IT-systeem zou moeten worden uitgevoerd. Zodra de kopie van het document in het IT-systeem van de operator zit, is er echter geen risico meer op misbruik op het niveau van het verkooppunt.

De duur van bewaring van de identificatiegegevens en van de kopieën van identificatiedocumenten bedraagt 12 maanden na het einde van het contract, zoals in het huidige artikel 127, maar wordt voortaan rechtstreeks in dat artikel vastgesteld (en niet meer via verwijzing naar artikel 126).

De duur van bewaring in paragraaf 3 is niet van toepassing in geval van andersluidende wettelijke bepalingen. Dat is het geval voor wat betreft artikel 127, § 9, eerste lid, 1° (indirecte identificatiemethode via het IP-adres). In dat geval wordt de duur van bewaring van de gegevens vastgesteld door artikel 126 zelf.

Paragraaf 4: betrouwbaarheid van de identificatie

Inleiding

Het is van fundamenteel belang dat de operatoren, binnen de grenzen van hun middelen, garanderen dat de identificatie van de abonnee die een natuurlijke persoon is, betrouwbaar is.

Gezichtsvergelijkingsmethode

Teneinde de naleving van de verplichting in hoofde van de operator om de betrouwbaarheid van de identificatie te

dorénavant le recours au traitement automatisé de données biométriques. En pratique, l'opérateur peut comparer des photos que l'abonné prend lui-même de son visage avec la photo figurant sur son document d'identification. De la sorte, l'opérateur peut s'assurer que la personne qui entend s'identifier est bien la même personne que la personne dont la photo se trouve sur le document d'identification.

Lorsque les résultats du traitement automatisé de données biométriques ne sont pas concluants pour une personne spécifique, l'opérateur pourra faire examiner par ses experts l'identification de cette personne.

La modification législative est introduite pour tenir compte de l'article 6, § 4, de la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, tel que modifié par la loi du 25 novembre 2018. Il ressort de cet article que la photographie du titulaire ne peut être utilisée que si cette utilisation est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

La méthode de comparaison faciale permet d'assurer une identification fiable de l'abonné. Elle permet également d'éviter (identification à distance) ou de limiter très fortement (identification dans un point de vente) le rôle joué par un point de vente pour l'identification de l'abonné. Or la pratique a montré que ce rôle est la raison principale des identifications incorrectes (négligence du point de vente ou même fraude de ce dernier).

Au point 104 de son avis sur l'avant-projet de loi "conservation des données", l'Autorité de protection des données indique ce qui suit:

"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."

waarborgen, te vergemakkelijken, beoogt artikel 127 voortaan het gebruik van de geautomatiseerde verwerking van biometrische gegevens. In de praktijk kan de operator foto's die de abonnee zelf van zijn gezicht neemt vergelijken met de foto die op zijn identificatiedocument staat. Op die manier kan de operator zich ervan vergewissen dat de persoon die zich wil identificeren wel degelijk dezelfde persoon is als diegene van wie de foto op het identificatiedocument staat.

Wanneer de resultaten van de geautomatiseerde verwerking van biometrische gegevens niet overtuigend zijn voor een specifieke persoon, zal de operator de identificatie van deze persoon kunnen laten onderzoeken door zijn experten.

De wetswijziging wordt ingevoerd om rekening te houden met artikel 6, § 4, van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten, zoals gewijzigd bij de wet van 25 november 2018. Uit dat artikel blijkt dat de foto van de houder maar mag worden gebruikt als dat gebruik is toegestaan door of krachtens een wet, een decreet of een ordonnantie.

De methode van gezichtsvergelijking maakt het mogelijk om de abonnee op betrouwbare wijze te identificeren. Ze maakt het ook mogelijk om de rol die een verkooppunt speelt bij de identificatie van de abonnee te vermijden (identificatie van op afstand) of heel sterk te beperken (identificatie in een verkooppunt). De praktijk heeft immers uitgewezen dat deze rol de voornaamste reden is voor incorrecte identificaties (slordigheid van het verkooppunt of zelfs fraude door deze laatste).

In punt 104 van haar advies over het voorontwerp van wet "gegevensbewaring" geeft de Gegevensbeschermingsautoriteit het volgende aan:

"De Autoriteit [stelt] 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."

Le gouvernement ne partage pas le point de vue de l'Autorité de protection des données pour les raisons suivantes.

Une technologie n'est pas intrusive dans la vie privée des abonnés en raison de sa nature mais peut l'être selon ses conditions de mise en œuvre et son utilisation. Le gouvernement est d'avis que le traitement de données biométriques prévu par l'article 127 est moins sensible d'un point de vue vie privée que la reconnaissance faciale ou des empreintes digitales qui permettent de déverrouiller un smartphone, étant donné que dans le deuxième cas de figure, les données biométriques doivent être conservées. Il n'est pas admissible que la législation soit plus stricte pour une finalité publique (identification de l'abonné dans le cadre de l'article 127) que pour des usages du secteur privé (ex. déverrouiller un smartphone). Par ailleurs, le secteur bancaire dispose déjà de la possibilité d'utiliser les paramètres biométriques en vertu de sa législation sectorielle spécifique.

Par ailleurs, le traitement de données biométriques bénéficie d'un haut niveau de protection à l'article 9 du RGPD, qui s'applique en l'espèce. En effet, en vertu de cet article, l'abonné de l'opérateur devra donner son consentement explicite au traitement de ses données, ce que l'article 127 rappelle. Pour que ce consentement soit libre, l'abonné doit avoir la possibilité de s'identifier autrement que via un traitement automatisé de ses données biométriques, ce que l'article 127 prévoit également de manière explicite. Par exemple, si l'abonné refuse la technique de comparaison faciale, l'opérateur peut l'inviter à s'identifier auprès de l'un de ses points de vente. Dans ce cas, ce sera le personnel de ce point de vente qui devra s'assurer que la personne qui présente le document d'identité correspond bien à la personne qui y figure ("procédure manuelle"). Il convient cependant de rappeler qu'en cas d'utilisation de l'eID pour s'identifier, le point de vente peut demander l'introduction du code PIN (ce qui permet d'éviter tout type de fraude). De plus, en vertu du principe de minimisation des données visé à l'article 5 du RGPD, le traitement des données devra être limité à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, à savoir dans ce cas-ci s'assurer que la personne qui prend la photo correspond à la personne sur le document d'identification.

La méthode d'identification basée sur le traitement de données biométriques a été introduite dans l'article 127 à la demande de certains opérateurs, ce qui montre une demande du marché. Les opérateurs constatent que le nombre d'achats effectués à l'aide de téléphones intelligents augmente significativement, ce qui s'explique probablement par la pandémie

De regering deelt het standpunt van de Gegevensbeschermingsautoriteit niet om de volgende redenen.

Een technologie is niet indringend in de persoonlijke levenssfeer van de abonnees wegens de aard ervan maar kan dat zijn naargelang van de voorwaarden voor de uitvoering en het gebruik ervan. De regering is van mening dat de verwerking van biometrische gegevens waarin artikel 127 voorziet, minder gevoelig is vanuit privacystandpunt dan gezichtsherkenning of vingerafdrukken, waarmee een smartphone ontgrendeld kan worden, aangezien in het tweede geval de biometrische gegevens bewaard moeten worden. Het is niet toelaatbaar dat de wetgeving strikter is voor een openbaar doel (identificatie van de abonnee in het kader van artikel 127) dan voor toepassingen van de privésector (bijv. ontgrendelen van een smartphone). Bovendien beschikt de banksector reeds over de mogelijkheid om de biometrische parameters te gebruiken krachtens de specifieke sectorale wetgeving.

Bovendien wordt de verwerking van biometrische gegevens sterk beveiligd door artikel 9 van de AVG, dat hier van toepassing is. Krachtens dat artikel moet de abonnee van de operator immers zijn uitdrukkelijke toestemming geven voor de verwerking van zijn gegevens, waaraan artikel 127 herinnert. Om te kunnen spreken van een vrije toestemming moet de abonnee de mogelijkheid hebben om zich op een andere manier te identificeren dan via een geautomatiseerde verwerking van zijn biometrische gegevens, hetgeen artikel 127 ook expliciet voorschrijft. Als de abonnee bijvoorbeeld de gezichtsvergelijkingstechniek weigert, kan de operator hem of haar uitnodigen om zich te identificeren bij een van zijn verkooppunten. In dat geval zal het personeel van dat verkooppunt moeten nagaan of de persoon die het identificatiedocument voorlegt, wel degelijk overeenstemt met de persoon die daarop vermeld is ("manuele procedure"). Er moet evenwel aan worden herinnerd dat in geval van gebruik van de eID om zich te identificeren, het verkooppunt kan vragen om de pincode in te tikken (waardoor elke vorm van fraude kan worden vermeden). Krachtens het principe van de minimale gegevensverwerking waarvan sprake in artikel 5 van de AVG, moet de gegevensverwerking beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt; in dit geval betekent dat: zich ervan vergewissen dat de persoon die de foto neemt overeenstemt met de persoon op het identificatiedocument.

De identificatiemethode die gebaseerd is op de verwerking van biometrische gegevens is ingevoerd in artikel 127 op vraag van sommige operatoren, wat wijst op een vraag vanwege de markt. De operatoren stellen vast dat het aantal aankopen met behulp van smartphones aanzienlijk stijgt, hetgeen waarschijnlijk wordt verklaard door de COVID-pandemie. Het

COVID. Il est important de leur permettre de faciliter la souscription par le biais d'un téléphone intelligent à des services de communications électroniques.

Étant donné que la loi oblige les opérateurs à identifier leurs abonnés de manière fiable au bénéfice des autorités et qu'il convient d'éviter des fraudes en matière d'identité, il est essentiel de permettre aux opérateurs de pouvoir remplir ces tâches au moyen des méthodes d'identification les plus appropriées et fiables convenant au contexte de chaque canal numérique et à tous les groupes cibles. À titre d'exemple, la méthode proposée empêchera qu'une personne puisse s'identifier à l'aide d'une eID volé ou d'un passeport volé.

Cette méthode innovante offre de multiples avantages à l'abonné: il ne doit plus se rendre dans un point de vente de l'opérateur en vue de son identification, cette méthode est simple d'utilisation et ne requiert pas l'installation préalable d'applications sur le téléphone intelligent.

Il est vrai que le client peut toujours revenir à des méthodes alternatives telles qu'itsme et le lecteur eID, ainsi qu'à d'autres méthodes alternatives dans d'autres canaux de vente tels que le magasin physique.

Toutefois, ces méthodes ne sont pas toujours les plus appropriées pour offrir une réponse dans chaque contexte numérique. L'identification sur la base de la comparaison faciale est complémentaire et constitue un complément nécessaire aux méthodes existantes.

Il est ainsi difficile d'estimer la croissance que connaîtra la méthode itsme. Celle-ci est facile d'utilisation mais nécessite une activation préalable, ce qui n'est pas le cas lors de l'utilisation des données biométriques. Les opérateurs estiment ainsi que les clients ne disposeront pas toujours d'itsme.

Il est possible d'utiliser le lecteur eID via un ordinateur mais pas via un smartphone, ce qui limite les possibilités de vérification de l'identité d'un client via un smartphone.

De plus, l'utilisation des données biométriques est une solution pour les résidents non belges sans carte électronique belge pour étrangers ou pour les étrangers en visite en Belgique. L'eID et itsme ne sont pas disponibles pour ces clients.

Les avancées technologiques en la matière ont augmenté la fiabilité de cette méthode. L'autorisation ministérielle prévue

is belangrijk dat ze de mogelijkheid krijgen om de inschrijving via een smartphone op elektronische-communicatiediensten te vergemakkelijken.

Aangezien de wet de operatoren verplicht om hun abonnees op een betrouwbare manier te identificeren ten voordele van de autoriteiten en dat identiteitsfraude moet worden vermeden, is het van fundamenteel belang dat de operatoren in staat worden gesteld om deze taken te vervullen via de meest geschikte en betrouwbare identificatiemethodes die passen binnen de context van elk digitaal kanaal en voor alle doelgroepen. De voorgestelde methode zal bijvoorbeeld verhinderen dat iemand zich kan identificeren met behulp van een gestolen eID of een gestolen paspoort.

Deze innoverende methode biedt de abonnee talrijke voordelen: hij of zij hoeft niet meer naar een verkooppunt van de operator te gaan om zich te identificeren, deze methode is eenvoudig in gebruik en vereist geen voorafgaande installatie van applicaties op de smartphone.

Het is waar dat de klant altijd kan terugvallen op alternatieve methodes zoals itsme en de eID reader en ook op alternatieve methodes in andere verkoopkanalen zoals in de fysische winkel.

Evenwel zijn deze methodes niet steeds het meest geschikt om een antwoord te bieden in elke digitale context. De identificatie op basis van gezichtsvergelijking is complementair en is een noodzakelijke aanvulling voor de reeds bestaande methodes.

Zo is het moeilijk in te schatten welke groei de itsme-methode nog zal kennen. itsme is gemakkelijk in gebruik maar vereist wel een voorafgaande activatie. Dit is niet het geval bij het gebruik van de biometrische gegevens. Zo zijn de operatoren van oordeel dat klanten niet steeds over itsme zullen beschikken.

Het gebruik van de eID-lezer is mogelijk via een computer maar niet via een smartphone. De mogelijkheden voor de verificatie van de identiteit van een klant via smartphone zijn daardoor beperkt.

Het gebruik van de biometrische gegevens is bovendien een oplossing voor niet-Belgische inwoners zonder Belgische elektronische kaart, voor buitenlanders of voor buitenlanders op bezoek in België. Voor deze klanten zijn de eID reader en itsme niet beschikbaar.

De technologische vooruitgang op dat gebied heeft de betrouwbaarheid van die methode vergroot. De ministeriële

pour valider cette méthode d'identification au cas par cas ne porte que sur la question de savoir si cette méthode est suffisamment fiable pour les autorités (en particulier la police et les services de renseignement et de sécurité). Cette autorisation n'a pas pour objet de se prononcer sur le respect de la législation visant à protéger la vie privée des abonnés.

Pour répondre aux préoccupations de l'Autorité de protection des données, certaines conditions entourant l'usage de cette technologie ont été précisées dans l'article même, le RGPD restant d'application. L'abonné doit donner son consentement (au sens du RGPD) et pour que le consentement soit valable, l'opérateur doit lui offrir une alternative pour s'identifier. L'opérateur ne pourra pas communiquer les données biométriques à un tiers au sens du RGPD. Il convient à cet égard de noter que l'opérateur fera généralement appel à un ou plusieurs sous-traitants pour la mise en place de la solution de la comparaison faciale. Ces sous-traitants ne sont pas considérés comme des tiers, puisque leur rôle est essentiel pour le fonctionnement de la solution. En vertu des principes de finalité et de nécessité du GDPR, l'opérateur ne pourra traiter les données que dans la mesure nécessaire pour le traitement prévu par la loi, à savoir la comparaison faciale employée uniquement afin de vérifier la fiabilité de l'identité. Par conséquent, l'opérateur ne peut pas conserver les paramètres biométriques du visage de la personne. Cependant, ce principe ne peut pas aller jusqu'à rendre la comparaison faciale en pratique techniquement impossible à réaliser. Seules les données nécessaires de la carte eID sont conservées en vue de l'identification du client.

L'autorisation des ministres peut porter sur une demande d'un opérateur ou d'un fournisseur de solution de comparaison faciale. Dans ce dernier cas, les opérateurs qui font appel à ce fournisseur bénéficieront en pratique de l'autorisation.

Au point 52 de son avis sur les amendements, l'Autorité de protection des données indique à juste titre que "le traitement de données à caractère personnel – en particulier la comparaison automatisée entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage – constitue, bien évidemment, une ingérence dans la vie privée des abonnés, quand bien même les données biométriques ne sont pas conservées."

Elle ajoute que "Cette ingérence présente d'ailleurs un caractère particulièrement important au vu du caractère sensible des données traitées et des risques de fraude à l'identité qui découlent d'une violation de telles données." (point 52)

machtiging die wordt bepaald om deze identificatiemethode te valideren per geval, heeft enkel betrekking op de vraag of deze methode voldoende betrouwbaar is voor de veiligheidsdiensten (in het bijzonder de politie en de inlichtingen- en veiligheidsdiensten). Deze machtiging heeft niet tot doel een uitspraak te doen over de naleving van de wetgeving die tot doel heeft de privacy van de abonnees te beschermen.

Om op de bezorgdheid van de Gegevensbeschermingsautoriteit te antwoorden, zijn een aantal voorwaarden voor het gebruik van deze technologie gepreciseerd in het artikel zelf, waarbij de AVG van toepassing blijft. De abonnee moet toestemming geven (in de zin van de AVG) en opdat de toestemming geldig is, moet de operator hem of haar een alternatief bieden om zich te identificeren. De operator zal de biometrische gegevens niet mogen meedelen aan een derde zoals bedoeld in de AVG. Wat dat betreft moet worden opgemerkt dat de operator doorgaans een beroep zal doen op een of meer onderaannemers voor de invoering van de oplossing van de gezichtsvergelijking. Deze onderaannemers worden niet beschouwd als derden, aangezien hun rol essentieel is voor de werking van de oplossing. Krachtens de principes inzake doel en noodzaak van de AVG mag de operator de gegevens maar verwerken voor zover dit noodzakelijk is voor de wettelijk bepaalde verwerking, namelijk de gezichtsvergelijking die enkel toegepast wordt om de betrouwbaarheid van de identiteit na te gaan. Bijgevolg mag de operator de biometrische parameters van het gezicht van de persoon niet bewaren. Dat principe mag echter niet zo ver gaan dat de gezichtsvergelijking in de praktijk technisch onmogelijk wordt. Enkel de noodzakelijke gegevens van de eID-kaart worden bewaard met het oog op de identificatie van de klant.

De machtiging van de ministers kan slaan op een verzoek van een operator of van een aanbieder van oplossingen voor gezichtsvergelijking. In dat laatste geval zullen de operatoren die op die aanbieder een beroep doen in de praktijk de machtiging hebben.

In punt 52 van haar advies over de amendementen wijst de Gegevensbeschermingsautoriteit er terecht op dat "de verwerking van persoonsgegevens – met name de geautomatiseerde vergelijking tussen de biometrische parameters op de foto van het identiteitsbewijs van de abonnee en die van zijn of haar gezicht – duidelijk een inmenging in het privéleven van abonnees vormt, ook al worden de biometrische gegevens niet opgeslagen."

Ze voegt daaraan toe dat "Deze inmenging bijzonder belangrijk [is] gezien de gevoelige aard van de verwerkte gegevens en de risico's van identiteitsfraude die uit een inbreuk op dergelijke gegevens voortvloeien." (punt 52)

Concernant le caractère sensible des données, il convient de tenir compte des éléments suivants:

— le système de comparaison faciale qui est autorisé se distingue des méthodes de reconnaissance faciale beaucoup plus intrusive dans la vie privée (par exemple pouvoir reconnaître une personne qui se trouve dans la rue à l'aide d'une caméra et d'une base de données); le système de comparaison faciale visé dans l'article 127 revient à automatiser le contrôle manuel fait dans un point de vente (vérifier que la personne qui se présente correspond bien à la personne sur le document d'identité);

— une conservation des paramètres biométriques du visage n'est pas permise dans le cadre du système de comparaison faciale (seule une copie du document d'identification est obligatoire si ce document n'est pas une carte d'identité électronique belge);

— dans le secteur bancaire, nous constatons que des solutions semblables avec reconnaissance faciale sont déjà utilisées depuis plusieurs années. Les smartphones aussi prévoient déjà des options de reconnaissance faciale afin d'y avoir accès;

— cette méthode d'identification n'a pas vocation à être utilisée à chaque utilisation du service, mais en principe uniquement lors de la souscription au service.

Concernant le risque de fraude, il convient de noter que les systèmes de comparaison faciale sont devenus très sophistiqués et le seront encore d'avantage à l'avenir, de sorte que le risque de fraude à l'identité est bien plus faible en mettant en œuvre ce type de méthode que lors d'une identification dans un point de vente. C'est justement pour éviter une fraude à l'identité que plusieurs opérateurs souhaitent mettre en œuvre cette méthode de comparaison faciale.

En cas de nouveaux types de tentatives de fraude, c'est à l'opérateur à prendre les mesures adéquates pour éviter ce type de fraude (bloquer cette méthode d'identification ou implémenter des mesures nécessaires). L'existence d'un certain (type de) fraude n'est pas un argument pour interdire une méthode mais doit amener l'opérateur à prendre des mesures pour réduire le risque. Toutes les méthodes d'identification sont susceptibles de fraude (même itsme ou l'identification par l'eID).

En note de bas de page n° 33 de son avis sur les amendements, l'Autorité de protection des données indique que "les systèmes de reconnaissance faciale se sont révélés

Met betrekking tot de gevoelige aard van de gegevens moet rekening worden gehouden met de volgende elementen:

— het gezichtsvergelijkingssysteem dat is toegestaan, onderscheidt zich van de gezichtsherkenningsmethodes die veel dieper doordringen in de persoonlijke levenssfeer (bijvoorbeeld een persoon op straat kunnen herkennen met behulp van een camera en een gegevensbank); het in artikel 127 bedoelde gezichtsvergelijkingssysteem komt neer op de automatisering van de handmatige controle die in een verkooppunt wordt verricht (nagaan of de persoon die zich aandient, overeenkomt met de persoon op het identiteitsdocument);

— de biometrische parameters van het gezicht bewaren is niet toegestaan in het kader van een gezichtsvergelijkingssysteem (alleen een kopie van het identificatiedocument is verplicht als dat document geen Belgische elektronische identiteitskaart is);

— in de banksector zien we dat gelijkaardige oplossingen met gezichtsvergelijking reeds verschillende jaren in gebruik zijn. Ook smartphones voorzien reeds in opties van gezichtsherkenning om toegang te krijgen tot de smartphone;

— deze identificatiemethode moet niet bij elk gebruik van de dienst worden gebruikt, maar in principe alleen bij de intekening op de dienst.

Met betrekking tot het risico op fraude moet worden opgemerkt dat de gezichtsvergelijkingssystemen zeer geavanceerd geworden zijn en dat in de toekomst nog meer zullen zijn, zodat het risico op identiteitsfraude veel kleiner is wanneer dergelijke methodes worden gebruikt dan bij een identificatie in een verkooppunt. Het is precies om identiteitsfraude te voorkomen dat veel operatoren deze gezichtsvergelijkingsmethode willen invoeren.

Bij nieuwe soorten van pogingen tot fraude moet de operator de passende maatregelen nemen om dat soort van fraude te voorkomen (die identificatiemethode blokkeren of de nodige maatregelen implementeren). Dat (een bepaalde soort) fraude bestaat, is geen argument om een methode te verbieden maar moet de operator ertoe aanzetten maatregelen te treffen om het risico te beperken. Bij alle identificatiemethodes kan fraude worden gepleegd (zelfs bij itsme of de identificatie via de eID).

In voetnoot nr. 33 van haar advies over de amendementen wijst de Gegevensbeschermingsautoriteit erop dat "gezichtsherkenningssystemen kwetsbaar zijn voor "*morphing* attacks".

vulnérables aux attaques de "*morphing*". Dans ces attaques, les images faciales de deux individus (ou plus) sont combinées (morphées) et l'image faciale morphée résultante est ensuite présentée lors de l'enregistrement comme une référence biométrique. Si l'image morphée est acceptée, il est probable que tous les individus ayant contribué à l'image faciale morphée puissent être identifiés avec succès par rapport à celle-ci. Les attaques par *morphing* constituent donc une menace sérieuse pour les systèmes de reconnaissance faciale. Cette vulnérabilité crée un risque de fraudes à l'identité."

Le risque de "*morphing attacks*" (l'utilisation de photos de différentes personnes transformées en une seule photo) voudrait dire que la photo sur l'eID serait également manipulée de cette manière. Cependant, pour le selfie, il est possible de vérifier que le client est bel et bien "vivant" et qu'il ne présente pas une autre photo manipulée. Dans un tel scénario, le client reçoit des instructions pour prendre un selfie depuis divers angles. Avec un tel contrôle du selfie, la possibilité de manipuler celui-ci est exclue.

Selon l'Autorité de protection des données (point 54 de son avis), il existe "un risque non-négligeable que, à la suite d'une fuite de données, des photos utilisées dans le cadre de la comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage restent en circulation."

Il convient à cet égard de rappeler qu'il est interdit de conserver les données biométriques du visage au-delà de la comparaison. Par ailleurs, il est plus facile pour un opérateur de contrôler la fiabilité d'un fournisseur d'une solution de comparaison faciale (qui comprend des professionnels de l'identification) que ses nombreux points de ventes (des personnes qui ne sont pas spécialistes de l'identification).

L'opérateur est par ailleurs tenu d'informer l'IBPT et l'Autorité de protection des données de toute fuite de données.

À la note de bas de page n° 36, l'Autorité de protection des données "relève que les individus ne peuvent pas vérifier que leur photo ne sera effectivement pas enregistrée, quand bien même une interdiction formelle serait reprise dans le dispositif, en particulier, parce que la reconnaissance faciale se fait à partir de moyens électroniques dont ils ne peuvent pas contrôler la configuration."

Cependant, ce risque n'est pas propre à un système de comparaison faciale mais existe pour toute information digitale qui est confiée à un tiers, comme par exemple la messagerie

Bij deze aanvallen worden de gezichtsbeelden van twee (of meer) personen gecombineerd (gemorfd) en het resulterende gemorfde gezichtsbeeld wordt vervolgens bij de registratie gepresenteerd als biometrische referentie. Indien het gemorfde beeld wordt aanvaard, is het waarschijnlijk dat alle personen die aan het gemorfde gezichtsbeeld hebben bijgedragen, er met succes mee kunnen worden geïdentificeerd. *Morphing*-aanvallen vormen dan ook een ernstige bedreiging voor gezichtsherkenningssystemen. Deze kwetsbaarheid creëert een risico van identiteitsfraude."

Het risico van "*morphing attacks*" (het gebruik van foto's met verschillende personen gemorfd in één foto) zou betekenen dat de foto op de eID op deze manier zou gemanipuleerd zijn. Maar voor de selfie zelf kan getest worden dat de klant wel degelijk "levend" aanwezig is en niet een andere gemanipuleerde foto presenteert. De klant krijgt in dergelijk scenario instructies om een selfie te nemen vanuit verschillende posities. Met dergelijke controle van de selfie wordt uitgesloten dat de selfies gemanipuleerd kunnen worden.

Volgens de Gegevensbeschermingsautoriteit (punt 54 van haar advies) bestaat er "een niet te verwaarlozen risico [...] dat, na het uitlekken van gegevens, de foto's die worden gebruikt bij de vergelijking tussen de biometrische parameters op de foto van het identiteitsbewijs van de abonnee en die van zijn of haar gezicht in omloop blijven."

In dit verband moet erop worden gewezen dat het verboden is om de biometrische gegevens van het gezicht langer te bewaren dan de vergelijking. Bovendien is het voor een operator gemakkelijker om de betrouwbaarheid van een leverancier van een gezichtsvergelijkingsoplossing (die werkt met professionals op het gebied van identificatie) te controleren dan zijn talrijke verkooppunten (personen die geen specialist zijn op het gebied van identificatie).

De operator moet overigens het BIPT en de Gegevensbeschermingsautoriteit op de hoogte brengen van elk gegevenslek.

In voetnoot nr. 36 merkt de Gegevensbeschermingsautoriteit op dat "personen niet kunnen controleren dat hun foto niet wordt opgenomen, zelfs indien in het systeem een formeel verbod is opgenomen, met name omdat gezichtsherkenning gebaseerd is op elektronische middelen waarvan zij de configuratie niet kunnen controleren."

Dat risico is echter niet eigen aan een gezichtsvergelijkingssysteem maar bestaat voor alle digitale informatie die aan een derde wordt toevertrouwd, zoals bijv. instant

instantanée ou le courrier électronique. Dans ces exemples, comment un citoyen peut-il vérifier que ses données sont correctement détruites et ne sont pas conservées?

Dans son avis (point 53), l'Autorité de protection des données indique que "la comparaison faite avec l'utilisation de la biométrie qui permet de déverrouiller un smartphone est fallacieuse. En effet, premièrement, au contraire de ce qui est prévu dans le projet, les données biométriques utilisées pour déverrouiller un smartphone sont gardées dans une enclave et ne quittent pas le smartphone. Deuxièmement, au contraire de la photo conservée sur la carte d'identité, les smartphones ne stockent pas l'image complète du visage de la personne, mais uniquement des points caractéristiques ou des motifs, un sous-ensemble de caractéristiques extrait de l'image du visage de la personne concernée ("template"); ce qui réduit les risques de fraude à l'identité en cas de violation de ces données."

Selon l'explication donnée par l'Autorité de protection des données, "les données biométriques utilisées pour déverrouiller un smartphone sont gardées dans une enclave" du téléphone. Or dans le cadre de la comparaison faciale visées à l'article 127 de la loi télécom, les données biométriques du visage ne sont mêmes pas gardées.

Concernant la conservation par l'opérateur de la photo du document d'identification, cette conservation doit se faire uniquement pour les autres documents d'identification que la carte d'identité électronique et cette conservation vaut quelle que soit la méthode d'identification mise en œuvre (également pour une identification dans un point de vente).

Selon l'Autorité de protection des données, la méthode de comparaison faciale ne répond pas à l'exigence de nécessité (c'est-à-dire qu'il ne doit pas exister de moyens moins intrusifs permettant d'atteindre l'objectif). (point 52 de son avis) "En effet, il existe d'autres moyens d'authentification à distance qui sont plus sécurisés que l'utilisation de la reconnaissance faciale, à savoir l'usage de l'eID et le recours à des prestataires de services de confiance qualifiés qui offrent un service de signature électronique qualifiée (par exemple: Itsme). Ces deux outils offrent, en effet, un niveau de sécurité supérieur à celui de la reconnaissance faciale tout en permettant d'atteindre l'objectif poursuivi qui est de veiller à la fiabilité de l'identification de la personne concernée. […] À partir du moment où une méthode alternative moins intrusive dans le droit à la protection des données à caractère personnel est disponible pour assurer la fiabilité des données d'identification collectées, le législateur ne peut pas autoriser le recours à la reconnaissance faciale". (point 54)

messaging of e-mail. Hoe kan een burger in de genoemde voorbeelden controleren of zijn gegevens correct vernietigd zijn en niet bewaard worden?

In haar advies (punt 53) wijst de Gegevensbeschermingsautoriteit erop dat "de vergelijking die wordt gemaakt met het gebruik van biometrische gegevens om een smartphone te ontgrendelen, misleidend is. Ten eerste worden, in tegenstelling tot wat in het ontwerp is voorzien, de biometrische gegevens die worden gebruikt om een smartphone te ontgrendelen, bewaard in een enclave en verlaten zij de smartphone niet. Ten tweede slaan smartphones, in tegenstelling tot de foto op de identiteitskaart, niet het volledige beeld van het gezicht van de betrokkene op, maar alleen kenmerkende punten of patronen, ·een subset van kenmerken die uit het beeld van het gezicht van de betrokkene zijn geëxtraheerd ("template"); dit vermindert het risico van identiteitsfraude in het geval van een inbreuk op deze gegevens."

Volgens de uitleg van de Gegevensbeschermingsautoriteit worden "de biometrische gegevens die worden gebruikt om een smartphone te ontgrendelen, bewaard in een enclave" van de telefoon. In het kader van de in artikel 127 van de telecomwet bedoelde gezichtsvergelijking worden de biometrische gegevens van het gezicht echter zelfs niet bewaard.

De operator moet de foto van het identificatiedocument alleen bewaren indien het een ander identificatiedocument betreft dan de elektronische identiteitskaart, ongeacht de gebruikte identificatiemethode (ook bij een identificatie in een verkooppunt).

Volgens de Gegevensbeschermingsautoriteit beantwoordt de gezichtsvergelijkingsmethode niet aan de noodzakelijkheidsvereiste (dat wil zeggen dat er geen minder ingrijpende middelen mogen bestaan om het doel te bereiken). (punt 52 van haar advies) "Er zijn immers andere middelen voor authenticatie op afstand die veiliger zijn dan het gebruik van gezichtsherkenning, namelijk het gebruik van eID en het gebruik van gekwalificeerde "trust service providers" die een gekwalificeerde elektronische handtekeningendienst aanbieden (bijvoorbeeld Itsme). Deze twee instrumenten bieden een hoger veiligheidsniveau dan gezichtsherkenning, terwijl toch de doelstelling wordt bereikt om de betrouwbaarheid van de identificatie van de betrokken persoon te waarborgen. [...] Zolang een alternatieve methode beschikbaar is die minder indringend is in het recht op bescherming van persoonsgegevens om de betrouwbaarheid van de verzamelde identificatiegegevens te waarborgen, kan de wetgever het gebruik van gezichtsherkenning niet toestaan." (punt 54)

Dans son avis sur l'amendement, le Conseil d'État indique ce qui suit:

— "4.2. Tout traitement de données à caractère personnel doit, entre autres, respecter les exigences générales reprises à l'article 5, paragraphe 1er, du RGPD.

Parmi ces exigences se trouve le principe de minimisation des données qui requiert que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

— S'agissant de la méthode d'identification en cause, qui repose sur le traitement de données biométriques, les justifications reprises dans la justification de l'amendement ne sont pas convaincantes.

Il appartient dès lors à l'auteur de l'amendement de préciser, dans la justification de celui-ci, les éléments qui permettent de considérer que le principe de minimisation des données est effectivement respecté en l'espèce, alors que d'autres moyens, moins intrusifs au regard de la vie privée, existent et apparaissent être suffisants pour démontrer l'identité de l'abonné, même pour ceux qui ne peuvent avoir recours à l'eID ou à des prestataires de services de confiance qualifiés qui offrent un service de signature électronique qualifiée."

De l'avis du gouvernement, le principe de minimisation des données cité par le Conseil d'État vise à minimiser les données qui peuvent être traitées dans le cadre d'un traitement de données mais non à exclure certaines méthodes d'identification de l'abonné. Ce principe indique que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Il ne s'agit pas d'un principe de minimisation des traitements de données, de sorte que certains traitements de données ne seraient pas admis car d'autres traitements de données moins intrusif permettraient d'atteindre le même objectif.

Estimer que le principe de minimisation des données doit mener à exclure la méthode de comparaison faciale porterait atteinte aux intérêts de l'utilisateur final, car cela limiterait les possibilités dont il dispose pour s'identifier. Par exemple, cela voudrait dire qu'une personne qui dispose d'un passeport ne peut plus s'identifier à distance à l'aide de la méthode de comparaison faciale mais devrait par exemple se rendre dans un point de vente pour s'identifier. Si le point de vente a des

In zijn advies over het amendement wijst de Raad van State op het volgende:

— "4.2. Elke verwerking van persoonsgegevens moet onder meer voldoen aan de algemene vereisten van artikel 5, lid 1, van de AVG.

Een van die vereisten is het beginsel van de minimale gegevensverwerking, naar luidt waarvan de persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij verwerkt worden.

— Met betrekking tot de betrokken identificatiemethode, die berust op de verwerking van biometrische gegevens, zijn de redenen die in de verantwoording van het amendement gegeven worden niet overtuigend.

Het staat derhalve aan de indiener van het amendement om in de verantwoording ervan te preciseren op grond van welke elementen ervan uit kan worden gegaan dat het beginsel van de minimale gegevensverwerking in casu daadwerkelijk nageleefd is, terwijl er andere middelen bestaan die minder ingrijpend zijn in het licht van de persoonlijke levenssfeer en voldoende lijken om de identiteit van de abonnee aan te tonen, zelfs voor degenen die geen gebruik kunnen maken van de eID of van gekwalificeerde verleners van vertrouwensdiensten die een dienst voor gekwalificeerde elektronische handtekeningen aanbieden."

Volgens de regering dient het door de Raad van State aangehaalde beginsel van minimale gegevensverwerking om de gegevens die mogen worden verwerkt in het kader van een gegevensverwerking tot een minimum te beperken, maar niet om bepaalde methodes voor de identificatie van de abonnee uit te sluiten. Dit beginsel bepaalt dat de persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt. Het gaat niet om een beginsel waarmee de gegevensverwerkingen tot een minimum worden beperkt zodat bepaalde gegevensverwerkingen niet toegestaan zouden zijn omdat met andere, minder ingrijpende gegevensverwerkingen hetzelfde doel zou kunnen worden bereikt.

Door ervan uit te gaan dat het beginsel van minimale gegevensverwerking moet leiden tot de uitsluiting van de gezichtsvergelijkingsmethode, zouden de belangen van de eindgebruiker worden geschaad, want dat zou de mogelijkheden die hij ter beschikking heeft om zich te identificeren, beperken. Dat zou bijvoorbeeld willen zeggen dat een persoon die een paspoort heeft, zich niet meer op afstand kan identificeren met behulp van de gezichtsvergelijkingsmethode, maar

doutes sur l'authenticité du passeport, il pourrait refuser à son titulaire de souscrire au service. Alors qu'il est possible que cette personne aurait pu s'identifier à distance à l'aide de l'outil de comparaison faciale. Si on pousse le raisonnement de l'Autorité de protection des données jusqu'au bout, il faudrait interdire l'identification de l'abonné dans un point de vente, car elle est moins sécurisée que l'identification à distance à l'aide de itsme ou d'une lecture de la carte d'identité électronique.

— Selon l'avis du Conseil d'État (point 4.3), Conformément à l'article 9, paragraphe 1er, et paragraphe 2, a), du RGPD autorise le traitement des données biométriques aux fins d'identifier une personne physique de manière unique porte sur des données sensibles si

"la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1er ne peut pas être levée par la personne concernée".

Or, à ce jour, le droit de l'Union et le droit belge permettent toujours de lever l'interdiction de traiter des données biométriques aux fins d'identifier une personne physique de manière unique.

La méthode de comparaison faciale est une bonne méthode pour atteindre les finalités visées par le gouvernement.

Avec cette méthode de reconnaissance faciale, les opérateurs peuvent réduire l'usurpation d'identité. Cette méthode permet aussi de ne pas faire intervenir les points de vente, qui sont les "maillons faibles" en matière de fiabilité de l'identification de l'abonné. Cette augmentation de la fiabilité de l'identification est bénéfique pour les autorités, pour les opérateurs, qui sont victimes des fraudes (d'où l'intérêt de plusieurs opérateurs de mettre en œuvre cette méthode) et pour l'abonné (éviter un détournement de son identité). Même si une personne parvient à s'identifier avec un faux document d'identification, la copie de ce document d'identification autre que la carte d'identité électronique belge comprendra une photo correcte de l'abonné, ce qui pourrait permettre aux autorités de démarrer une enquête.

bijvoorbeeld naar een verkooppunt zou moeten gaan om zich te identificeren. Als het verkooppunt twijfels heeft over de authenticiteit van het paspoort, zou het de houder ervan kunnen weigeren om op de dienst in te tekenen. Terwijl het mogelijk is dat die persoon zich op afstand had kunnen identificeren met behulp van het gezichtsvergelijkingsinstrument. Als de redenering van de Gegevensbeschermingsautoriteit tot het einde wordt doorgetrokken, zou de identificatie van de abonnee in een verkooppunt moeten worden verboden, aangezien die minder beveiligd is dan de identificatie op afstand met behulp van itsme of het lezen van de elektronische identiteitskaart.

— In het advies van de Raad van State (punt 4.3) staat dat krachtens artikel 9, lid 1 en lid 2, a), van de AVG de verwerking van biometrische gegevens met het oog op de unieke identificatie van een natuurlijk persoon mogelijk is indien

"de betrokkene (…) uitdrukkelijke toestemming gegeven [heeft] voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven"."

Tot nog toe hebben het Unierecht en het Belgische recht echter niet verboden om het verbod om biometrische gegevens te verwerken met het oog op de unieke identificatie van een natuurlijke persoon, op te heffen.

De gezichtsvergelijkingsmethode is ook een goede methode om de door de regering beoogde doelstellingen te bereiken.

Met deze methode van gezichtsvergelijking kunnen operatoren identiteitsfraude verminderen. Dankzij deze methode is het ook niet langer nodig om een beroep te doen op de verkooppunten, die de "zwakke schakels" zijn wanneer het gaat om de betrouwbaarheid van de identificatie van de abonnee. Dat de betrouwbaarheid van de identificatie daardoor toeneemt, komt niet alleen de autoriteiten ten goede, maar ook de operatoren, die het slachtoffer zijn van fraude (vandaar het belang van verschillende operatoren om van deze methode gebruik te maken) en de abonnee (die zo misbruik van zijn identiteit voorkomt). Zelfs als een persoon erin slaagt om zich te identificeren met een vals identiteitsdocument, zal op de kopie van dat identiteitsdocument dat geen Belgische elektronische identiteitskaart is, een correcte foto van de abonnee staan, waardoor de autoriteiten een onderzoek zouden kunnen opstarten.

La méthode de comparaison faciale permet aux opérateurs de répondre à leur obligation d'effectuer une identification fiable de l'abonné et de s'adapter aux besoins des abonnés (voir infra).

Il s'agit d'une méthode acceptable du point de vue de la vie privée, dès lors que les données de biométrie du visage ne sont pas conservées. Comme déjà indiqué, cela permet de ne pas faire intervenir les points de vente, qui sont parfois eux-mêmes à l'origine de fraude (ex. réutilisation frauduleuse de données d'identification d'une personne pour identifier une autre personne).

Cela permet aussi d'augmenter les possibilités pour un abonné de s'identifier et de faciliter son identification, en particulier pour les identifications en ligne. Pour de nombreux utilisateurs qui maîtrisent la technologie, c'est devenu une habitude quotidienne. La comparaison des paramètres biométriques d'un selfie et de la photo sur un document d'identité offre de nouvelles possibilités d'identification fiable. Cette solution en particulier peut fortement faciliter l'identification de clients, surtout en cas d'identification par smartphone, où l'utilisation du lecteur d'eID belge n'est pas possible.

En réponse à la note de bas de page n° 37 de l'avis de l'Autorité de protection des donnée sur les amendements, le gouvernement ne nie pas que "le recours à code pin associée à l'utilisation de l'eID en vue de l'authentification de son titulaire empêche, en principe, qu'une personne puisse s'authentifier avec une carte eID volée, sans qu'il soit nécessaire de recourir à la reconnaissance faciale." Cependant, la méthode de comparaison faciale l'empêche également.

À la note de bas de page n° 39, de son avis, l'Autorité de protection des données indique qu'elle "n'est pas convaincue par l'argumentation selon laquelle, étant donné que les clients ne disposeront pas toujours d'Itsme, il convient d'autoriser le recours à la reconnaissance faciale pour assurer la fiabilité des données d'identification collectées. Tout d'abord, force est constater que l'introduction du COVID-19 *Safe Ticket* (CST) dans la vie quotidienne des personnes vivant en Belgique a amené une grande partie de la population à installer Itsme sur son smartphone afin d'y installer l'application *CovidSafe. BE* et d'y récupérer les certificats (de vaccination, de test ou de rétablissement) constituant le CST. Par ailleurs, le fait que les personnes ne résidant pas en Belgique ne puissent pas installer Itsme ou s'authentifier par le biais d'une carte eID ne peut justifier le fait d'autoriser, à l'égard de toute la population, la mise en place d'un traitement de données qui n'apparait pas nécessaire et qui est dès lors disproportionné. En effet,

Dankzij de gezichtsvergelijkingsmethode kunnen de operatoren voldoen aan hun verplichting om een betrouwbare identificatie van de abonnee uit te voeren en zich aan te passen aan de behoeften van de abonnees (cf. *infra*).

Het gaat om een aanvaardbare methode vanuit privacyoogpunt aangezien de biometrische gegevens van het gezicht niet worden bewaard. Zoals reeds werd aangegeven, is het daardoor niet langer nodig om een beroep te doen op de verkooppunten, die soms zelf aan de basis liggen van fraude (bijvoorbeeld frauduleus hergebruik van identificatiegegevens van een persoon om een andere persoon te identificeren).

Daardoor is het ook mogelijk om een abonnee meer mogelijkheden te bieden om zich te identificeren en zijn identificatie te vergemakkelijken, in het bijzonder voor online identificaties. Voor vele gebruikers die mee zijn met de technologie is dit een dagelijkse gewoonte geworden. De vergelijking van de biometrische parameters van een selfie en de foto op een identiteitsdocument geeft nieuwe mogelijkheden om een betrouwbare identificatie uit te voeren. Deze oplossing kan specifiek de online identificatie voor de klant sterk vergemakkelijken vooral in geval van identificatie via smartphone waar het gebruik van de Belgische eID lezer niet mogelijk is.

In antwoord op voetnoot nr. 37 van het advies van de Gegevensbeschermingsautoriteit over de amendementen ontkent de regering niet dat "het gebruik van de pincode in combinatie met het gebruik van de eID voor de authenticatie van de houder in beginsel [verhindert] dat een persoon zich kan authenticeren met een gestolen eID-kaart, zonder dat gezichtsherkenning nodig is." De gezichtsvergelijkingsmethode verhindert dat echter ook.

In voetnoot nr. 39 van haar advies wijst de Gegevensbeschermingsautoriteit erop dat ze "niet overtuigd [is] door het argument dat, aangezien klanten niet altijd toegang zullen hebben tot Itsme, het gebruik van gezichtsherkenning moet worden toegestaan om de betrouwbaarheid van de verzamelde identificatiegegevens te garanderen. In de eerste plaats is het duidelijk dat de introductie van het COVID-19 *Safe Ticket* (CST) in het dagelijkse leven van de inwoners van België ertoe heeft geleid dat een groot deel van de bevolking Itsme op zijn smartphone heeft geïnstalleerd om de applicatie *CovidSafe. BE* te installeren en om de certificaten (van vaccinatie, test of herstel) waaruit het CST bestaat. Overigens kan het feit dat personen die niet in België wonen, Itsme niet kunnen installeren en zich niet met een eID-kaart kunnen authenticeren, geen rechtvaardiging vormen voor het toestaan van de verwerking van gegevens voor de gehele bevolking, hetgeen niet noodzakelijk en dus onevenredig lijkt Er zijn immers andere

il existe pour ces personnes d'autres moyens de s'identifier (par exemple en se présentant à un point de vente)."

L'utilisation d'itsme requiert d'abord qu'un client suive préalablement une procédure d'enregistrement. Sans cet enregistrement, le client ne peut pas passer une commande instantanément. En outre, il y a également des clients pour lesquels *itsme* n'est pas accessible, par exemple ceux qui possèdent une identité étrangère. Avec la reconnaissance faciale, l'obstacle pour les clients est très faible et cela donne aux clients facilement accès aux moyens de communication tout en ayant une identification fiable. Cela offre aux clients qui sont moins familiarisés avec le monde numérique la possibilité de s'identifier via une procédure simple et intuitive.

L'opérateur doit offrir à l'abonné au moins une manière alternative de s'identifier.

Une manière alternative de s'identifier est par exemple une des alternatives suivantes:

— en cas d'identification à distance, la personne peut être invitée à s'identifier dans un point de vente;

— si la méthode de comparaison faciale est mise en place dans un point de vente, une méthode alternative serait que le point de vente lui-même (et plus l'outil de comparaison faciale) vérifie que la personne qui se présente correspond bien à la personne qui est reprise sur le document d'identification (procédure manuelle);

— en cas d'identification à distance par un opérateur qui ne dispose pas de point de vente (uniquement vente de services en ligne), la personne peut être identifiée via un paiement en ligne (conservation de la référence de paiement).

Si un opérateur qui ne dispose pas de points de vente présente uniquement comme alternative pour s'identifier une identification en ligne via "*itsme*" ou via la lecture de la carte de l'eID, il ne s'agit pas d'une véritable alternative. En effet, dans ce cas, une personne qui ne dispose que d'un passeport international ne pourra pas s'identifier.

Le gouvernement estime qu'il ne serait pas opportun de freiner une innovation positive que constitue la comparaison faciale mais de bien l'encadrer. Les autorités et les opérateurs doivent pouvoir lutter à armes égales avec les fraudeurs et les criminels, qui ne vont pas hésiter à utiliser toute innovation technologique pour arriver à leurs fins.

manieren voor deze mensen om zich te identificeren (b.v. door naar een verkooppunt te gaan)."

Het gebruik van itsme vereist eerst dat een klant voorafgaandelijk een registratieprocedure moet doorlopen. Zonder deze registratie kan de klant niet onmiddellijk een order plaatsen. Bovendien zijn er ook klanten waarvoor *itsme* niet toegankelijk is, bijvoorbeeld voor klanten met een buitenlandse identiteit. De barrière voor de klant is bij gezichtsvergelijking zeer laag en geeft klanten gemakkelijk toegang tot communicatiemiddelen met tegelijkertijd een betrouwbare identificatie. Het geeft klanten die minder vertrouwd zijn met de digitale wereld de mogelijkheid om zich via een eenvoudige intuïtieve procedure te laten identificeren.

De operator moet de abonnee minstens een alternatieve manier aanbieden om zich te identificeren.

Een alternatieve manier om zich te identificeren kan bijvoorbeeld op de volgende wijzen:

— in geval van identificatie op afstand, kan de persoon uitgenodigd worden om zich te identificeren in een verkooppunt;

— indien een verkooppunt beschikt over de methode voor gezichtsvergelijking, zou een alternatieve methode erin kunnen bestaan dat het verkooppunt zelf (naast de tool voor gezichtsvergelijking) nagaat of de persoon die zich aanmeldt wel degelijk overeenstemt met de persoon vermeld op het identificatiedocument (manuele procedure);

— in geval van een identificatie op afstand door een operator die niet over een verkooppunt beschikt (enkel onlineverkoopdiensten), kan de persoon geïdentificeerd worden via een onlinebetaling (bewaring van de betalingsreferentie).

Indien een operator die niet over verkooppunten beschikt, enkel als alternatieve wijze voor identificatie een onlineidentificatie via "*itsme*" aanbiedt of via het lezen van de e-ID, gaat het niet over een daadwerkelijk alternatief. Indien een persoon niet over een internationaal paspoort beschikt, zal die persoon zich immers niet kunnen identificeren.

De regering meent dat het niet opportuun zou zijn om een positieve vernieuwing zoals gezichtsvergelijking af te remmen, maar dat die goed gereguleerd moet worden. De autoriteiten en de operatoren moeten met gelijke wapens kunnen strijden tegen fraudeurs en criminelen, die niet zullen aarzelen om elke technologische vernieuwing te gebruiken om hun doelstellingen te bereiken.

L'introduction du code PIN

La possibilité pour l'opérateur d'exiger l'introduction du code PIN lorsqu'un abonné s'identifie à l'aide de sa carte eID permet d'éviter que l'opérateur ou le point de vente ne doivent faire un contrôle de la correspondance entre le porteur de la carte et la carte elle-même et permet également de vérifier l'authenticité du document.

Au point 55 de son avis sur l'amendement, l'Autorité de protection des données indique ce qui suit:

"55. Le nouvel article 127 § 4, dernier alinéa, prévoit que "Lorsque l'abonné s'identifie à l'aide d'une carte d'identité électronique belge et que l'opérateur n'a pas mis en oeuvre la méthode de comparaison faciale visée à l'alinéa 3, l'opérateur peut demander à l'abonné l'introduction du code PIN". Au vu des considérations qui précèdent, il convient […] de remplacer le mot "peut" par le mot "doit". En effet, si l'objectif est de veiller à ce que les données d'identification collectées soient fiables, il est pertinent d'exiger systématiquement que les personnes qui présentent leur carte d'identité électronique s'authentifie au moyen du code pin."

Le gouvernement encourage les points de vente à demander à l'abonné d'introduire le code PIN lorsqu'il s'identifie à l'aide d'une carte eID mais estime que rendre l'introduction du code PIN obligatoire est disproportionné.

D'abord, cela compliquerait l'obligation pour les abonnés de s'identifier et il existe déjà plusieurs moyens pour s'assurer que l'identification à l'aide de l'eID est suffisamment fiable. Il n'est pas évident pour les clients d'utiliser le code PIN de l'eID belge. Beaucoup de clients ne connaissent plus leur code PIN et la procédure pour demander sa récupération requiert un certain nombre d'étapes auprès de la commune. L'utilisation du code PIN de l'eID belge n'est dès lors pas une solution pratique pour de nombreux clients, ce qui accroît l'obstacle pour la commande de services, et pousse les clients à renoncer à leur commande. Il existe des possibilités permettant aux opérateurs de contrôler si une eID a été déclarée perdue ou volée. Dans ce cas, l'identification peut être refusée. Une telle vérification accroît la fiabilité de l'identification. Dans les magasins, l'on vérifie via une inspection visuelle que le client correspond à la photo sur les documents d'identité. Dans les magasins, l'on peut également utiliser un lecteur eID, avec lequel la présence de la carte eID peut être contrôlée sur la base du certificat sur l'eID. L'introduction d'un code PIN

Invoering van de pincode

Door de mogelijkheid voor de operator om te eisen dat de pincode wordt ingetikt wanneer een abonnee zich aan de hand van zijn eID-kaart identificeert, kan de operator of het verkooppunt vermijden de overeenstemming te moeten nagaan tussen de kaarthouder en de kaart zelf en kan eveneens de authenticiteit van het document nagegaan worden.

In punt 55 van haar advies over het amendement wijst de Gegevensbeschermingsautoriteit op het volgende:

"55. het nieuwe artikel 127, § 4, laatste lid, bepaalt "Wanneer de abonnee zich aan de hand van een Belgische elektronische identiteitskaart identificeert en de operator de in het derde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast, kan de kan de operator aan de abonnee vragen om de pincode in te tikken". In het licht van bovenstaande overwegingen moeten de woorden "en de operator de in het derde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast" worden geschrapt en het woord "kan" moet worden verangen door het woord "moet"". Indien het de bedoeling is dat de verzamelde identificatiegegevens betrouwbaar zijn, moet immers systematisch worden geëist dat personen die hun elektronische identiteitskaart tonen, zich authenticeren door middel van de pincode."

De regering moedigt de verkooppunten aan om de abonnee te vragen om de pincode in te voeren wanneer hij/zij zich met behulp van een eID-kaart identificeert, maar meent dat het onevenredig is om de invoering van de pincode verplicht te maken.

In de eerste plaats zou dat de verplichting van de abonnees om zich te identificeren bemoeilijken en er bestaan al verschillende middelen om te waarborgen dat de identificatie met behulp van de eID voldoende betrouwbaar is. Het is voor klanten niet evident om de PIN code van de Belgische eID te gebruiken. Vele klanten kennen hun PIN code niet meer en de procedure om deze terug op te vragen vraagt een aantal stappen naar de gemeente. Het gebruik van de PIN code van de Belgische eID is daarom geen praktische oplossing voor vele klanten waardoor het de barrière voor het bestellen van diensten verhoogt en klanten afzien van hun order. Er zijn mogelijkheden voor operatoren om te controleren of een eID werd aangegeven als verloren of gestolen. In dat geval kan de identificatie geweigerd worden. Dergelijke verificatie verhoogt de betrouwbaarheid van de identificatie. In de winkels wordt via visuele inspectie gecontroleerd dat de klant overeenkomt met de foto op de identiteitsdocumenten. In de winkels kan ook gebruik gemaakt worden van een eID lezer waarmee de fysische aanwezigheid van de eID kaart kan

constituerait un obstacle qui n'est pas nécessaire pour les clients afin de passer une commande. Il existe également des possibilités en ligne pour scanner l'eID et contrôler que l'eID est physiquement présente. Un tel contrôle offre également une grande sécurité d'une identification fiable.

Par ailleurs, il n'est pas possible de demander l'introduction d'un code PIN pour une carte d'identité étrangère ou un passeport. Un fraudeur utilisera donc un faux passeport ou une fausse carte d'identité, plutôt qu'une eID (un faux document ou un eID volée ou perdue), pour s'identifier.

Paragraphe 5: méthode d'identification directe: documents d'identification admis pour les personnes physiques

Introduction

Pour répondre à l'arrêt de la Cour constitutionnelle du 18 novembre 2021, l'article 127 reprend dorénavant une liste de documents d'identification admis.

Dans le point B.8.4.1. de son arrêt précité, la Cour constitutionnelle indique que "Pour ce qui est des données d'identification et des documents d'identification concernés, l'article 127 de la loi attaquée dispose qu'il doit s'agir de documents comportant le numéro de registre national […]".

Ceci n'est cependant pas exigé dans l'article 127, dès lors que certains documents d'identité, tel un passeport international, sont admis pour s'identifier, sans que ces documents ne comprennent le numéro de registre national belge.

En principe, un Belge doit s'identifier en Belgique à l'aide de sa carte d'identité électronique belge et non à l'aide de son passeport international. De plus, il est plus difficile pour un opérateur de vérifier la fiabilité d'un passeport international que la fiabilité d'une carte d'identité belge. Cependant, on ne peut pas exclure que des Belges résidant à l'étranger disposent d'un passeport belge mais plus d'une carte d'identité belge. Il convient de permettre à ces personnes lors de leur visite en Belgique de souscrire à l'aide de leur passeport à des services de communications électroniques prépayés. Lorsque la carte d'identité électronique belge d'une personne a été volée ou perdue, cette personne pourra aussi utiliser son passeport belge pour s'identifier.

worden gecontroleerd op basis van het certificaat op de eID. Het invoeren van een PIN code zou een onnodige barrière opwerpen voor klanten om een bestelling te doen. Ook online zijn er mogelijkheden om de eID in te scannen en te controleren dat de eID fysisch aanwezig is. Dergelijke controle geeft ook een grote zekerheid van een betrouwbare identificatie.

Het is overigens niet mogelijk om de invoering van een pincode te vragen voor een buitenlandse identiteitskaart of een paspoort. Een fraudeur zal dus eerder een vals paspoort of een valse identiteitskaart gebruiken dan een eID (een vals document of een gestolen of verloren eID) om zich te identificeren.

Paragraaf 5: directe identificatiemethode: identificatiedocumenten die toegestaan zijn voor natuurlijke personen

Inleiding

Om te beantwoorden aan het arrest van het Grondwettelijk Hof van 18 november 2021 bevat artikel 127 voortaan een lijst van toegestane identificatiedocumenten.

In punt B.8.4.1. van zijn voormelde arrest zegt het Grondwettelijk Hof: "Wat de betrokken identificatiegegevens en identificatiedocumenten betreft, bepaalt artikel 127 van de bestreden wet dat het moet gaan om documenten die het rijksregisternummer bevatten [...]".

Dat wordt echter in artikel 127 niet geëist, aangezien bepaalde identificatiedocumenten, zoals een internationaal paspoort, toegestaan zijn om zich te identificeren, terwijl die documenten toch geen Belgisch rijksregisternummer bevatten.

In principe moet een Belg zich in België identificeren aan de hand van zijn Belgische elektronische identiteitskaart en niet door middel van zijn internationaal paspoort. Bovendien is het moeilijker voor een operator om de betrouwbaarheid van een internationaal paspoort te controleren dan de betrouwbaarheid van een Belgische identiteitskaart. Toch kan niet worden uitgesloten dat Belgen die in het buitenland verblijven, over een Belgisch paspoort beschikken maar niet langer over een Belgische identiteitskaart. Deze personen moeten bij hun bezoek aan België de mogelijkheid krijgen om aan de hand van hun paspoort in te tekenen op voorafbetaalde elektronischecommunicatiediensten. Wanneer de Belgische elektronische identiteitskaart van een persoon werd gestolen of verloren is gegaan, zal die persoon ook zijn Belgisch paspoort kunnen gebruiken om zich te identificeren.

L'annexe 12 est une attestation de remplacement ou de déclaration de perte, de vol ou de destruction d'une carte d'identité, d'une carte pour étrangers ou de tout autre document de séjour. D'une part, il y a un risque de falsification de ce type de document. Mais, d'autre part, refuser ce type de document signifierait qu'une personne ne pourrait pas souscrire à un service de communications électroniques lorsqu'elle ne dispose plus de son document d'identification et dès lors que de nombreuses personnes ne disposent pas d'un passeport belge.

Vu qu'il est possible qu'un document d'identification ait été oublié sur la liste et que si c'est le cas, une personne pourrait ne pas être en mesure de s'identifier auprès d'un opérateur afin de pouvoir bénéficier d'un service de communications électroniques, il est prévu que le Roi puisse compléter en urgence cette liste. L'arrêté royal devra cependant être confirmé par la Chambre des représentants.

La possibilité pour les opérateurs de refuser certains documents d'identification

Lors de la consultation publique sur les amendements, les opérateurs ont indiqué qu'admettre une trentaine de différents types de documents d'identification entraine des investissements supplémentaires pour eux (nombreux processus à développer) et qu'il est très difficile pour eux de garantir l'authenticité d'autant de documents.

Cependant, permettre aux opérateurs de refuser certains documents d'identification mènerait en pratique à une situation où des personnes vulnérables ne trouveraient aucun opérateur pour souscrire un produit télécom ou n'auraient plus de choix entre différents opérateurs. On peut s'attendre à ce qu'en pratique, tous les opérateurs qui disposent de points de vente refusent les mêmes types de documents d'identification (car représentant des coûts d'adaptation de processus sans que les titulaires de ces documents ne constituent une source de revenus suffisants pour l'opérateur).

Pour réconcilier les différents intérêts en jeu et tenir compte de la préoccupation des opérateurs, ces derniers peuvent refuser un document d'identification autre que l'eID pour autant qu'ils offrent à l'abonné une manière alternative de s'identifier (par exemple le paiement en ligne ou la vérification par une base de données externe) et que l'abonné puisse en pratique s'identifier à l'aide de cette manière alternative.

Bijlage 12 is een bewijs van vervanging of aangifte van verlies, diefstal of vernietiging van een identiteitskaart, een vreemdelingenkaart of elk ander verblijfsdocument. Enerzijds bestaat het risico van vervalsing van dit soort van document. Maar anderzijds zou het weigeren van dit soort van document inhouden dat een persoon niet zou kunnen intekenen op een elektronische-communicatiedienst wanneer deze niet langer over zijn of haar identificatiedocument beschikt en aangezien veel mensen niet over een Belgisch paspoort beschikken.

Vermits het mogelijk is dat een identificatiedocument vergeten wordt op de lijst en het, in dat geval kan gebeuren dat een persoon zich bij een operator niet kan identificeren om een elektronische-communicatiedienst te kunnen krijgen, is bepaald dat de Koning deze lijst met spoed kan aanvullen. Het koninklijk besluit zal evenwel bekrachtigd moet worden door de Kamer van volksvertegenwoordigers.

Mogelijkheid voor de operatoren om bepaalde identificatiedocumenten te weigeren

Bij de openbare raadpleging over de amendementen hebben de operatoren erop gewezen dat het aanvaarden van een dertigtal verschillende soorten identificatiedocumenten extra investeringen met zich meebrengt voor hen (tal van processen die moeten worden ontwikkeld) en dat het zeer moeilijk is voor hen om de authenticiteit van zoveel documenten te waarborgen.

De operatoren de mogelijkheid bieden bepaalde identificatiedocumenten te weigeren, zou in de praktijk evenwel tot een situatie leiden waar kwetsbare personen geen enkele operator zouden vinden om in te tekenen op een telecomproduct of geen keuze meer zouden hebben tussen verschillende operatoren. Het valt te verwachten dat in de praktijk alle operatoren die over verkooppunten beschikken dezelfde soorten identificatiedocumenten weigeren (aangezien zij kosten met zich meebrengen om processen aan te passen zonder dat de houders van die documenten een bron van voldoende inkomsten vormen voor de operator).

Om de verschillende belangen die op het spel staan, te verzoenen en rekening te houden met de bezorgdheid van de operatoren, kunnen die laatsten een ander identificatiedocument dan de eID weigeren voor zover zij de abonnee een alternatieve wijze bieden om zich te identificeren (bijvoorbeeld de onlinebetaling of de controle door een externe gegevensbank) en de abonnee zich in de praktijk kan identificeren aan de hand van die alternatieve wijze.

La copie de documents d'identification.

L'alinéa 3 reprend un principe déjà contenu dans l'article 127 actuel. L'opérateur ne peut pas conserver une copie de la carte d'identité électronique belge, dès lors qu'il est possible d'extraire de cette carte d'identité, de manière électronique et fiable, des données relatives à l'identité civile de la personne physique (en particulier le numéro de registre national). Par contre, les opérateurs sont moins familiers avec les cartes d'identité étrangères et les passeports étrangers, ce qui justifie qu'ils doivent conserver une copie de ces documents, en ce compris la photo figurant sur ce document.

Au point 57 de son avis sur les amendements, l'Autorité de protection des données indique qu'il faut supprimer l'obligation pour les opérateurs de conserver une copie des autres documents d'identification que l'eID, dès lors "que la prise de copie de document d'identité génère nécessairement un risque élevé pour les droits et libertés des personnes concernées au vu des conséquences potentiellement graves d'une fuite de données se rapportant à ces documents (fraude à l'identité)". Le Conseil d'État indique dans son avis "que ces documents ne peuvent être copiés que dans la mesure où il n'est pas possible d'extraire de manière électronique et sécurisée les données d'identification et pour autant que des mesures techniques soient prises par les opérateurs pour éviter toute reproduction conforme du document d'identité copié" (point 5).

Le gouvernement n'est pas d'accord avec la proposition de supprimer la copie du document d'identification autre que l'eID et ce pour les raisons suivantes.

Le risque de fraude est bien plus élevé pour les documents d'identification autres que l'eID et il n'est généralement pas possible de lire ces documents autres que l'eID pour en extraire de manière électronique et sécurisée les données. Par ailleurs, les opérateurs sont tenus d'accepter une trentaine de documents d'identification et il est difficile pour ses derniers d'assurer l'authenticité d'autant de documents (dont certains ne sont présentés que très rarement dans un point de vente).

La présentation d'un faux document d'identification ne pourra pas être détectée si l'opérateur ne conserve que des données d'identification, lorsque ces données paraissent crédibles.

Par contre, le fait que l'abonné a présenté un faux document pour s'identifier pourrait apparaitre d'un examen attentif par les autorités de la copie du document d'identification.

Kopie van identificatiedocumenten

Het derde lid neemt een principe over dat reeds in het huidige artikel 127 vervat is. De operator mag geen kopie van de Belgische elektronische identiteitskaart bewaren, aangezien het mogelijk is om uit die identiteitskaart, elektronisch en op betrouwbare wijze, gegevens op te halen met betrekking tot de burgerlijke identiteit van de natuurlijke persoon (in het bijzonder het rijksregisternummer). De operatoren zijn daarentegen minder vertrouwd met de buitenlandse identiteitskaarten en vreemdelingenpassen, waardoor het gerechtvaardigd is dat zij van die documenten een kopie moeten bewaren, met daarbij horend een foto op dit document.

De Gegevensbeschermingsautoriteit wijst in punt 57 van haar advies over de amendementen erop dat de verplichting voor de operatoren om een kopie van de andere identificatiedocumenten dan de eID te bewaren, moet worden geschrapt aangezien "het maken van kopieën van identiteitsdocumenten noodzakelijkerwijs een groot risico inhoudt voor de rechten en vrijheden van de betrokken personen, gezien de mogelijk ernstige gevolgen van een datalek met betrekking tot deze documenten (identiteitsfraude)". De Raad van State vermeldt in zijn advies "dat die documenten slechts gekopieerd mogen worden voor zover het niet mogelijk is om de identificatiegegevens op elektronisch en beveiligde wijze op te vragen en voor zover de operatoren technische maatregelen nemen om te voorkomen dat van het gekopieerde identiteitsdocument enige conforme reproductie gemaakt wordt" (punt 5).

De regering is het niet eens met het voorstel om de kopie van het andere identificatiedocument dan de eID te schrappen, zulks om de volgende redenen.

Het risico van fraude is veel groter voor de andere identificatiedocumenten dan de eID en over het algemeen is het niet mogelijk die andere documenten dan de eID te lezen om de gegevens elektronisch en op beveiligde wijze eruit te extraheren. De operatoren moeten overigens een dertigtal identificatiedocumenten aanvaarden en het is moeilijk voor die laatsten om de authenticiteit van zoveel documenten (waarvan bepaalde slechts zeer zelden in een verkooppunt worden overgelegd) te waarborgen.

De overlegging van een vals identificatiedocument kan niet worden opgespoord indien de operator enkel identificatiegegevens bewaart wanneer die gegevens betrouwbaar lijken te zijn.

Het gegeven dat de abonnee een vals document heeft overgelegd om zich te identificeren, zou evenwel aan het licht kunnen komen door een aandachtig onderzoek door de

Par ailleurs, ce document d'identification, même s'il est faux, permettra aux autorités de commencer une enquête (par exemple car plusieurs documents d'identification faux se ressemblent et dès lors que le document d'identification comprend généralement une photo de l'abonné).

La conservation d'une copie du document d'identification permet aussi parfois à l'opérateur de détecter lui-même une fraude.

Des erreurs d'encodage peuvent aussi survenir lorsque l'opérateur enregistre les données dans son système informatique. Seule la conservation de la copie du document d'identification permettra de détecter ces erreurs d'encodage et de les rectifier.

Conserver la copie du document d'identification donne aussi à l'IBPT la possibilité de contrôler que l'identification a bien été faite sur base d'un document d'identification admis par la loi.

En d'autres termes, conserver une copie du document d'identification permet d'augmenter la fiabilité de l'identification et de s'assurer que les données sont exactes et de qualité, conformément aux principes du RGPD.

L'obligation de prendre systématiquement une copie des documents d'identité (excepté l'eID) est déjà inscrite dans la loi depuis des années. Les opérateurs ont pris les mesures nécessaires pour adapter leurs systèmes afin de satisfaire à cette obligation. Les opérateurs demandent de la stabilité dans la réglementation.

Cependant, avec la détention obligatoire actuelle, les opérateurs ne voient pas de grands risques parce que les copies des documents d'identification sont conservées en sécurité dans une base de données uniquement accessible à l'équipe qui doit répondre aux questions des autorités. Des processus spécifiques ont été mis en place pour la conservation des documents d'identité pour satisfaire au contexte légal.

Comme le Conseil d'État l'indique dans son avis (point 9), "L'article 9, paragraphe 2, g), du RGPD semble pouvoir constituer la base sur laquelle la photo en question pourrait être conservée."

Cette disposition énonce:

"le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit

autoriteiten van de kopie van het identificatiedocument. Dat identificatiedocument zal de autoriteiten, hoewel het vals is, overigens de mogelijkheid bieden een onderzoek op te starten (bijvoorbeeld omdat verschillende valse identificatiedocumenten op elkaar lijken en aangezien het identificatiedocument over het algemeen een foto van de abonnee bevat).

Het bewaren van een kopie van het identificatiedocument biedt de operator ook soms de mogelijkheid zelf fraude op te sporen.

Coderingsfouten kunnen ook voorkomen wanneer de operator de gegevens in zijn computersysteem registreert. Enkel de bewaring van de kopie van het identificatiedocument zal de mogelijkheid bieden die coderingsfouten op te sporen en ze te verbeteren.

De kopie van het identificatiedocument bewaren, biedt ook het BIPT de mogelijkheid te controleren dat de identificatie wel degelijk gebeurde aan de hand van een door de wet aanvaard identificatiedocument.

Een kopie van het identificatiedocument bewaren, maakt het met andere woorden mogelijk de betrouwbaarheid van de identificatie te verhogen en zich ervan te vergewissen dat de gegevens juist en kwaliteitsvol zijn, overeenkomstig de beginselen van de AVG.

De verplichting om systematisch een kopie te nemen van de identificatiedocumenten (behalve de eID) staat al verschillende jaren in de wet. De operatoren hebben de nodige maatregelen genomen om hun systemen aan te passen om zodanig aan deze verplichting te voldoen. De operatoren vragen stabiliteit in de regelgeving.

De operatoren zien met de huidige verplichte bewaring evenwel geen grote risico omdat de kopieën van de identificatiedocumenten veilig bewaard worden in een database die enkel toegankelijk is voor het team dat vragen van autoriteiten moet beantwoorden. Er werden specifieke processen opgesteld voor de bewaring van de identiteitsdocumenten om aan de wettelijke context te voldoen.

Zoals de Raad van State vermeldt in zijn advies (punt 9): "Artikel 9, lid 2, g), van de AVG lijkt de basis te kunnen vormen waarop de foto in kwestie zou kunnen worden bewaard."

In die bepaling is het volgende gesteld:

"de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk

d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée".

Au point 57 de son avis sur les amendements, l'Autorité de protection des données indique ce qui suit:

"Afin d'éviter toute prise de copie de la carte d'identité belge, il convient de mettre en place une solution technologique qui garantisse que les données d'identité du titulaire d'une carte d'identité électronique soient extraites en vue de leur insertion directe dans la base de données".

Une disposition a été insérée dans l'article 127 pour répondre à cette préoccupation.

Paragraphe 6: méthode d'identification directe: données d'identité civile

Alors que l'arrêté royal "cartes prépayées" oblige les opérateurs à conserver uniquement le numéro de registre national lorsque le document d'identification présenté est une carte d'identité électronique belge, le présent projet les oblige à conserver en plus le nom et le prénom de l'abonné et ce pour les raisons suivantes:

— L'article 107, § 4, de la loi télécom prévoit que "Les opérateurs concernés par une communication d'urgence vers un service d'urgence offrant de l'aide sur place, si nécessaire en se coordonnant entre eux, fournissent au PSAP le plus approprié, dès que l'appel leur parvient et gratuitement, les données d'identification de l'appelant." Selon l'article 2, 57°, de cette même loi, l'"identification de l'appelant" comprend "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'abonné et l'endroit où le terminal se situe au moment de l'appel". (c'est nous qui soulignons);

— Cela permet aussi qu'une demande d'une autorité envers un opérateur utilise comme critère de recherche le nom et le prénom de l'abonné et ne doive pas se baser sur le numéro de registre national, qui n'est pas nécessairement connu de l'autorité.

Le paragraphe 6, alinéa 2, qui suit l'avis de l'Autorité de protection des données sur les amendements de ne constituer qu'une seule liste de données, ne laisse pas aux opérateurs le

recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene".

De Gegevensbeschermingsautoriteit vermeldt in punt 57 van haar advies over de amendementen het volgende:

"Om te voorkomen dat de Belgische identiteitskaart wordt gekopieerd, moet [...] een technologische oplossing worden gevonden om ervoor te zorgen dat de identiteitsgegevens van de houder van een elektronische identiteitskaart worden geëxtraheerd om rechtstreeks te worden opgenomen in de databank".

In artikel 127 werd een bepaling ingevoegd om aan die bezorgdheid tegemoet te komen.

Paragraaf 6: directe identificatiemethode: gegevens van burgerlijke identiteit

Terwijl het koninklijk besluit "prepaid kaarten" de operatoren verplicht om enkel het rijksregisternummer te bewaren wanneer het voorgelegde identificatiedocument een Belgische elektronische identiteitskaart is, verplicht dit ontwerp de operatoren om bovendien de naam en voornaam van de abonnee te bewaren en wel om de volgende redenen:

— Artikel 107, § 4, van de telecomwet bepaalt: "De operatoren betrokken bij een noodcommunicatie naar een nooddienst die ter plaatse hulp biedt, leveren, indien nodig met onderlinge coördinatie, zodra ze de oproep ontvangen en gratis aan de meest geschikte PSAP de identificatiegegevens van de oproeper." Volgens artikel 2, 57°, van diezelfde wet omvat de "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 abonnee en de plaats waar het eindtoestel zich bevindt op het ogenblik van de oproep bepaalt". (wij onderlijnen);

— Dit maakt het ook mogelijk dat een verzoek van een autoriteit aan een operator als zoekcriterium de naam en voornaam van de abonnee gebruikt en zich niet moet baseren op het rijksregisternummer, dat niet noodzakelijk voor de autoriteit bekend is.

Paragraaf 6, tweede lid, dat het advies van de Gegevensbeschermingsautoriteit over de amendementen volgt om slechts één lijst van gegevens samen te stellen, laat de

choix de conserver les données visées dans ce paragraphe ou pas. Si une donnée est disponible en fonction d'une méthode d'identification directe, la donnée doit être conservée.

La photo n'est pas reprise dans les documents d'identification de l'abonné. Mais il convient de rappeler que la photo se trouve sur le document d'identification et que les opérateurs doivent conserver une copie de ce document, sauf pour ce qui concerne la carte d'identité électronique belge.

Dans la pratique, un opérateur peut identifier une personne en faisant un lien avec une identification déjà effectuée. Par exemple un enfant peut être identifié en faisant le lien avec un parent pour lequel des données d'identification fiables ont déjà été récoltées.

Dans le point B.8.4.1. de son arrêt du 18 novembre 2021, la Cour constitutionnelle indique que "[…] l'article 127 de la loi attaquée dispose […] que le numéro de registre national est une donnée à caractère personnel qui doit être collectée et traitée dans ce contexte".

En réalité, un opérateur ne doit collecter et conserver le numéro de registre national de son abonné que lorsque l'abonné s'identifie à l'aide d'un document d'identification qui comprend ce numéro (ex. la carte d'identité électronique belge).

Le paragraphe 6 de l'article 127 limite les données d'identification que les opérateurs peuvent conserver dans le cadre de la méthode d'identification directe. L'opérateur peut cependant conserver d'autres données pour d'autres finalités que l'identification de l'abonné au profit des autorités, pour autant que le RGPD l'y autorise.

Paragraphe 7: méthode d'identification directe: identification de l'abonné qui est une personne morale

L'article 9 de l'arrêté royal "cartes prépayées" prévoit que "Lorsqu'une carte prépayée est achetée par une personne physique ou morale, l'entreprise concernée collecte et vérifie selon une des méthodes d'identification valides l'identité de la personne physique qui demande l'activation de la carte." Le principe qui découle de cet article (lorsque l'abonné est une personne morale, l'opérateur identifie au moins une personne physique qui agit pour le compte de la personne morale) a été repris dans le paragraphe 7 de l'article 127. Ce même principe n'est pas repris pour les formules avec facturation ("*postpaid*"), étant donné que dans ce cas-là, l'opérateur a déjà un intérêt commercial significatif d'identifier la personne

operatoren niet de keuze de in die paragraaf bedoelde gegevens al dan niet te bewaren. Indien een gegeven beschikbaar is op grond van een directe identificatiemethode, moet het gegeven worden bewaard.

De foto wordt niet opgenomen in de identificatiedocumenten van de abonnee. Er moet evenwel op worden gewezen dat de foto zich op het identificatiedocument bevindt en dat de operatoren een kopie van dat document moeten bewaren, behalve voor wat de Belgische elektronische identiteitskaart betreft.

In de praktijk kan een operator een persoon identificeren door een link te leggen met een reeds uitgevoerde identificatie. Een kind kan bijvoorbeeld geïdentificeerd worden door de link te leggen met een ouder voor wie reeds betrouwbare identificatiegegevens zijn verzameld.

In punt B.8.4.1. van zijn arrest van 18 november 2021 vermeldt het Grondwettelijk Hof dat "[…] artikel 127 van de bestreden wet [bepaalt] […] dat het rijksregisternummer een persoonsgegeven is dat in dit verband dient te worden verzameld en verwerkt".

In werkelijkheid moet een operator het rijksregisternummer van zijn abonnee maar verzamelen en bewaren wanneer de abonnee zich identificeert aan de hand van een identificatiedocument waarop dat nummer vermeld is (bijv. Belgische elektronische identiteitskaart).

Artikel 127, paragraaf 6, beperkt de identificatiegegevens die de operatoren kunnen bewaren in het kader van de directe identificatiemethode. De operator kan evenwel andere gegevens bewaren voor andere doeleinden dan de identificatie van de abonnee ten gunste van de autoriteiten, voor zover de AVG hem daartoe machtigt.

Paragraaf 7: directe identificatiemethode: identificatie van de abonnee die een rechtspersoon is

Artikel 9 van het koninklijk besluit "prepaid kaarten" bepaalt: "Wanneer een voorafbetaalde kaart wordt gekocht door een natuurlijke persoon of een rechtspersoon, verzamelt en verifieert de betrokken onderneming volgens één van de geldige identificatiemethodes de identiteit van de natuurlijke persoon die de activering van de kaart vraagt." Het principe dat uit dat artikel voortvloeit (wanneer de abonnee een rechtspersoon is, identificeert de operator minstens een natuurlijke persoon die voor rekening van de rechtspersoon optreedt) is overgenomen in paragraaf 7 van artikel 127. Datzelfde principe wordt niet overgenomen voor de formules met facturering ("postpaid"), aangezien de operator in dat geval reeds een

morale (en particulier en vue de lancer une procédure en justice si la personne morale ne paie pas ses factures).

Paragraphe 8: délégations au Roi pour fixer les règles entourant les méthodes d'identification directe

Le paragraphe 8 de l'article 127 comprend des délégations au Roi. Ces délégations au Roi forment en partie la base juridique de l'arrêté royal "carte prépayée". En effet, cet arrêté royal fait une liste exhaustive des méthodes d'identification directes que les opérateurs peuvent utiliser pour identifier les abonnés de cartes prépayées. Par ailleurs, la méthode d'identification visée à l'article 19 de cet arrêté royal (la vérification par un moyen de communication électronique) est soumise à une autorisation préalable du ministre des Télécoms et du ministre de la Justice. Finalement, cet arrêté royal impose des obligations tant aux opérateurs qu'aux utilisateurs finaux.

Lors de la consultation publique relative au présent amendement, certains opérateurs ont indiqué qu'il y avait un risque de recoupement entre l'article 127 de la loi télécom d'une part et l'arrêté royal carte prépayée d'autre part. Afin d'éviter ces recoupements, cet arrêté royal sera revu pour y supprimer les éléments qui sont dorénavant directement traités dans l'article 127 de la loi télécom.

Dans son arrêt du 18 novembre 2021, la Cour constitutionnelle a indiqué que l'article 127 devait déterminer les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. Elle n'a cependant pas jugé que toutes les règles entourant une méthode d'identification de l'abonné devaient être reprises dans la loi. Le faire rendrait la loi très complexe. Cela reviendrait à devoir reprendre le contenu de l'arrêté royal "cartes prépayées" dans la loi. Cet arrêté royal précise d'autres éléments que les données d'identification et les documents d'identité (par exemple l'utilisation obligatoire de check-doc pour ce qui concerne la carte d'identité électronique).

Paragraphe 9: identification de l'abonné par une méthode d'identification indirecte

Introduction

Dans le point 73 de son avis sur les amendements, l'Autorité de protection des données indique "que la qualité des données d'identification recueillies par le biais d'une méthode d'identification indirecte apparait incertaine et ne garantit

aanzienlijk commercieel belang heeft om de rechtspersoon te identificeren (in het bijzonder om een gerechtelijke procedure in te stellen als de rechtspersoon de rekeningen niet betaalt).

Paragraaf 8: delegaties aan de Koning om de regels inzake directe identificatiemethodes vast te stellen

Artikel 127, paragraaf 8, omvat delegaties aan de Koning. Die delegaties aan de Koning vormen gedeeltelijk de rechtsgrond van het koninklijk besluit "voorafbetaalde kaart". Dat koninklijk besluit voorziet immers in een exhaustieve lijst van de directe identificatiemethodes die de operatoren kunnen gebruiken om de abonnees van voorafbetaalde kaarten te identificeren. De identificatiemethode bedoeld in artikel 19 van dat koninklijk besluit (de verificatie via elektronisch communicatiemiddel) is overigens onderworpen aan een voorafgaande machtiging van de minister van Telecommunicatie en van de minister van Justitie. Ten slotte worden in dat koninklijk besluit verplichtingen opgelegd aan zowel de operatoren als de eindgebruikers.

Bij de openbare raadpleging over dit amendement hebben sommige operatoren erop gewezen dat er een risico van overlapping was tussen artikel 127 van de telecomwet en het koninklijk besluit voorafbetaalde kaart. Om die overlappingen te voorkomen, zal dat koninklijk besluit worden herzien met het oog op de schrapping erin van de elementen die voortaan direct in artikel 127 van de telecomwet worden behandeld.

In zijn arrest van 18 november 2021 heeft het Grondwettelijk Hof aangegeven dat artikel 127 de identificatiegegevens die worden verzameld en verwerkt en de identificatiedocumenten die in aanmerking komen, moest bepalen. Het heeft evenwel niet geoordeeld dat alle regels inzake een methode voor de identificatie van de abonnee in de wet opgenomen moesten worden. Door dat te doen zou de wet heel ingewikkeld worden. Dit zou erop neerkomen dat de inhoud van het koninklijk besluit "prepaid kaarten" in de wet opgenomen zou moeten worden. Dat koninklijk besluit preciseert andere elementen buiten de identificatiegegevens en de identificatiedocumenten (bijvoorbeeld het verplichte gebruik van check-doc wat de elektronische identiteitskaart betreft).

Paragraaf 9: identificatie van de abonnee via een indirecte identificatiemethode

Inleiding

De Gegevensbeschermingsautoriteit wijst in punt 73 van haar advies over de amendementen erop "dat de kwaliteit van de identificatiegegevens die door middel van een indirecte identificatiemethode worden verzameld, onzeker lijkt en niet

pas que la personne qui sera identifiée est bien la personne qui aura effectivement utilisé le service de communications électroniques."

Pour les autorités, le fait de disposer d'informations, même si la fiabilité de ces informations n'est pas absolue, est mieux que de disposer d'aucune information (aucune enquête n'est alors possible). Dans ce cas, les autorités judiciaires et les services de renseignement et de sécurité n'ont pas de choix que de mettre en œuvre des mesures plus attentatoires à la vie privée (perquisition du domicile ou de matériel informatique, interception du contenu des communications électroniques, etc.).

Les données d'identifications permettent de démarrer une enquête (identifier les suspects et éliminer certaines personnes) mais ne sont pas les seuls éléments pour fonder une condamnation. Ces éléments doivent être corroborés avec d'autres éléments. Il convient également de rappeler que dans un procès pénal, ce sont les autorités judiciaires qui ont la charge de la preuve. Il est dès lors nécessaire que ces autorités disposent des éléments pertinents pour apporter cette preuve.

Par ailleurs, dans bien des cas, un opérateur identifiera l'abonné (celui qui conclut le contrat avec l'opérateur) et non l'utilisateur effectif du service. Il reviendra aux autorités, sur base de leur enquête, de retrouver l'utilisateur effectif du service.

Au point 74 de son avis relatif à l'amendement n° 6 (remplacement de l'article 127 de la loi télécom), l'Autorité de protection des données indique que "L'amendement étend toutefois les catégories d'autorités qui peuvent avoir recours à ces méthodes d'identification indirecte. Jusqu'à présent, seuls les services de renseignements et de sécurité pouvaient, sans équivoque, identifier un utilisateur final à partir de la référence de l'opération de paiement".

Toutefois, cet amendement n'étend pas les catégories d'autorités qui peuvent avoir recours à ces méthodes d'identification indirecte. La question des autorités qui peuvent obtenir des données des opérateurs est traitée dans l'article 127/1 en projet de la loi télécom ainsi que dans les lois organiques qui permettent aux autorités d'obtenir des données des opérateurs. Pour ce qui concerne la question de la possibilité pour les autorités judiciaires d'identifier un utilisateur final à partir de la référence de l'opération de paiement, il est renvoyé à l'amendement visant à modifier le Code d'instruction criminelle.

garandeert dat de persoon die zal worden geïdentificeerd, de persoon is die daadwerkelijk van de elektronische-communicatiedienst gebruik zal hebben gemaakt."

Voor de autoriteiten is het beter over informatie te beschikken, zelfs indien die informatie niet volstrekt betrouwbaar is, dan over helemaal geen informatie te beschikken (dan is geen enkel onderzoek mogelijk). In dat geval hebben de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten geen andere keuze dan maatregelen ten uitvoer te leggen die de persoonlijke levenssfeer meer aantasten (huiszoeking van de woonplaats of van computermateriaal, onderschepping van de inhoud van de elektronische communicatie, enz.).

De identificatiegegevens bieden de mogelijkheid een onderzoek op te starten (de verdachten identificeren en bepaalde personen elimineren) maar dit zijn niet de enige elementen om een veroordeling op te baseren. Die elementen moeten worden gestaafd met andere elementen. Er moet tevens op worden gewezen dat in een strafproces de gerechtelijke autoriteiten de bewijslast hebben. Het is dan ook noodzakelijk dat die autoriteiten over de relevante elementen beschikken om dat bewijs te leveren.

In tal van gevallen zal een operator overigens de abonnee (diegene die het contract sluit met de operator) en niet de daadwerkelijke gebruiker van de dienst identificeren. Het is aan de autoriteiten om op grond van hun onderzoek de daadwerkelijke gebruiker van de dienst te vinden.

De Gegevensbeschermingsautoriteit wijst in punt 74 van haar advies over amendement nr. 6 (vervanging van artikel 127 van de telecomwet) op het volgende: "Het amendement breidt echter de categorieën van autoriteiten uit die deze indirecte identificatiemethoden kunnen gebruiken. Tot nu toe konden alleen inlichtingendiensten en veiligheidsdiensten een eindgebruiker ondubbelzinnig identificeren aan de hand van de kenmerken van de betalingstransactie".

Dat amendement breidt evenwel niet de categorieën van autoriteiten uit die deze indirecte identificatiemethoden kunnen gebruiken. De aangelegenheid van de autoriteiten die gegevens van de operatoren kunnen verkrijgen, wordt behandeld in het ontworpen artikel 127/1 van de telecomwet alsmede in de organieke wetten die de autoriteiten de mogelijkheid bieden gegevens van de operatoren te verkrijgen. Met betrekking tot de mogelijkheid voor de gerechtelijke autoriteiten om een eindgebruiker te identificeren aan de hand van de kenmerken van de betalingstransactie wordt verwezen naar het amendement dat ertoe strekt het Wetboek van Strafvordering te wijzigen.

1° Conservation de l'adresse IP

Cette méthode d'identification est particulièrement utile pour les opérateurs qui offrent des services gratuits (OTT). Les données qui doivent être conservées ainsi que leur durée de conservation sont fixés à l'article 126 de la loi télécom. En d'autres termes, l'article 127 n'impose pas aux OTT d'obligation supplémentaire par rapport aux obligations qui leur sont déjà imposées dans le cadre de l'article 126 de la loi télécom.

2° Conservation du numéro de téléphone

Cette méthode d'identification est particulièrement utile pour les opérateurs qui offrent des services wifi (gratuits ou payants).

3° Conservation de la référence de paiement bancaire

L'alinéa 1er, 3°, correspond à la méthode d'identification prévue à l'article 17 de l'arrêté royal "cartes prépayées".

Il convient de rappeler que les données d'identité civile sont considérées par la Cour de Justice de l'Union européenne comme des données non sensibles, dès lors qu'elles ne fournissent pas d'information sur une communication électronique. Il en va de même des références du paiement, qui permettent uniquement de retrouver l'identité civile. Comme il ne s'agit pas de données sensibles, le Conseil d'État français a jugé qu'"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 données relatives aux paiements" (arrêt du 21/04/2021, n° 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres, point 36).

Par ailleurs, les données de paiement permettent aussi de vérifier l'exactitude des données d'identité civile qui sont conservées par l'opérateur.

Dans le cadre de l'identification de l'abonné par la référence de paiement bancaire, la seule donnée fiable est cette référence. Les données qui sont communiquées par l'abonné à l'opérateur (son nom, son prénom, l'adresse de son domicile et sa date de naissance) ne sont pas fiables. Il reviendra aux autorités (et non aux opérateurs) de s'adresser aux institutions bancaires, afin d'obtenir l'identité de l'abonné.

Au point 76 de son avis, l'Autorité de protection des données indique qu'"à propos de la collecte de données en cas de paiement électronique en ligne, l'Autorité constate que la

1° Bewaring van het IP-adres

Deze identificatiemethode is bijzonder nuttig voor de operatoren die gratis diensten aanbieden (OTT). De gegevens die moeten worden bewaard en de bewaartermijn ervan worden vastgelegd in artikel 126 van de telecomwet. Met andere woorden, artikel 127 legt de OTT geen extra verplichting op ten aanzien van de verplichtingen die hen reeds worden opgelegd in het kader van artikel 126 van de telecomwet.

2° Bewaring van het telefoonnummer

Deze identificatiemethode is bijzonder nuttig voor de operatoren die wifidiensten aanbieden (gratis of betalend).

3° Bewaring van de referentie van de betaling via de bank

Het eerste lid, 3°, komt overeen met de identificatiemethode die bepaald is in artikel 17 van het koninklijk besluit "prepaid kaarten".

Er dient aan te worden herinnerd dat de gegevens van burgerlijke identiteit door het Hof van Justitie van de Europese Unie worden beschouwd als niet-gevoelige gegevens, aangezien ze nu eenmaal geen informatie geven over een elektronische communicatie. Hetzelfde geldt voor de referenties van de betaling waarmee het enkel mogelijk is om de burgerlijke identiteit terug te vinden. Aangezien het niet om gevoelige gegevens gaat heeft de Franse Conseil d'État geoordeeld dat "uit de richtlijn van 12 juli 2002 en de AVG duidelijk blijkt dat zij zich niet verzetten tegen een algemene en ongedifferentieerde bewaring gedurende een jaar van de betalingsgegevens" (arrest van 21/04/2021, nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK e.a., punt 36).

Bovendien is het aan de hand van de betalingsgegevens ook mogelijk om de juistheid van de gegevens van burgerlijke identiteit die door de operator worden bewaard, na te gaan.

In het kader van de identificatie van de abonnee door de referentie van de betaling via de bank is die referentie het enige betrouwbare gegeven. De gegevens die de abonnee aan de operator meedeelt (zijn naam, zijn voornaam, het adres van zijn woonplaats en zijn geboortedatum), zijn niet betrouwbaar. De autoriteiten (en niet de operatoren) moeten een beroep doen op de bankinstellingen om de identiteit van de abonnee te verkrijgen.

De Gegevensbeschermingsautoriteit wijst in punt 76 van haar advies erop dat "de Autoriteit met betrekking tot het verzamelen van gegevens in geval van online elektronische

collecte de la date et du lieu de naissance va au-delà de ce qui est nécessaire pour atteindre la finalité d'identification indirecte et est dès lors contraire à l'article 5.1.c) du RGPD. L'amendement sera revu afin de supprimer l'obligation de collecter ces deux données."

Le lieu de naissance a été supprimé. La date de naissance permettra aussi de distinguer des homonymes. Il est également demandé aux abonnés d'introduire l'adresse de leur domicile. Cela permettra aux autorités de vérifier si les données introduites par l'abonné sont crédibles ou non et pourrait être une information utile pour les services d'urgence offrant de l'aide à distance lors d'un appel vers ces services.

4° L'identification de l'abonné par l'enregistrement du numéro de châssis du véhicule

Cette méthode d'identification a été introduite à la demande des opérateurs et est une méthode pratique tant pour les opérateurs que pour les autorités.

5 °Centres fermés et les lieux d'hébergement

L'alinéa 1er, 5°, reprend dans la loi une solution qui a été trouvée pour les étrangers qui résident dans des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers. Cette solution a été mise en place par l'arrêté ministériel du 31 août 2017 désignant en tant qu'autorité publique l'Office des étrangers du SPF Intérieur conformément à l'article 9, alinéa 2, de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée (*Moniteur belge* 11/09/2017).

Ce sont les centres fermés et les lieux d'hébergement qui identifient leurs résidents et qui fournissent à l'opérateur certaines données. Sur base des informations reçues de l'opérateur, les autorités judiciaires pourront s'adresser au centre fermé ou au lieu d'hébergement, pour obtenir plus d'information sur l'identité de l'abonné.

Il convient de noter qu'un opérateur n'a pas d'obligation d'offrir des services de communications électroniques (par exemple des cartes prépayées) dans un centre fermé.

betaling op[merkt] dat het verzamelen van geboortedatum en –plaats verder gaat dan wat nodig is om het doel van indirecte identificatie te verwezenlijken en derhalve in strijd is met artikel 5.1.c) van de AVG. Het amendement zal worden herzien om de verplichting tot het verzamelen van deze twee gegevens te schrappen."

De geboorteplaats werd geschrapt. De geboortedatum zal ook de mogelijkheid bieden homoniemen te onderscheiden. De abonnees worden ook gevraagd het adres van hun woonplaats in te voeren. Dat biedt de autoriteiten de mogelijkheid te controleren of de door de abonnee ingevoerde gegevens al dan niet geloofwaardig zijn en dat zou nuttige informatie kunnen zijn voor de nooddiensten die hulp op afstand bieden bij een oproep naar die diensten.

4° Identificatie van de abonnee door de registratie van het chassisnummer van het voertuig

Deze identificatiemethode werd ingevoerd op verzoek van de operatoren en is zowel voor de operatoren als voor de autoriteiten een praktische methode.

5° Gesloten centra en woonunits

Het tweede lid, 5°, neemt in de wet een oplossing over die gevonden is voor vreemdelingen die verblijven in gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen. Deze oplossing is ingevoerd door het ministerieel besluit van 31 augustus 2017 waarbij de FOD Binnenlandse zaken, Dienst Vreemdelingenzaken, wordt aangewezen als overheid overeenkomstig artikel 9, tweede lid, van het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart (*Belgisch Staatsblad* 11/09/2017).

Het zijn de gesloten centra en de woonunits die hun bewoners identificeren en die bepaalde gegevens aan de operator verstrekken. Op basis van de informatie die ontvangen is van de operator zullen de gerechtelijke autoriteiten zich kunnen wenden tot het gesloten centrum of de woonunit om meer informatie te krijgen over de identiteit van de abonnee.

Er moet worden opgemerkt dat een operator niet verplicht is elektronische-communicatiediensten (bijvoorbeeld voorafbetaalde kaarten) aan te bieden in een gesloten centrum.

6° Facilitation par une autre personne morale qu'un centre fermé ou un lieu d'hébergement de la souscription à un service de communications électroniques

Des solutions pratiques se sont mises en place pour permettre à des personnes physiques fragiles d'accéder aux services de communications électroniques. Ces solutions consistent à ce qu'une personne morale facilite la souscription à un service de communications électroniques d'un opérateur au nom et pour le compte d'une personne physique. Cette personne morale peut être par exemple un hôpital (qui agit pour ses patients de longue durée), une maison de retraite (qui agit pour ses retraités), un CPAS (qui agit pour les personnes qu'il aide), une ASBL (qui aide des personnes dans la rue). Cette disposition ne vise donc pas des abonnements qui seraient conclus par exemple par un employeur pour ses employés ou par une université pour ses étudiants ou une identification effectuée à l'aide d'informations détenues par une banque.

Cette personne morale devra s'identifier auprès de l'opérateur mais l'article 127 ne fixe pas les modalités de l'identification de cette personne morale, sauf si elle souscrit à un service de communications électroniques mobile fourni sur la base d'une carte prépayée. Dans ce cas, une personne physique qui agit pour le compte de la personne morale devra être identifiée conformément au paragraphe 7 de l'article 127.

C'est la personne morale qui agit pour le compte de la personne physique qui est responsable de la correcte identification de la personne physique. La responsabilité de l'opérateur est de correctement identifier la personne morale. En principe, la personne morale devra identifier la personne physique à l'aide d'un document d'identification visé au paragraphe 5 de l'article 127. L'agrément ministériel que devra obtenir la personne morale pourra cependant apporter des dérogations en la matière.

Pour éviter toute dérive, en principe, les obligations de la personne morale sont les mêmes que celles applicables au point de vente. Cette méthode d'identification n'est acceptée que pour autant que la personne morale soit en mesure d'identifier avec certitude les abonnés.

Au point 82 de son avis, l'Autorité de protection des données indique ce qui suit:

"La quatrième obligation consiste à fournir à l'opérateur une copie du document d'identification des abonnés, sauf lorsqu'il s'agit de la carte d'identité électronique belge, conformément au paragraphe 5, alinéa 3. Pour une identité

6° Vergemakkelijking door een andere rechtspersoon dan een gesloten centrum of een woonunit voor het intekenen op een elektronische-communicatiedienst

Er zijn praktische oplossingen ingevoerd om kwetsbare natuurlijke personen de mogelijkheid te bieden toegang te hebben tot de elektronische-communicatiediensten. Deze oplossingen bestaan erin dat een rechtspersoon het intekenen op een elektronische-communicatiedienst van een operator in naam en voor rekening van een natuurlijke persoon vergemakkelijkt. Die rechtspersoon kan bijvoorbeeld een ziekenhuis zijn (dat optreedt voor de patiënten die er langdurig verblijven), een rusthuis (dat optreedt voor de gepensioneerden ervan), een OCMW (dat optreedt voor de personen die het helpt), een vzw (die personen op straat helpt). Die bepaling beoogt dan ook geen abonnementen die zouden worden afgesloten bijvoorbeeld door een werkgever voor zijn werknemers of door een universiteit voor haar studenten of een identificatie verricht met behulp van informatie waarover een bank beschikt.

Die rechtspersoon zal zich bij de operator moeten identificeren maar in artikel 127 worden de nadere regels voor de identificatie van die rechtspersoon niet vastgelegd, tenzij hij intekent op een mobiele elektronische-communicatiedienst die wordt geleverd op basis van een voorafbetaalde kaart. In dat geval moet een natuurlijke persoon die handelt voor rekening van de rechtspersoon worden geïdentificeerd overeenkomstig artikel 127, paragraaf 7.

De rechtspersoon die handelt voor rekening van de natuurlijke persoon is verantwoordelijk voor de correcte identificatie van de natuurlijke persoon. De operator is verantwoordelijk voor de correcte identificatie van de rechtspersoon. In beginsel moet de rechtspersoon de natuurlijke persoon identificeren aan de hand van een identificatiedocument bedoeld in artikel 127, paragraaf 5. De ministeriële erkenning die de rechtspersoon moet verkrijgen, kan evenwel afwijkingen ter zake aanbrengen.

Om verwarring te voorkomen zijn de verplichtingen van de rechtspersoon, in principe, dezelfde als die die op de verkooppunten toepasselijk zijn. Deze identificatiemethode wordt enkel aanvaard voor zover de rechtspersoon in staat is met zekerheid de abonnees te identificeren.

De Gegevensbeschermingsautoriteit stelt in punt 82 van haar advies het volgende:

"De vierde verplichting bestaat uit het verstrekken aan "de operator (van) een kopie van het identificatiedocument van de abonnees, behalve wanneer het gaat om de Belgische elektronische identiteitskaart, conform paragraaf 5, derde lid".

de motifs à ceux exprimés lors de l'examen de l'article 127 § 5, alinéa 3, l'Autorité estime que cette quatrième obligation doit être supprimée."

Ce point de l'avis ne peut être suivi, pour les mêmes motifs que ceux qui justifient que le point de vente de l'opérateur doit collecter une copie du document d'identification autre que l'eID. Cette personne morale joue un rôle similaire à un point de vente. Par contre, la copie du document d'identification ne sera pas fournie à l'opérateur mais conservée par la personne morale. Dès lors, si nécessaire, les autorités s'adresseront à la personne morale pour obtenir plus d'informations et cette copie.

Une autre situation que celle visée à l'article 127, § 9, est souscription par une personne physique à un service de communications électroniques pour le compte d'une autre personne physique (son partenaire dans un couple, un enfant ou un parent, une personne malade, etc.)..

Généralement, ce type d'identification se fera sur base d'une méthode d'identification directe. Dans tous les cas, il faut que l'identification par l'opérateur soit fiable. Une identification fiable de la personne pour le compte de laquelle la souscription est faite ne sera pas toujours possible dès lors que cette personne ne se présente pas dans un point de vente de l'opérateur. Dans ce cas, l'opérateur pourra identifier de manière fiable la personne physique qui représente la personne absente. L'opérateur peut aussi identifier les deux personnes (tant la personne physique qui prend contact avec lui que la personne physique au nom de laquelle la souscription est faite).

Il convient cependant de tenir compte que l'article 5 de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée restreint la possibilité pour une personne physique qui s'identifie auprès de l'opérateur de céder à un tiers une carte prépayée active (ceci est cependant permis au sein de la famille).

Délégation au Roi

Une délégation au Roi est nécessaire pour pouvoir préciser ces méthodes d'identification indirecte. Ainsi, pour ce qui concerne l'identification par une méthode de paiement (alinéa 1er, 3°), l'article 17 de l'arrêté royal "cartes prépayées" fixe certaines conditions.

Om dezelfde redenen als die welke werden aangevoerd bij de beoordeling van artikel 127, § 5, 3e lid, is de Autoriteit van mening dat deze vierde verplichting moet worden geschrapt."

Dit punt van het advies kan niet worden gevolgd om dezelfde redenen als deze die verantwoorden dat het verkooppunt van de operator een kopie van het andere identificatiedocument dan de eID moet opvragen. Die rechtspersoon speelt een soortgelijke rol als een verkooppunt. De kopie van het identificatiedocument wordt evenwel niet aan de operator verstrekt maar wordt door de rechtspersoon bewaard. Indien nodig zullen de autoriteiten dan ook een beroep doen op de rechtspersoon om meer informatie en deze kopie te verkrijgen.

Een andere situatie dan deze bedoeld in artikel 127, § 9, is het intekenen door een natuurlijke persoon op een elektronische-communicatiedienst voor rekening van een andere natuurlijke persoon (zijn partner in een koppel, een kind of een ouder, een zieke persoon, enz.).

Over het algemeen gebeurt dit soort identificatie op grond van een directe identificatiemethode. In ieder geval moet de identificatie door de operator betrouwbaar zijn. Een betrouwbare identificatie van de persoon voor wiens rekening de intekening gebeurt, zal niet altijd mogelijk zijn aangezien deze persoon zich niet meldt in een verkooppunt van de operator. In dat geval kan de operator de natuurlijke persoon die de afwezige persoon vertegenwoordigt op betrouwbare wijze identificeren. De operator kan ook beide personen identificeren (zowel de natuurlijke persoon die contact met hem opneemt als de natuurlijke persoon in wiens naam de intekening gebeurt).

Er moet evenwel rekening mee gehouden worden dat in artikel 5 van het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart de mogelijkheid wordt beperkt voor een natuurlijke persoon die zich bij de operator identificeert om aan een derde een actieve voorafbetaalde kaart af te staan (dat is evenwel toegestaan binnen de familie).

Delegatie aan de Koning

Een delegatie aan de Koning is noodzakelijk om deze indirecte identificatiemethodes te kunnen preciseren. Wat de identificatie via een betaalmethode betreft (eerste lid, 3°) stelt artikel 17 van het koninklijk besluit "prepaid kaarten" aldus een aantal voorwaarden vast.

Paragraphe 10: identification de l'utilisateur habituel du service

L'alinéa 1er reprend une disposition de l'actuel article 127, § 1er, alinéa 3. Comme la Cour constitutionnelle l'indique dans son arrêt du 18 novembre 2021, "L'article 127, § 1er, alinéa 3, de la loi du 13 juin 2005 contient seulement la présomption réfragable selon laquelle cet utilisateur final est également celui qui utilise cette carte de téléphonie mobile. Le principe de légalité en matière pénale n'est pas applicable à une telle disposition." (B. 24.3). La Cour constitutionnelle ajoute ce qui suit: "B.26.2. La disposition attaquée n'établit dès lors pas de responsabilité pénale automatique ou de responsabilité objective de l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié en ce qui concerne l'utilisation qu'en fait un tiers. Elle remplit principalement une fonction d'avertissement, étant donné qu'elle rappelle la présomption de départ de toute enquête pénale et de toute enquête par les services de renseignement et de sécurité, à savoir la présomption selon laquelle c'est le propriétaire ou l'utilisateur habituel d'un objet qui l'a utilisé pour commettre l'infraction ou pour menacer la sécurité nationale. Les enquêteurs écartent cette présomption dès qu'elle est infirmée par les éléments de preuve recueillis."

Les délégations au Roi dans l'alinéa 2 sont nécessaires pour soutenir plusieurs règles de l'arrêté royal "cartes prépayées", à savoir la règle prévue à l'article 5 de cet arrêté royal qui limite la possibilité de céder une carte prépayée active à un tiers et l'obligation dans ce même article pour une personne morale qui a acquis des cartes prépayées de conserver "une liste actualisée permettant de faire le lien entre une carte prépayée et la personne physique à laquelle cette carte a été attribuée".

L'évolution montre qu'il est (de plus en plus) difficile pour les autorités d'exploiter les services de communications électroniques dans leurs enquêtes. Dans certains cas, un abonné parvient à s'identifier sous une fausse identité auprès de l'opérateur. La jurisprudence de la CJUE a fortement réduit la possibilité d'imposer aux opérateurs de conserver des métadonnées de manière généralisée et indifférenciée. Il est de plus en plus difficile pour les autorités judiciaires et les services de renseignement et de sécurité d'avoir accès au contenu des communications, vu la mise en place de la 5G et la généralisation de systèmes d'encryptage de bout en bout.

Il est donc essentiel de permettre aux autorités judiciaires et aux services de renseignements et de sécurité de

Paragraaf 10: identificatie van de effectieve gebruiker van de dienst

Het eerste lid neemt een bepaling over van het huidige artikel 127, § 1, derde lid. Het Grondwettelijk Hof geeft dat aan in zijn arrest van 18 november 2021: "Artikel 127, § 1, derde lid, van de wet van 13 juni 2005 bevat slechts het weerlegbare vermoeden dat die eindgebruiker ook degene is die deze belkaart gebruikt. Het strafrechtelijk wettigheidsbeginsel is niet van toepassing op een dergelijke bepaling." (B.24.3). Het Grondwettelijk Hof voegt het volgende daaraan toe: "B.26.2. De bestreden bepaling vestigt bijgevolg geen automatische strafrechtelijke verantwoordelijkheid of objectieve aansprakelijkheid van de geïdentificeerde eindgebruiker van een vooraf betaalde belkaart voor het gebruik dat een derde daarvan maakt. Zij heeft voornamelijk een waarschuwingsfunctie, aangezien zij het uitgangspunt van elk strafrechtelijk onderzoek en van elk onderzoek door de inlichtingen- en veiligheidsdiensten in herinnering brengt, namelijk het uitgangspunt dat de eigenaar of gewoonlijke gebruiker van een voorwerp vermoedelijk degene is die het heeft gebruikt om een misdrijf te plegen of om de nationale veiligheid te bedreigen. De onderzoekers verlaten dat uitgangspunt zodra het wordt ontkracht door de verzamelde bewijselementen."

De delegaties aan de Koning in het tweede lid zijn noodzakelijk om verschillende regels van het koninklijk besluit "prepaid kaarten" te ondersteunen, namelijk de regel van artikel 5 van dat koninklijk besluit, dat de mogelijkheid beperkt om een actieve voorafbetaalde kaart af te staan aan een derde en de verplichting in datzelfde artikel voor een rechtspersoon die voorafbetaalde kaarten verworven heeft, om een "geactualiseerde lijst [...] aan de hand waarvan het verband tussen een voorafbetaalde kaart en de natuurlijke persoon aan wie deze kaart werd toegewezen kan worden vastgesteld" te bewaren.

Uit de evolutie blijkt dat het (meer en meer) moeilijk is voor de autoriteiten om zich in hun onderzoeken de elektronischecommunicatiediensten ten nutte te maken. In sommige gevallen slaagt een abonnee erin om zich onder een valse identiteit bij de operator te identificeren. De jurisprudentie van het HvJ-EU heeft de mogelijkheid om de operatoren ertoe te verplichten op algemene en ongedifferentieerde wijze metagegevens te bewaren, sterk ingeperkt. Het is steeds moeilijker voor de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten om toegang te krijgen tot de inhoud van de communicatie, gelet op de invoering van 5G en de veralgemening van eind-tot-eindencryptie.

Het is dus van fundamenteel belang dat de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten voordeel

bénéficier des nouvelles opportunités qu'offrent l'évolution des technologies. C'est dans ce cadre qu'il est prévu que les opérateurs doivent conserver les numéros de cartes SIM qui sont intégrées dans des véhicules connectés en faisant le lien avec le numéro de châssis de ces véhicules. L'identification de la société avec laquelle l'opérateur a contracté (l'abonné) ne sera pas suffisante pour les autorités, qui chercheront à connaître l'identité de la personne physique ou morale qui est le propriétaire du véhicule et l'identité du conducteur principal de ce dernier.

Au point 86 de son avis sur les amendements, l'Autorité de protection des données remet en cause l'obligation pour l'opérateur de conserver le lien entre le numéro de châssis d'un véhicule et le numéro de carte SIM. De l'avis du gouvernement, l'objectif poursuivi est légitime (pouvoir identifier le conducteur habituel du véhicule) et la mesure présente un intérêt opérationnel très important dans les enquêtes judiciaires (par exemple à partir d'un véhicule impliqué dans une infraction grave, retrouver son auteur). Il n'y a pas de moyen moins intrusif dans la vie privée pour atteindre cet objectif.

— Dans son avis sur les amendements (point 12), le Conseil d'État indique "Le numéro d'identification d'un véhicule peut donner accès à de nombreuses informations sur le véhicule concerné et, de manière indirecte, sur son propriétaire. Eu égard à la finalité de l'identification du propriétaire du véhicule, il convient de prévoir que seule cette dernière information pourra être communiquée aux autorités dans le cadre de leurs missions."

Comme l'opérateur conserve le lien entre la carte SIM et le numéro de châssis, l'autorité judiciaire communiquera à l'opérateur le numéro de carte SIM pour obtenir le numéro de châssis ou le numéro de châssis du véhicule pour obtenir le numéro de carte SIM. C'est aux autorités et non à l'opérateur à accéder aux informations sur le véhicule et sur son propriétaire.

Paragraphe 11: sanction applicable et délégation au Roi

Ce paragraphe reprend le texte des paragraphes 4 et 5 de l'article 127 actuel.

kunnen halen uit de nieuwe kansen die door de evolutie van de technologieën worden geboden. In dat kader is net bepaald dat de operatoren de nummers van simkaarten die geïntegreerd zijn in geconnecteerde voertuigen bewaard moeten worden door de link te leggen met het chassisnummer van die voertuigen. De identificatie van de maatschappij waarmee de operator een contract heeft gesloten (de abonnee) zal niet volstaan voor de autoriteiten, die zullen proberen de identiteit te achterhalen van de natuurlijke persoon of rechtspersoon die de eigenaar van het voertuig is alsook de identiteit van de hoofdbestuurder van het voertuig.

De Gegevensbeschermingsautoriteit stelt in punt 86 van haar advies over de amendementen de verplichting voor de operator om het verband tussen het chassisnummer van een voertuig en het simkaartnummer te bewaren, opnieuw ter discussie. Volgens de regering is de nagestreefde doelstelling legitiem (de gebruikelijke bestuurder van het voertuig kunnen identificeren) en is de maatregel van zeer groot operationeel belang in de gerechtelijke onderzoeken (bijvoorbeeld aan de hand van een voertuig dat betrokken is bij een ernstig misdrijf de dader ervan terugvinden). Er is geen middel dat minder ingrijpend is in de persoonlijke levenssfeer om dat doel te bereiken.

— De Raad van State wijst in zijn advies over de amendementen (punt 12) op het volgende: "Het identificatienummer van een voertuig kan toegang verlenen tot heel wat gegevens over het desbetreffende voertuig en, onrechtstreeks, over zijn eigenaar. Gelet op het doel van de identificatie van de eigenaar van het voertuig, dient te worden bepaald dat enkel die laatste informatie aan de autoriteiten zal kunnen worden verstrekt in het kader van hun opdrachten."

Aangezien de operator het verband tussen de simkaart en het chassisnummer bewaart, zal de gerechtelijke autoriteit aan de operator het simkaartnummer meedelen om het chassisnummer te verkrijgen of het chassisnummer van het voertuig om het simkaartnummer te verkrijgen. Het is aan de autoriteiten en niet aan de operator om toegang te hebben tot de informatie over het voertuig en over de eigenaar ervan.

Paragraaf 11: toepasselijke sanctie en delegatie aan de Koning

Deze paragraaf neemt de tekst over van de paragrafen 4 en 5 van het huidige artikel 127.

Conclusions: Lien entre l'article 126 et 127 de la loi télécom

Lors de la consultation publique sur l'avant-projet de loi "conservation des données", les opérateurs se sont interrogés quant à la plus-value des obligations de conservation de données d'identification prévues par l'article 127, étant donné que les opérateurs conservent déjà de telles données sur base de l'article 126. L'utilité de l'article 127 réside dans le fait qu'il oblige les opérateurs à collecter des données alors que dans le cadre de l'article 126, un opérateur ne doit pas conserver de données s'il ne les génère ou ne les traite pas. Or, les données d'identité civile de l'abonné ne sont pas des données que l'opérateur génère. Dans un certain nombre de cas, le traitement de ces données n'est pas indispensable pour fournir le service de communications électroniques (par exemple, pour les services souscrits à l'aide d'une carte prépayée ou si aucun paiement n'est requis pour la fourniture du service).

Ceci peut être illustré par deux exemples. Le nom et le prénom de l'abonné sont repris dans les données qui sont conservées en vertu des deux articles. Mais dans le cadre de l'article 126, l'opérateur ne conservera ce nom et ce prénom que s'il les traite. Le nom et prénom seront collectés sans que la fiabilité de ces données ne soit nécessairement vérifiée. Par contre, dans le cadre d'une méthode d'identification directe en application de l'article 127, l'opérateur devra conserver le nom et le prénom de l'abonné qui est une personne physique et l'opérateur devra s'assurer que ces données sont fiables (ex. lecture de ces données de la carte d'identité électronique).

La référence de paiement bancaire est également une donnée qui est conservée en vertu des deux articles. Cependant, selon l'article 126, il s'agit d'une donnée que l'opérateur ne devra conserver que s'il la traite ou la génère et qu'une autorité consultera pour vérifier l'identité de l'abonné. Dans le cadre de l'article 127, l'opérateur conservera cette donnée dans le cadre d'une méthode d'identification indirecte qui repose sur la conservation de la référence de paiement pour permettre l'identification de l'abonné (et pas uniquement pour vérifier cette identité).

Conclusies: Link tussen artikel 126 en 127 van de telecomwet

Tijdens de openbare raadpleging over het voorontwerp van wet "gegevensbewaring" hebben de operatoren zich vragen gesteld bij de meerwaarde van de in artikel 127 vastgestelde verplichtingen om identificatiegegevens te bewaren, aangezien de operatoren reeds dergelijke gegevens bewaren op grond van artikel 126. Het nut van artikel 127 ligt in het feit dat het de operatoren verplicht om gegevens te verzamelen, terwijl in het kader van artikel 126, een operator geen gegevens moet bewaren als hij die niet genereert of ze niet verwerkt. Welnu, de gegevens van burgerlijke identiteit van de abonnee zijn geen gegevens die de operator genereert. In een aantal gevallen is de verwerking van deze gegevens niet absoluut noodzakelijk om de elektronische-communicatiedienst te verstrekken (bijvoorbeeld voor de diensten waarop is ingetekend via een prepaid kaart of wanneer voor de dienstverstrekking niet hoeft te worden betaald).

Dit kan met twee voorbeelden worden geïllustreerd. De naam en de voornaam van de abonnee maken deel uit van de gegevens die krachtens de twee artikelen worden bewaard. In het kader van artikel 126 zal de operator die naam en voornaam echter maar bewaren als hij die verwerkt. De naam en voornaam zullen worden verzameld zonder dat de betrouwbaarheid van deze gegevens noodzakelijkerwijs geverifieerd zal zijn. Daarentegen zal de operator in het kader van een directe identificatiemethode overeenkomstig artikel 127, de naam en de voornaam moeten bewaren van de abonnee die een natuurlijke persoon is en zal de operator moeten nagaan of deze gegevens betrouwbaar zijn (bijv. lezen van deze gegevens van de elektronische identiteitskaart).

De referentie van de betaling via de bank is ook een gegeven dat krachtens die twee artikelen wordt bewaard. Volgens artikel 126 gaat het evenwel om een gegeven dat de operator enkel zal moeten bewaren als hij het verwerkt of genereert en dat een autoriteit zal raadplegen om de identiteit van de abonnee te verifiëren. In het kader van artikel 127 zal de operator dat gegeven bewaren in het kader van een indirecte identificatiemethode die berust op de bewaring van de referentie van de betaling om de abonnee te kunnen identificeren (en niet alleen om die identiteit na te gaan).

On notera que l'adresse IP, qui est une des données qui est conservée en vertu de l'article 126 de la loi télécom, constitue la méthode d'identification indirecte visée à l'article 127, paragraphe 9, alinéa 1er, 1°.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Het IP-adres, dat een van de gegevens is dat wordt bewaard krachtens artikel 126 van de telecomwet, vormt de indirecte identificatiemethode bedoeld in artikel 127, paragraaf 9, eerste lid, 1°.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 7 **DU GOUVERNEMENT**

Art. 40 *(nouveau)*

Insérer un article 40, rédigé comme suit:

"Art. 40. Les modifications à l'article 127 ne s'applique que pour les identifications par les opérateurs des abonnés qui sont réalisées après l'entrée en vigueur de la présente loi.

L'article 127, § 5, alinéa 2, entre au vigueur deux ans après la publication de la présente loi.

Entre l'entrée en vigueur de la présente loi et la date fixée à l'alinéa 2, les opérateurs visés à l'article 127, § 5, alinéa 2, permettent aux abonnés de s'identifier à l'aide des documents visés à l'article 127, § 5, alinéa 2, 1° à 18°, 20° à 24°, 26°, 28° et 31°, dans le cadre d'au moins une méthode d'identification de leur choix.

Les opérateurs mettent en œuvre l'article 127, § 6, au plus tard 24 mois après la publication de la présente loi.

Lorsqu'un opérateur met en œuvre la méthode d'identification indirecte visée à l'article 127, § 9, alinéa 1er, 3°, il conserve les données qui y sont visées au plus tard 24 mois après la publication de la présente loi.

Les opérateurs mettent en œuvre l'article 127, § 9, alinéa 1er, 6°, et alinéa 2 au plus tard 24 mois après la publication de la présente loi. Les personnes morales visées par ces dispositions obtiennent l'agrément au plus tard 24 mois après la publication de la présente loi."

JUSTIFICATION

Tout d'abord, il convient d'indiquer que les modifications à l'article 127 de la loi télécom ne s'appliqueront que pour les identifications des abonnés qui sont réalisées après l'entrée en vigueur de la loi (les nouveaux contrats). En d'autres

Nr. 7 **VAN DE REGERING**

Art. 40 *(nieuw)*

Een artikel 40 invoegen, luidende:

"Art. 40. De wijzigingen van artikel 127 zijn enkel van toepassing voor de identificaties door de operatoren van de abonnees die gebeuren na de inwerkingtreding van deze wet.

Artikel 127, § 5, tweede lid, wordt van kracht twee jaar na de bekendmaking van deze wet.

Tussen de inwerkingtreding van deze wet en de in het tweede lid vastgestelde datum maken de in artikel 127, § 5, tweede lid, bedoelde operatoren het voor de abonnees mogelijk om zich te identificeren aan de hand van de documenten bedoeld in artikel 127, § 5, tweede lid, 1° tot 18°, 20° tot 24°, 26°, 28° en 31°, in het kader van minstens één identificatiemethode van hun keuze.

De operatoren leggen artikel 127, § 6, uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer.

Wanneer een operator de indirecte identificatiemethode bedoeld in artikel 127, § 9, eerste lid, 3°, ten uitvoer legt, bewaart hij de gegevens die erin worden beoogd uiterlijk 24 maanden na de bekendmaking van deze wet.

De operatoren leggen artikel 127, § 9, eerste lid, 6°, en tweede lid, uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer. De in deze bepalingen beoogde rechtspersonen verkrijgen de erkenning uiterlijk 24 maanden na de bekendmaking van deze wet."

VERANTWOORDING

Allereerst moet worden vermeld dat de wijzigingen in artikel 127 van de telecomwet enkel van toepassing zullen zijn voor de contracten die na de inwerkingtreding van de wet worden gesloten. De operatoren zullen met andere woorden

termes, les opérateurs ne devront pas procéder à une nouvelle identification des abonnés identifiés avant l'entrée en vigueur de la loi.

L'article 127 oblige les opérateurs à accepter toute une série de documents d'identité dans le cadre de l'identification de l'abonné. Dès lors que certains opérateurs n'acceptent pas tous ces documents d'identité en pratique, vu les difficultés d'enregistrer de manière automatique les données qui se trouvent sur ces documents dans leurs bases de données et vu certains doutes qui pourraient exister quant à la fiabilité de certains documents, un délai est donné aux opérateurs pour adapter leurs systèmes.

Pour ce qui concerne les données à collecter prévues par l'article 127, § 6, les opérateurs disposent de 24 mois après la publication de la loi pour mettre en œuvre les nouvelles exigences.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

de abonnees die reeds waren geïdentificeerd voor de inwerkingtreding van de wet, niet opnieuw moeten identificeren.

Artikel 127 verplicht de operatoren om een hele reeks identificatiedocumenten te aanvaarden in het kader van de identificatie van de abonnee. Aangezien sommige operatoren in de praktijk niet al deze identificatiedocumenten aanvaarden, gelet op de moeilijkheden om de gegevens die op deze documenten vermeld zijn in hun databanken te registreren en gelet op bepaalde twijfels die zouden kunnen bestaan in verband met de betrouwbaarheid van sommige documenten, wordt aan de operatoren een termijn toegestaan om hun systemen aan te passen.

Wat betreft de te verzamelen minimale gegevens waarvan sprake in artikel 127, § 6, beschikken de operatoren over 24 maanden na de bekendmaking van de wet om aan de nieuwe eisen te voldoen.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 8 **DU GOUVERNEMENT**

Art. 16

Remplacer cet article par ce qui suit:

"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 un 5° et un 6°, rédigés comme suit:

"5° demande de données d'identification: demande de l'Institut ou de ses officiers de police judiciaire adressée à un opérateur ou à une autre personne morale de communiquer des données autres que celles conservées en vertu de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, et visant à identifier:

— l'abonné ou l'utilisateur habituel du service de communications électroniques, son équipement terminal ou le dispositif matériel ou logiciel intégré dans cet équipement terminal ou installé auprès de l'abonné en vue de la fourniture du service de communications électroniques, ou;

— les services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

6° demande de métadonnées: demande de l'Institut ou de ses officiers de police judiciaire adressée à un opérateur de communiquer des métadonnées de communications électroniques autres que celles conservées en vertu de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, autre qu'une demande de données d'identification et visant notamment à:

a) déterminer les métadonnées liées à une communication électronique;

b) localiser l'équipement terminal;

Nr. 8 **VAN DE REGERING**

Art. 16

Dit artikel vervangen als volgt:

"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 een bepaling onder 5° en een bepaling onder 6°, luidende:

"5° verzoek om identificatiegegevens: verzoek van het Instituut of van zijn officieren van gerechtelijke politie gericht aan een operator of een andere rechtspersoon om andere gegevens te verstrekken dan deze bewaard krachtens artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie en met het oog op de identificatie van:

— de abonnee of de gewoonlijke gebruiker van de elektronische-communicatiedienst, zijn eindapparatuur of de hardware of software die is ingebouwd in deze eindapparatuur of is geïnstalleerd bij de abonnee met het oog op de verstrekking van de elektronische-communicatiedienst, of;

— de elektronische-communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

6° verzoek om metagegevens: verzoek van het Instituut of van zijn officieren van gerechtelijke politie gericht aan een operator om andere elektronische-communicatiemetagegevens te verstrekken dan deze bewaard krachtens artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie en dat geen verzoek om identificatiegegevens is, teneinde met name:

a) de metagegevens in verband met een elektronische communicatie te bepalen;

b) de eindapparatuur te lokaliseren;

c) déterminer si l'équipement terminal est allumé ou éteint.".”

JUSTIFICATION

Les trois types de demandes de l'IBPT en matière de données d'identification et de métadonnées

Dans son avis n° 71 184/4 du 25 avril 2022 sur les projets d'amendements au 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, le Conseil d'État a indiqué qu'il convient "de s'assurer que les "données relatives à l'abonné ou à l'utilisateur habituel du service" définies à l'article 2, 5°, en projet de la loi du 17 janvier 2003, auxquelles l'IBPT peut accéder conformément à l'article 15, § 1er, en projet, ne comprennent que des données d'identification, à défaut de quoi un contrôle préalable externe devra être mis en place pour pouvoir accéder aux autres données".

Pour tenir compte de cet avis et du point 77 de l'avis de l'Autorité de protection des données (ci-après APD) n° 66/2022 du 1er avril 2022 sur ces projets d'amendements, selon lequel l'adresse IP à la source de la connexion permet de "déduire des informations relatives à la localisation de l'utilisateur du service (en particulier s'il s'agit de services de messagerie)", la définition de l'article 2, 5°, de la loi IBPT-statut a été revue.

À la place d'une définition à l'article 2, 5°, l'article 2 introduit dorénavant deux définitions, en faisant une distinction entre les demandes de données d'identification (ci-après la première catégorie de demande) et les demandes de métadonnées (ci-après la deuxième catégorie de demande). La deuxième catégorie de demandes vise les demandes de métadonnées autres que les demandes de données d'identification, vu que certaines données qui servent généralement à identifier une personne (par exemple une adresse IP à la source de la connexion) sont des métadonnées (voir la définition de métadonnées de communications électroniques introduite dans l'article 2 de la loi télécom par le projet de loi). Il convient cependant de noter que certaines données qui permettent d'identifier une personne ne sont pas des métadonnées (comme par exemple l'identité civile d'une personne).

Une demande de données d'identification vise à identifier:

c) te bepalen of de eindapparatuur is ingeschakeld of uitgeschakeld.".”

VERANTWOORDING

De drie types van verzoeken van het BIPT op het vlak van identificatie- en metagegevens

In zijn advies nr. 71 184/4 van 25 april 2022 over amendementen op een 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 stelt de Raad van State: "Er moet dus voor gezorgd worden dat de "gegevens in verband met de abonnee of de gewoonlijke gebruiker van de dienst" zoals gedefinieerd in het ontworpen artikel 2, 5°, van de wet van 17 januari 2003, waartoe het BIPT toegang kan hebben overeenkomstig het ontworpen artikel 15, § 1, enkel identificatiegegevens bevatten, zoniet zal een voorafgaande externe controle moeten worden ingevoerd om toegang te hebben tot de andere gegevens".

Teneinde rekening te houden met dat advies en met punt 77 van het advies van de Gegevensbeschermingsautoriteit (hierna "GBA") nr. 66/2022 van 1 april 2022 over deze ontwerpamendementen, dat stelt dat het IP-adres aan de bron van de verbinding het mogelijk maakt om "informatie af te leiden over de plaats waar de gebruiker van de dienst zich bevindt (met name wanneer het berichtendiensten betreft)", werd de definitie van artikel 2, 5° van de BIPT-statuutwet herzien.

In de plaats van een definitie in artikel 2, 5°, introduceert artikel 2 nu twee definities waarbij een onderscheid wordt gemaakt tussen de verzoeken om identificatiegegevens (hierna de "eerste categorie van verzoeken") en de verzoeken om metagegevens (hierna de "tweede categorie van verzoeken"). De tweede categorie van verzoeken beoogt de andere verzoeken om metagegevens dan de verzoeken om identificatiegegevens, aangezien bepaalde gegevens die over het algemeen dienen om een persoon te identificeren (bijvoorbeeld een IP-adres aan de bron van de verbinding) metagegevens zijn (zie de definitie van elektronische-communicatiemetagegevens ingevoerd in artikel 2 van de telecomwet door het wetsontwerp). Er dient evenwel te worden opgemerkt dat bepaalde gegevens die het mogelijk maken om een persoon te identificeren geen metagegevens zijn (zoals bijv. de burgerlijke identiteit van een persoon).

Een verzoek om identificatiegegevens beoogt de identificatie van:

— l'abonné (la personne qui conclut le contrat avec l'opérateur) ou l'utilisateur habituel du service;

— l'équipement terminal (par exemple un téléphone ou un ordinateur);

— le dispositif matériel ou logiciel intégré dans cet équipement terminal (par exemple la carte (e-)SIM) ou installé auprès de l'abonné en vue de la fourniture du service de communications électroniques (par exemple le modem dans le cadre d'un service d'accès à internet);

— les services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (les données de souscription).

Il convient de noter que l'identification de l'équipement terminal ou du dispositif matériel ou logiciel intégré dans cet équipement terminal ou installé auprès de l'abonné en vue de la fourniture du service de communications électroniques vise in fine à identifier l'abonné ou l'utilisateur habituel du service.

Une demande de métadonnées vise généralement à:

— déterminer les métadonnées liées à une communication électronique (par exemple qui appelle qui, à quel moment ou à quelle fréquence et combien de temps);

— déterminer la localisation de l'équipement terminal (dans le cadre d'une communication de contenu ou dans le cadre d'une communication de données de signalisation entre l'équipement terminal et le réseau);

— déterminer si l'équipement terminal est allumé ou éteint ("on/off").

Si l'IBPT demande à un opérateur des données conservées sur base des articles 126 ou 127 de la loi télécom, il s'agira en principe d'une demande de données d'identification. Des exceptions à ce principe sont possibles pour certaines demandes spécifiques. Par exemple, s'il était demandé à un opérateur qui offre un service de messagerie d'identifier toutes les adresses IP liées à un WIFI qui ont permis à la personne recherchée de se connecter à son compte du service de messagerie et s'il était demandé par la suite aux opérateurs concernés d'identifier les personnes (morales ou physiques) qui ont mis ce WIFI à disposition de la personne recherchée. Dans ce cas, les différentes adresses des exploitants de ces WIFI (par exemple l'adresse de différents commerces) permettront de déterminer la localisation de la

— de abonnee (de persoon die het contract sluit met de operator) of de gewoonlijke gebruiker van de dienst;

— de eindapparatuur (bijvoorbeeld een telefoon of een computer);

— de hardware of software die is geïntegreerd in die eindapparatuur (bijvoorbeeld de (e-)simkaart) of is geïnstalleerd bij de abonnee met het oog op de verstrekking van de elektronische-communicatiedienst (bijvoorbeeld de modem in het kader van een internettoegangsdienst);

— de elektronische-communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden (de abonnementsgegevens).

Er dient te worden opgemerkt dat de eindapparatuur of de hardware of software die geïntegreerd is in die eindapparatuur of geïnstalleerd is bij de abonnee met het oog op de verstrekking van de elektronische-communicatiedienst in fine beoogt om de abonnee of de gewoonlijke gebruiker van de dienst te identificeren.

Een verzoek om metagegevens beoogt over het algemeen:

— de elektronische-communicatiemetagegevens te bepalen (bijvoorbeeld wie belt wie, wanneer of met welke frequentie en voor hoe lang);

— de plaats van het eindtoestel te bepalen (in het kader van een communicatie van inhoud of in het kader van een communicatie van signaliseringsgegevens tussen de eindapparatuur en het netwerk);

— te bepalen of de eindapparatuur is ingeschakeld of uitgeschakeld ("on/off").

Indien het BIPT aan een operator gegevens vraagt die werden bewaard op basis van de artikelen 126 of 127 van de telecomwet, zal het in principe een verzoek om identificatiegegevens betreffen. Er zijn uitzonderingen op dat principe mogelijk voor bepaalde specifieke verzoeken. Wanneer een operator die een berichtendienst aanbiedt bijvoorbeeld zou worden gevraagd om alle IP-adressen te identificeren die zijn gelinkt aan een wifi en aan de hand waarvan een gezochte persoon heeft kunnen inloggen op zijn account van de berichtendienst en wanneer vervolgens zou worden gevraagd aan de betrokken operatoren om de personen (rechtspersonen of natuurlijke personen) te identificeren die deze wifi ter beschikking hebben gesteld van de gezochte persoon. In dat geval zal de locatie van de persoon tijdens de verbindingen met de

personne lors des connexions aux différents WIFI. Dans ce cas, la demande vise à localiser une personne et n'est donc pas une demande de données d'identification. L'IBPT devra donc examiner si sa demande de données envers l'opérateur est bien une demande de données d'identification.

Si l'IBPT demande à un opérateur des données conservées en vertu de l'article 122 de la loi télécom, il conviendra de vérifier que la demande constitue bien une demande de données d'identification, les données conservées sur base de cet article étant variées (de données d'identification civile à des métadonnées liées à une communication électronique).

Par exemple, l'opérateur devra exploiter des données conservées en vertu de l'article 122 pour répondre à une demande visant à déterminer tous les numéros de téléphone contactés par une personne déterminée pendant une certaine période. Il ne s'agit pas d'une demande de données d'identification mais d'une demande relative aux métadonnées de la communication. Par contre, demander à un opérateur à qui un numéro de téléphone donné a été attribué est une demande de données d'identification.

Un grand nombre de métadonnées conservées en vertu des articles 126 et 127 de la loi télécom pourront ou devront également l'être également en vertu de l'article 122. Dès lors que les données énumérées aux articles 126 et 127 doivent être considérées comme étant "en principe" des données qui servent à répondre à une demande de données d'identification, il peut être utile de se référer à ces données pour déterminer si une demande de données conservées sur la base de l'article 122 relève ou non de la notion de demande de données d'identification.

Une demande qui vise à obtenir des données conservées par les opérateurs sur base de l'article 123 de la loi télécom sera toujours une demande de métadonnées, vu qu'il s'agit de données de location traitées par l'opérateur en dehors d'une communication de contenu.

Les demandes de données d'identification 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 demandes de métadonnées, dès lors qu'elles ne permettent pas de tirer des conclusions précises relatives à la vie privée de l'abonné ou de l'utilisateur habituel du service.

verschillende wifi's kunnen worden bepaald aan de hand van de verschillende adressen van de exploitanten van deze wifi's (bijvoorbeeld het adres van verschillende handelszaken). Het verzoek beoogt in dat geval een persoon te lokaliseren en is dus geen verzoek tot identificatiegegevens. Het BIPT zal dus moeten nagaan of zijn verzoek om gegevens aan de operator wel degelijk een verzoek om identificatiegegevens is.

Indien het BIPT aan een operator gegevens vraagt die zijn bewaard krachtens artikel 122 van de telecomwet, zal moeten worden gecontroleerd of het verzoek wel degelijk een verzoek om identificatiegegevens betreft aangezien de gegevens bewaard op basis van dat artikel variëren (van gegevens van burgerlijke identiteit tot elektronische-communicatiemetagegevens).

De operator zal bijvoorbeeld gegevens moeten benutten die werden bewaard krachtens artikel 122 om een verzoek te beantwoorden dat beoogt alle telefoonnummers te bepalen die een gegeven persoon gedurende een gegeven periode heeft gecontacteerd. Het betreft geen verzoek om identificatiegegevens maar een verzoek met betrekking tot de metagegevens van de communicatie. Vragen aan een operator aan wie een gegeven telefoonnummer is toegewezen, betreft daarentegen een verzoek om identificatiegegevens.

Een groot aantal metagegevens bewaard krachtens de artikelen 126 en 127 van de telecomwet zullen ook kunnen of moeten bewaard worden krachtens artikel 122. Aangezien de gegevens opgesomd in de artikelen 126 en 127 moeten beschouwd worden als zijnde gegevens die "in principe" dienen om te antwoorden op een verzoek om identificatiegegevens, kan het nuttig zijn om te verwijzen naar deze gegevens om te bepalen of een verzoek om bewaarde gegevens op basis van artikel 122 al dan niet onder het begrip van een verzoek om identificatiegegevens valt.

Een verzoek dat is bedoeld om gegevens te verkrijgen die de operatoren bewaren krachtens artikel 123 van de telecomwet zal altijd een verzoek om metagegevens zijn, aangezien het locatiegegevens betreft die worden verwerkt door de operator buiten een communicatie van inhoud om.

De verzoeken om identificatiegegevens mogen, 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), worden beschouwd als gegevens die een mindere mate van gevoeligheid vertonen dan de verzoeken om metagegevens, aangezien daaruit geen precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de abonnee of de gewoonlijke gebruiker van de dienst.

Cette distinction entre d'une part une demande de données d'identification ("moins intrusives"), et d'autre part les autres demandes ("plus intrusives"), est structurante dans la jurisprudence de la CJUE, puisqu'elle a une incidence tant au niveau de la conservation de ces données qu'au niveau de l'accès à ces données.

En effet, selon l'arrêt "La Quadrature du Net" (aff. Jtes C-511/18, C-512/18 et C-520/18) du 6 octobre 2021, les données d'identification peuvent être soumises à une obligation de conservation généralisée et indifférenciée, alors que les métadonnées qui ne sont pas des données d'identification ne peuvent en principe être soumises qu'à une obligation de conservation ciblée (sauf cas de menace grave réelle et actuelle ou prévisible à l'égard de la sécurité nationale). Rappelons néanmoins que cette jurisprudence a été rendue en matière de recherche, de détection et de poursuite d'infractions pénales et de protection de la sécurité nationale; la CJUE ne s'étant pas prononcée à ce jour dans le cadre d'autres finalités permises par l'article 15, § 1er de la directive 2002/58 ("directive e-privacy"), telles que la lutte contre les fraudes et utilisations malveillantes du réseau ou de protection de la sécurité des réseaux.

Par ailleurs, pour ce qui concerne l'accès aux métadonnées, la CJUE a apporté des précisions dans son arrêt "Prokuratuur" (C-746/18) du 2 mars 2021, dont les enseignements ont été repris dans l'arrêt de la Cour constitutionnelle belge du 18 novembre 2021 (n° 158/2021). Conformément à ce dernier arrêt, il convient de prévoir un contrôle préalable externe (contrôle par une autorité administrative indépendante ou une juridiction) des demandes de métadonnées mais pas des demandes de données d'identification. Pour ces dernières demandes, la loi statut organise un contrôle préalable interne.

Pour les catégories de demandes 1 (demande de données d'identification) et 2 (demande de métadonnées), l'IBPT ne pourra pas recevoir de données conservées par l'opérateur dans le cadre de la conservation ciblée sur base géographique (article 126/1 de la loi télécom).

Une troisième catégorie de demande concerne la consultation des bases de données des opérateurs mettant en œuvre les articles 122 à 127 de la loi télécom à des fins de contrôle par l'IBPT (ou ses officiers de police judiciaire) du respect par un opérateur de ces articles et de leurs arrêtés d'exécution. Dans ce cadre, l'IBPT agit comme "contrôleur des données" (contrôle du respect par l'opérateur de la réglementation). Pour que ce contrôle soit efficace, un accès à certaines bases

Dat onderscheid tussen enerzijds een verzoek om ("minder indringende") identificatiegegevens en anderzijds de ("meer indringende") overige verzoeken is structurerend in de rechtspraak van het HvJ-EU aangezien het een impact heeft op zowel de bewaring van deze gegevens als op de toegang tot deze gegevens.

Volgens het arrest "La Quadrature du Net" (gevoegde zaken C-511/18, C-512/18 en C-520/18) van 6 oktober 2021, kunnen de identificatiegegevens onderworpen worden aan een verplichting van algemene en ongedifferentieerde bewaring terwijl de metagegevens die geen identificatiegegevens zijn in principe enkel kunnen worden onderworpen aan een verplichting van doelgerichte bewaring (behalve in gevallen van een reële en actuele of voorspelbare dreiging ten aanzien van de nationale veiligheid). We herinneren er evenwel aan dat deze rechtspraak werd gedaan op het stuk van onderzoek, opsporing en vervolging van strafrechtelijke inbreuken en van bescherming van de nationale veiligheid; het HvJ-EU heeft zich tot op heden nog niet uitgesproken in het kader van andere doeleinden toegestaan door artikel 15, § 1, van Richtlijn 2002/58 ("e-Privacyrichtlijn") zoals de strijd tegen fraude en kwaadwillig gebruik van het netwerk of bescherming van de netwerkveiligheid.

Wat overigens de toegang tot metagegevens betreft, heeft het HvJ-EU verduidelijkingen aangebracht in zijn arrest "Prokuratuur" (C-746/18) van 2 maart 2021, waarvan de lering werd overgenomen in het arrest van het Belgische Grondwettelijk Hof van 18 november 2021 (nr. 158/2021). Conform dat laatste arrest, dient te worden voorzien in een externe voorafgaande controle (controle door een onafhankelijke administratieve overheid of een rechtscollege) van de verzoeken om metagegevens maar niet van de verzoeken om identificatiegegevens. Voor deze laatste verzoeken organiseert de statuutwet een interne voorafgaande controle.

Voor de eerste categorie van verzoeken (verzoek om identificatiegegevens) en voor de tweede (verzoek om metagegevens) zal het BIPT geen gegevens kunnen ontvangen die worden bewaard door de operator in het kader van doelgerichte bewaring op geografische basis (artikel 126/1 van de telecomwet).

Een derde categorie betreft de verzoeken om toegang tot de databanken van de operatoren die de artikelen 122 tot 127 van de telecomwet ten uitvoer brengen voor controle door het BIPT (of zijn officieren van gerechtelijk politie) van de naleving van deze artikelen en de uitvoeringsbesluiten ervan door een operator. In dat kader treedt het BIPT op als "controleur van de gegevens" (controle van de inachtneming van de regelgeving door de operator). Opdat deze controle efficiënt zou zijn, is

de données de l'opérateur est nécessaire. Par contre, pour les demandes de catégories 1 et 2, l'opérateur fournit à l'IBPT certaines données (pas d'accès à une base de données).

La perspective pénale et la perspective administrative.

Pour chacune des trois catégories de demandes susmentionnées, on peut distinguer les deux perspectives suivantes:

— les officiers de police judiciaire de l'IBPT peuvent agir dans le cadre de leurs missions de recherche et de constat d'infractions pénales (la perspective pénale);

— le Conseil de l'IBPT peut aussi agir pour la mise en œuvre ou le contrôle de dispositions qui ne sont pas assorties de sanctions pénales ou pour sanctionner de manière administrative le non-respect d'une disposition assortie d'une sanction pénale, à la suite d'un PV d'un officier de police judiciaire, lorsque le procureur du Roi laisse à l'IBPT le soin de diligenter les poursuites (la perspective administrative).

Les données anonymes ou pseudonymes

Dans son avis n° 66/2022 du 1er avril 2022, l'APD considère que "s'il est possible que l'IBPT remplisse toutes ou certaines des missions énumérées ci-dessus à l'aide de données anonymisées ou pseudonymisées, le projet doit prévoir que seules des données anonymisées ou pseudonymisées pourront leur être transmises. Cet examen doit être fait de manière minutieuse, mission par mission." (considérant n° 92). L'APD souligne néanmoins "qu'il peut être particulièrement difficile de réellement anonymiser ou même pseudonymiser des métadonnées de communications électroniques. Il apparait, en effet, qu'il est tout à fait possible voire assez facile, de réidentifier des personnes à partir d'un set de métadonnées de communications électroniques anonymisées." (note de bas de page n° 55).

Il convient de préciser que, conformément à l'article 25 du Règlement général relatif à la protection des données (RGPD), l'IBPT en tant que responsable du traitement des données à caractère personnel qui lui sont transmises, met en œuvre les mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, de manière à mettre en œuvre les principes généraux du RGPD, tel que le principe de minimisation des données, et ainsi protéger les droits de la personne concernée. Les principes généraux du RGPD demeurent en effet applicables. Des mesures de pseudonymisation seront

toegang tot bepaalde databanken van de operator nodig. Voor de verzoeken van de eerste en tweede categorieën verstrekt de operator aan het BIPT bepaalde gegevens (geen toegang tot een databank).

Vanuit strafrechtelijk en administratief perspectief.

Voor elk van de drie voormelde verzoeken kan een onderscheid worden gemaakt tussen de twee volgende perspectieven:

— de officieren van gerechtelijke politie van het BIPT kunnen in het kader van hun opdrachten van opsporing en vaststelling van strafrechtelijke inbreuken handelen (strafrechtelijk perspectief);

— de Raad van het BIPT kan ook optreden in het kader van de tenuitvoerbrenging of de controle van bepalingen waar geen strafrechtelijke sancties aan vasthangen of om de niet-naleving van een bepaling gepaard met een strafrechtelijke sanctie op administratieve wijze te bestraffen, naar aanleiding van een pv van een officier van gerechtelijke politie wanneer de procureur des Konings het instellen van de vervolgingen overlaat aan het BIPT (administratief perspectief).

De anonieme of pseudonieme gegevens

In haar advies nr. 66/2022 van 1 april 2022 beschouwt de GBA dat "indien het mogelijk is dat het BIPT alle of sommige van de hierboven opgesomde taken uitvoert met behulp van geanonimiseerde of gepseudonimiseerde gegevens, het ontwerp moet bepalen dat alleen geanonimiseerde of gepseudonimiseerde gegevens aan hen kunnen worden doorgegeven. Dit onderzoek moet grondig gebeuren, opdracht per opdracht." (considerans nr. 92) De GBA wijst er echter op "dat het bijzonder moeilijk kan zijn om metagegevens betreffende elektronische communicatie effectief te anonimiseren of zelfs te pseudonimiseren. Het blijkt namelijk heel goed mogelijk, en zelfs heel gemakkelijk, om personen opnieuw te identificeren aan de hand van een reeks geanonimiseerde metadata van de elektronische communicatie." (voetnoot nr. 55).

Er dient te worden gepreciseerd dat, conform artikel 25 van de Algemene verordening gegevensbescherming (AVG), het BIPT als verantwoordelijk voor de verwerking van de persoonsgegevens die het wordt verstrekt, de gepaste technische en organisatorische maatregelen ten uitvoer brengt, zoals de pseudonimisering, zodat de algemene principes van de AVG worden gehanteerd, zoals het principe van de minimale gegevensverwerking, en aldus de rechten van de persoon in kwestie worden beschermd. De algemene principes van de AVG blijven immers van toepassing. In het kader van

donc prises dans toute la mesure du possible, dans le cadre des demandes de métadonnées, pour autant que cette mesure ne nuise pas à la finalité poursuivie.

Cependant, dans les cas suivants, la communication de l'opérateur à l'IBPT de données anonymes ou pseudonymes ne permet pas de répondre à l'objectif poursuivi: pour ce qui concerne les missions de constatation des infractions pénales poursuivies par les OPJ de l'IBPT, lorsque l'IBPT agit en tant que contrôleur des données et dans le cadre d'une demande de données d'identification (l'objectif d'identification s'oppose au principe même de la pseudonymisation ou anonymisation des données).

La possibilité de demander des données anonymes ou pseudonymes ne doit donc être examinée que dans le cas de figure restant, à savoir les demandes de métadonnées (demandes de catégorie 2) dans la perspective administrative. Cette possibilité ne sera mise en œuvre que si des données anonymes ou pseudonymes permettent toujours de rencontrer l'objectif poursuivi. Il n'est pas possible de prévoir dans le présent amendement les missions de l'IBPT pour lesquels des données anonymes ou pseudonymes seront suffisantes. C'est un examen qui devra être fait par l'IBPT au cas par cas.

Pour tenir compte de l'avis de l'APD, l'article 15 en projet de la loi IBPT-statut a été complété comme suit. D'abord, l'article 15, § 2, indique que l'IBPT doit demander à l'opérateur de lui fournir des données anonymisées ou pseudonymisées lorsque cela permet toujours de rencontrer l'objectif poursuivi. Ensuite, l'article 15, § 4, prévoit que lorsque l'IBPT estime que cela n'est pas le cas, il doit le motiver dans la demande adressée à l'APD dans le cadre du contrôle préalable (expliquer pourquoi des données anonymes ou pseudonymes ne permettent pas de remplir l'objectif poursuivi).

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

verzoeken om metagegevens zullen dus, zo goed als mogelijk, maatregelen van pseudonimisering worden getroffen op voorwaarde dat deze maatregel geen afbreuk doet aan het beoogde doeleinde.

In de volgende gevallen volstaat de verstrekking van anonieme of pseudonieme gegevens door de operator aan het BIPT echter niet om te beantwoorden aan het beoogde doel: wat betreft de opdrachten van vaststelling van strafrechtelijke inbreuken vervolgd door de OGP's van het BIPT, wanneer het BIPT handelt als controleur van de gegevens en in het kader van een verzoek om identificatiegegevens (het doel van identificatie staat lijnrecht tegenover het principe zelf van de pseudonimisering of anonimisering van de gegevens).

De mogelijkheid om te vragen om de gegevens te anonimiseren of te pseudonimiseren moet dus pas worden onderzocht in het resterende geval, met name de verzoeken om metagegevens (verzoeken van de tweede categorie) vanuit het administratief perspectief. Deze mogelijkheid zal pas ten uitvoer worden gebracht wanneer het nog steeds mogelijk is om op basis van de geanonimiseerde of gepseudonimiseerde gegevens het nagestreefde doel te bereiken. Het is niet mogelijk om in dit amendement de opdrachten van het BIPT te bepalen waarvoor anonieme of pseudonieme gegevens voldoende zullen zijn. Dat is een onderzoek dat het BIPT geval per geval zal moeten doen.

Om rekening te houden met het advies van de GBA werd ontwerpartikel 15 van de BIPT-statuutwet vervolledigd als volgt. In de eerste plaats geeft artikel 15, § 2, aan dat het BIPT aan de operator moet vragen om het geanonimiseerde of gepseudonimiseerde gegevens te verstrekken als het in dat geval nog steeds mogelijk is om aan het beoogde doel te beantwoorden. Vervolgens bepaalt artikel 15, § 4, dat wanneer het BIPT meent dat dat niet het geval is, het dat moet motiveren in het verzoek gericht aan de GBA in het kader van de voorafgaande controle (uitleggen waarom anonieme of pseudonieme gegevens niet volstaan om aan het beoogde doel te beantwoorden).

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 9 DU **GOUVERNEMENT**

Art. 17

Remplacer cet article par ce qui suit:

"Art. 17. À l'article 14 de la même loi, modifié en dernier lieu par la loi du 17 février 2022, le chiffre "15" est inséré entre les mots "les articles 14, § 2, 2°," et les mots "et 21, §§ 5 à 7"."

JUSTIFICATION

Il est important de veiller à ce que le respect du nouvel article 15 de la loi statut IBPT puisse être contrôlé par l'IBPT et que le non-respect d'une décision de l'IBPT prise sur base de ce nouvel article puisse être sanctionné. C'est la raison pour laquelle le contrôle de cet article a été ajouté à l'article 14, § 1er, 3°, d).

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Nr. 9 VAN DE **REGERING**

Art. 17

Dit artikel vervangen als volgt:

"Art. 17. In artikel 14 van dezelfde wet, laatstelijk gewijzigd bij de wet van 17 februari 2022, wordt het cijfer "15" ingevoegd tussen de woorden "de artikelen 14, § 2, 2°," en de woorden "en 21, §§ 5 tot 7"."

VERANTWOORDING

Het is belangrijk om erop toe te zien dat de naleving van het nieuwe artikel 15 van de BIPT-statuutwet kan worden gecontroleerd door het BIPT en dat de niet-naleving van een besluit van het BIPT genomen op grond van dat nieuwe artikel, bestraft kan worden. Dat is de reden waarom de controle van dat artikel toegevoegd is in artikel 14, § 1, 3°, d).

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 10 **DU GOUVERNEMENT**

Art. 18

Remplacer cet article par ce qui suit:

"Art. 18. Dans la même loi, l'article 15, abrogé par la loi du 16 mars 2015, est rétabli dans la rédaction suivante:

"Art. 15. § 1er. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), ce dernier peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de données d'identification. L'Institut fixe le délai de communication des données demandées.

§ 2. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), ce dernier peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de métadonnées. L'Institut fixe le délai de communication des données demandées.

Sauf en cas d'urgence dûment justifié et sauf lorsque des métadonnées anonymes sont demandées à l'opérateur, l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée à l'Autorité de protection des données et après avoir obtenu l'autorisation écrite de cette dernière.

En cas d'urgence dûment justifiée, l'Institut communique à l'Autorité de protection des données, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande ainsi que la justification de l'urgence. L'Autorité de protection des données effectue ultérieurement un contrôle.

Nr. 10 **VAN DE REGERING**

Art. 18

Dit artikel vervangen als volgt:

"Art. 18. In dezelfde wet, wordt artikel 15, opgeheven bij de wet van 16 maart 2015, hersteld als volgt:

"Art. 15. § 1. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mag het Instituut van een operator, schriftelijk en met redenen omkleed, eisen dat hij antwoordt op een verzoek om identificatiegegevens. Het Instituut bepaalt de termijn waarbinnen de gegevens moeten worden meegedeeld.

§ 2. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren, mag het Instituut van een operator, schriftelijk en met redenen omkleed, eisen dat hij antwoordt op een verzoek om metagegevens. Het Instituut bepaalt de termijn waarbinnen de gegevens moeten worden meegedeeld.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid en tenzij anonieme metagegevens worden gevraagd aan de operator, mag het Instituut het verzoek aan de operator pas richten na het voorleggen van een met redenen omkleed en schriftelijk verzoek aan de Gegevensbeschermingsautoriteit en na het ontvangen van de schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid deelt het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dat verzoek, de motivering van het verzoek, alsook de rechtvaardiging van de hoogdringendheid mee aan de Gegevensbeschermingsautoriteit. De Gegevensbeschermings-autoriteit voert daarna een controle uit.

Pour l'application du présent paragraphe, l'Institut demande à l'opérateur des métadonnées anonymisées ou pseudonymisées, sauf lorsqu'elles ne lui permettent pas de rencontrer l'objectif poursuivi.

§ 3. Par dérogation aux paragraphes 1 et 2 et afin de contrôler le respect par un opérateur de l'article 122, de l'article 123, de l'article 126, de l'article 126/1, de l'article 126/2 ou de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques ou d'un arrêté d'exécution d'un de ces articles, l'Institut peut exiger d'un opérateur, par demande écrite et motivée, de lui fournir l'accès lui permettant de consulter une base de données qui met en œuvre un de ces articles ou un de ces arrêtés d'exécution.

L'alinéa 1er n'est applicable pour ce qui concerne les articles 126, 126/1, 126/2 et 127 et leurs arrêtés d'exécution que pour autant que l'Institut soit chargé de sanctionner l'opérateur après la concertation avec le procureur du Roi visée à l'article 21/1.

La demande adressée à l'opérateur précise les noms des membres du personnel de l'Institut qui peuvent consulter cette base de données.

Ces membres du personnel ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des manquements commis par l'opérateur.

§ 4. Pour l'application des paragraphes 1 à 3, la motivation de la demande adressée à l'opérateur ou à l'Autorité de protection des données doit être développée au regard des circonstances.

Pour l'application des paragraphes 1er et 2, l'Institut doit motiver:

1° le lien entre les données demandées et la mission attribuée à l'Institut;

Voor de toepassing van deze paragraaf vraagt het Instituut aan de operator geanonimiseerde of gepseudonimiseerde metagegevens tenzij op basis daarvan niet aan het beoogde doel kan worden beantwoord.

§ 3. In afwijking van de paragrafen 1 en 2 en om de naleving door een operator van artikel 122, van artikel 123, van artikel 126, van artikel 126/1, van artikel 126/2 of van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie of van een besluit ter uitvoering van een van deze artikelen te controleren, kan het Instituut met een schriftelijk en met redenen omkleed verzoek van een operator eisen om aan het Instituut toegang te verlenen zodat het een databank kan raadplegen die een van deze artikelen of een van deze uitvoeringsbesluiten ten uitvoer legt.

Het eerste lid is wat betreft de artikelen 126, 126/1, 126/2 en 127 en de uitvoeringsbesluiten ervan slechts van toepassing voor zover het Instituut na het in artikel 21/1 bedoelde overleg met de procureur des Konings, ermee belast wordt de operator te sanctioneren.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de personeelsleden van het Instituut die deze databank mogen raadplegen.

Deze personeelsleden mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

§ 4. Voor de toepassing van de paragrafen 1 tot 3, moet de motivering van het verzoek gericht aan de operator of aan de Gegevensbeschermingsautoriteit uitgewerkt zijn in het licht van de omstandigheden.

Voor de toepassing van de paragrafen 1 en 2, moet het Instituut:

1° het verband motiveren tussen de gevraagde gegevens en de aan het Instituut toegewezen opdracht;

2° le caractère strictement nécessaire des données demandées dans le cadre de cette mission.

Pour l'application du paragraphe 2, l'Institut indique dans la demande adressée à l'Autorité de protection des données:

1° le motif pour lequel la communication par l'opérateur de métadonnées anonymisées ne permet pas de rencontrer l'objectif poursuivi;

2° le motif pour lequel la communication par l'opérateur de métadonnées pseudonymisées ne permet pas de rencontrer l'objectif poursuivi, sauf lorsque la demande précise que l'opérateur doit fournir de telles données.

Sont consignées dans un registre tenu auprès de l'Institut:

1° les demandes adressées aux opérateurs et à l'Autorité de protection des données;

2° la motivation de la demande et la justification de l'urgence communiquées à l'Autorité de protection des données conformément au paragraphe 2, alinéa 3;

3° les autorisations données par l'Autorité de protection des données."."

2° motiveren dat het niet meer gegevens vraagt dan die welke strikt nodig zijn in het kader van die opdracht.

Voor de toepassing van paragraaf 2 geeft het Instituut in het verzoek gericht aan de Gegevensbeschermingsautoriteit het volgende aan:

1° de reden waarom de verstrekking door de operator van geanonimiseerde metagegevens niet volstaat om het nagestreefde doel te bereiken;

2° de reden waarom de verstrekking door de operator van gepseudonimiseerde gegevens niet volstaat om het nagestreefde doel te bereiken, behalve wanneer het verzoek preciseert dat de operator dergelijke gegevens moet verstrekken.

Moeten worden opgenomen in een inventaris die bij het Instituut wordt bijgehouden:

1° de verzoeken gericht aan de operatoren en aan de Gegevensbeschermingsautoriteit;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de Gegevensbeschermingsautoriteit overeenkomstig paragraaf 2, derde lid;

3° de toestemmingen verleend door de Gegevensbeschermingsautoriteit."."

JUSTIFICATION

Introduction

Un nouvel article 15 est inséré dans la loi de manière à préciser les conditions matérielles et procédurales selon lesquelles l'Institut peut exiger d'un opérateur la communication ou l'accès à certaines données d'identification ou métadonnées.

Dans son avis n° 62/2022 du 1er avril 2022, l'APD indique ce qui suit:

— "À défaut d'une justification étayée de l'importance de l'objectif poursuivi (à la lumière des exigences mises en évidence par la CJUE), la disposition en projet devra

VERANTWOORDING

Inleiding

In de wet wordt een nieuw artikel 15 ingevoegd om de materiële en procedurele voorwaarden te verduidelijken volgens welke het Instituut van een operator de mededeling van of de toegang tot bepaalde identificatiegegevens of metagegevens kan eisen.

In advies nr. 62/2022 van 1 april 2022 preciseert de GBA het volgende:

— "Bij gebrek aan een gemotiveerde rechtvaardiging van het belang van het nagestreefde doel (in het licht van de door het HvJEU benadrukte vereisten), zal

être modifiée afin d'exclure la possibilité pour l'IBPT de demander accès à aux données conservées en exécution de l'article 126/1 de la loi télécom." (point 98);

— "l'exigence de prévisibilité, couplée au principe de minimisation des données consacré par l'article 5.1. c) du RGPD, requiert que la disposition en projet délimite précisément quelles sont les catégories de données auxquelles l'IBPT peut avoir accès pour remplir quelles missions." (point 99)

Dans son avis n° 71 184/4 du 25 avril 2022, le Conseil d'État indique qu'"Il appartient à l'auteur de l'amendement d'être en mesure d'établir les éléments qui permettent de justifier la nécessité et le caractère proportionné de la possibilité d'accéder à l'ensemble de ces données (ou une partie d'entre elles), et ce mission par mission dans le respect de la jurisprudence de la Cour de justice. La justification de l'amendement sera utilement complétée à cet égard."

Pour répondre à ces avis, les définitions de demande de données d'identification et de métadonnées excluent les données conservées sur base de l'article 126/1 de la loi télécom, de sorte que l'IBPT n'a pas accès à l'ensemble des métadonnées

Dès lors, la disposition délimite les catégories de données auxquelles l'IBPT peut avoir accès pour remplir ses missions, étant donné qu'il s'agit des données conservées par l'opérateur sur une autre base que l'article 126/1 de la loi télécom (à savoir sur pied des articles 122, 123, 126 et 127 de la loi télécom).

Il n'est pas possible de préciser davantage dans les articles en projet des sous-catégories de données qui sont nécessaires pour les missions de l'IBPT. En effet, il n'est pas possible de déterminer ce jour les données qui seront nécessaires dans le futur pour la mise en œuvre des missions de l'IBPT.

Finalement, la présente justification a été complétée pour montrer la nécessité d'obtenir des données conservées en vertu des articles 122, 123, 126 et 127 de la loi télécom.

Missions de l'IBPT et finalités visées à l'article 127/1, § 2, en projet de la loi télécom

Les paragraphes 1 et 2 de l'article 15 de loi IBPT-statut en projet visent les missions d'application et de contrôle du respect de la loi télécom (art. 14, § 1er, 3°, a) de la loi IBPT-statut)

de ontwerpbepaling moeten worden gewijzigd om de mogelijkheid uit te sluiten dat het BIPT toegang vraagt tot de gegevens die worden bewaard ter uitvoering van artikel 126/1 van de telecomwet." (punt 98);

— "het vereiste van voorspelbaarheid, gekoppeld aan het beginsel van de minimale gegevensverwerking dat is vastgelegd in artikel 5, § 1, c), van de AVG, vereist dat in de ontwerpbepaling precies wordt afgebakend tot welke categorieën gegevens het BIPT toegang kan hebben om welke taken te vervullen." (punt 99)

In zijn advies nr. 71 184/4 van 25 april 2022 stelt de Raad van State: "Het staat aan de steller van het amendement om de elementen te kunnen vaststellen die de noodzaak en de evenredigheid kunnen rechtvaardigen van de mogelijkheid om toegang te krijgen tot al die gegevens (of een deel ervan), en dat opdracht per opdracht met inachtneming van de rechtspraak van het Hof van Justitie. Het verdient aanbeveling de verantwoording van het amendement in dat opzicht aan te vullen."

Om te beantwoorden aan deze adviezen sluiten de definities van verzoek om identificatiegegevens en om metagegevens de gegevens bewaard op grond van artikel 126/1 van de telecomwet uit, zodat het BIPT niet tot alle metagegevens toegang heeft.

De bepaling bakent dan ook de categorieën van gegevens waartoe het BIPT toegang mag hebben om zijn opdrachten te vervullen af aangezien het gaat om gegevens die de operator bewaart krachtens een ander artikel dan artikel 126/1 van de telecomwet (met name op grond van de artikelen 122, 123, 126 en 127 van de telecomwet).

Het is niet mogelijk om in de ontwerpartikelen de subcategorieën van gegevens die nodig zijn voor de opdrachten van het BIPT verder in detail te preciseren. Het is immers op heden niet mogelijk om de data te bepalen die in de toekomst nodig zullen zijn om de opdrachten van het BIPT ten uitvoer te brengen.

Tot slot werd deze rechtvaardiging vervolledigd om de noodzaak aan te tonen om gegevens bewaard krachtens de artikelen 122, 123, 126 en 127 van de telecomwet te verkrijgen.

Opdrachten van het BIPT en doeleinden beoogd in ontwerpartikel 127/1, § 2, van de telecomwet

De paragrafen 1 en 2 van artikel 15 van de BIPT-ontwerpstatuutwet beogen de opdrachten inzake toepassing en controle van de naleving van de telecomwet (art. 14, § 1,

et des autres législations sectorielles en matière de sécurité des réseaux et des systèmes d'information, à savoir:

— 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 (ci-après loi "infrastructures critiques") (art. 14, § 1er, 3°, g), de la loi IBPT-statut);

— 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 (loi "NIS") (art. 14, § 1er, 3°, h), de la loi IBPT-statut), et;

— 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 (règlement "fuite de données" (art. 14, § 1er, 3°, i), de la loi IBPT-statut).

Ces missions relèvent des finalités suivantes prévues à l'article 127/1, § 2, de la loi télécom.

La prévention de menaces graves contre la sécurité publique (art. 127/1, § 2, 2° de la loi télécom)

Relèvent notamment de cette finalité, les missions de l'IBPT en exécution de la loi infrastructures critiques et de la loi NIS, en ce qui concerne le secteur des infrastructures numériques.

En effet, les incidents de sécurité des réseaux et des systèmes d'information utilisés pour la fourniture des services essentiels peuvent avoir un impact sur la continuité de ces services et donc sur le maintien d'activités sociétales et/ou économiques critiques. Tel est également le cas pour ce qui concerne les incidents de sécurité impactant les infrastructures critiques.

De tels incidents représentent donc des menaces graves à l'encontre de la sécurité publique. Or, selon la jurisprudence européenne, la finalité de protection par rapport à des menaces graves à l'encontre de la sécurité publique constitue un intérêt sociétal d'importance similaire à celui de la lutte contre la criminalité grave. Pour cette finalité, il peut être nécessaire d'obtenir des données conservées sur base des articles 122, 123, 126 et 127 de la loi télécom.

3°, a), van de BIPT-statuutwet) en van de overige sectorale wetgevingen betreffende de veiligheid van de netwerken en informatiesystemen, namelijk:

— 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 digitale infrastructuren (hierna de wet "kritieke infrastructuren") (art. 14, § 1, 3°, g) van de BIPT-statuutwet;

— 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 ("NIS"-wet) (art. 14, § 1, 3°, h) van de BIPT-statuutwet), en;

— 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 (Verordening "gegevenslek" (art. 14, § 1, 3°, i), van de BIPT-statuutwet).

Deze opdrachten hebben de volgende doeleinden waarin artikel 127/1, § 2, van de telecomwet voorziet.

De preventie van ernstige bedreigingen van de openbare veiligheid (art. 127/1, § 2, 2°, van de telecomwet)

Onder dit doeleinde vallen met name de opdrachten van het BIPT in uitvoering van de wet betreffende de kritieke infrastructuren en de NIS-wet, wat betreft de sector van de digitale infrastructuren.

Veiligheidsincidenten op de netwerken en de informatiesystemen die worden gebruikt voor de verstrekking van de essentiële diensten kunnen immers een impact hebben op de continuïteit van deze diensten en dus op het behoud van maatschappelijk en/of economisch kritieke activiteiten. Dat is ook het geval wat betreft de veiligheidsincidenten die een impact hebben op de kritieke infrastructuren.

Dergelijke incidenten vertegenwoordigen dus ernstige bedreigingen voor de openbare veiligheid. Verder, volgens de Europese rechtspraak, vormt het doel van bescherming in het licht van ernstige bedreigingen voor de openbare veiligheid een maatschappelijk belang van hetzelfde niveau als dat van de strijd tegen de zware criminaliteit. Hiertoe kan het nodig zijn om gegevens bewaard op basis van de artikelen 122, 123, 126 en 127 van de telecomwet te krijgen.

L'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques (art. 127/1, § 2, 4° de la télécom)

Relèvent en particulier de cette finalité, les missions de contrôle et d'application du Chapitre II/1 (De la sécurité des communications électroniques) de la loi télécom et les missions de l'IBPT en exécution des lois NIS et infrastructures critiques précitées.

Pour l'accomplissement de ces missions, il est indispensable pour l'IBPT de pouvoir recevoir communication de métadonnées brutes (non pseudonymisées ou anonymisées) afin de contrôler le respect par l'opérateur de son obligation de prendre les mesures appropriées (par exemple, bloquer une attaque DDOS).

Les catégories de données nécessaires pour ce faire sont celles visées aux articles 122, 123, 126 et 127 de la loi télécom. Afin de pouvoir, par exemple, analyser un incident de sécurité des réseaux ou d'effectuer une analyse préventive de la sécurité du réseau, il est indispensable de pouvoir examiner à la fois les données permettant d'identifier l'origine des communications électroniques ("moins intrusives") et d'autres métadonnées ("plus intrusives"), telles que des données permettant de localiser l'origine et la destination du trafic acheminé sur le réseau de l'opérateur. Pour ce qui concerne les données conservées en vertu des articles 126 et 127, cette finalité d'accès correspond à la finalité initiale de la conservation. Pour ce qui concerne les données conservées en vertu des articles 122 et 123, les finalités d'accès sont d'une importance au moins équivalente aux finalités de conservation initiale pour les besoins des opérateurs (à savoir: la facturation, la commercialisation de services, la lutte contre la fraude et l'utilisation malveillante des réseaux et services ou la sécurité des réseaux et services par les opérateurs).

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. 127/1, § 2, 9° de la loi télécom)

Il convient ici de faire une distinction entre la mission de l'IBPT en tant qu'autorité de contrôle des dispositions nationales prises en application de la directive 2002/58 (e-privacy) et la mission de contrôle de l'IBPT en tant qu'autorité de contrôle d'autres dispositions (en particulier les dispositions de la loi télécom visant à transposer le Code des communications électroniques européen).

Het onderzoek van veiligheidslekken inzake elektronischecommunicatienetwerken of –diensten (art. 127/1, § 2, 4°, van de telecomwet)

Onder dit doeleinde vallen de opdrachten van controle en tenuitvoerbrenging van Hoofdstuk II/1 (Veiligheid van de elektronische communicatie) van de telecomwet en de opdrachten van het BIPT in uitvoering van de hierboven vermelde NIS-wet en de wet betreffende de kritieke infrastructuren.

Voor de verwezenlijking van deze opdrachten is het onontbeerlijk voor het BIPT om ruwe (niet gepseudonimiseerde of geanonimiseerde) metagegevens te kunnen krijgen om de inachtneming door de operator van zijn verplichting om de gepaste maatregelen te treffen (bijvoorbeeld een DDOS-aanval blokkeren) te kunnen controleren.

De daartoe noodzakelijke categorieën van gegevens zijn deze beoogd in de artikelen 122, 123, 126 en 127 van de telecomwet. Om een veiligheidsincident op de netwerken te kunnen analyseren of een preventieve analyse uit te voeren van de netwerkveiligheid, moeten de ("minder ingrijpende") gegevens die de identificatie van de bron van de elektronische communicatie mogelijk maken en andere ("meer ingrijpende") metagegevens zoals de gegevens die het mogelijk maken om de herkomst en bestemming van het verkeer dat via het netwerk van de operator verloopt, absoluut tegelijk kunnen worden onderzocht. Wat betreft de gegevens bewaard krachtens de artikelen 126 en 127, stemt dit toegangsdoeleinde overeen met het initiële doel van de bewaring. Wat betreft de gegevens bewaard op grond van de artikelen 122 en 123 zijn de toegangsdoeleinden minstens even belangrijk als de doeleinden van initiële bewaring voor de behoeften van de operatoren (met name: de facturatie, de commercialisering van de diensten, de strijd tegen fraude en kwaadwillig gebruik van de netwerken en diensten of de beveiliging van de netwerken en diensten door de operatoren).

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. 127/1, § 2, 9°, van de telecomwet)

Hier dient een onderscheid gemaakt te worden tussen de opdracht van het BIPT als controleautoriteit voor de nationale bepalingen genomen in uitvoering van Richtlijn 2002/58 (e-Privacy) en de controleopdracht van het BIPT als controleautoriteit voor andere bepalingen (in het bijzonder de bepalingen van de telecomwet ter omzetting van het Europees wetboek voor elektronische communicatie).

En ce qui concerne le deuxième cas de figure, les missions d'application et de contrôle des dispositions de la loi télécom nécessitent parfois également la communication de métadonnées. Les catégories de données nécessaires pour ce faire sont également celles visées aux articles 122, 123, 126 et 127, à l'exclusion des données conservées en vertu de l'article 126/1.

Dans certains cas, tel qu'en matière de lutte contre les fraudes (article 121/8 de la loi télécom), la communication de métadonnées brutes est indispensable de manière à vérifier le respect par l'opérateur de son obligation de prendre les mesures appropriées. Comme en matière de sécurité des réseaux, il n'est pas possible d'effectuer une analyse correcte si celle-ci est fondée sur des données fictives.

Dans d'autres cas, tel que par exemple, lors du contrôle du respect par les opérateurs de leurs obligations en matière de protection des utilisateurs (p.ex. facturation détaillée), le recours à des données pseudonymes, voire anonymes, pourra faire partie des garanties de sécurité prises, sans que cela nuise à la finalité poursuivie. Tel pourra être le cas notamment lorsque la finalité requiert uniquement de pouvoir obtenir des données agrégées (tel que la détermination de la couverture du territoire national par les réseaux mobiles).

Concernant le premier cas de figure (la mission de l'IBPT en tant qu'autorité de contrôle des dispositions nationales prises en application de la directive 2002/58 (e-privacy)), les articles 15, § 3, et 25, § 3, en projet prévoient que l'IBPT et ses officiers de police judiciaire peuvent consulter les bases de données mettant en œuvre les articles 122, 123, 126, 126/1 et 127 de la loi télécom afin de contrôler le respect, par un opérateur, de ces dispositions.

Il convient de noter qu'une même mission de l'IBPT peut ressortir de plusieurs finalités. Par exemple, la sécurité des réseaux peut ressortir de la prévention de menaces graves contre la sécurité publique et du contrôle de la loi télécom, en plus de la finalité "sécurité des réseaux".

Paragraphe 1er: demande de données d'identification

En cas de demande de données d'identification, il est prévu que la demande motivée soit envoyée par l'Institut, dont le pouvoir de décision est exercé de façon collégiale par son Conseil. S'agissant d'une demande de données considérée comme "moins intrusive" par la jurisprudence précitée, le contrôle interne de la demande est assuré par cet exercice collectif du pouvoir de décision.

Wat betreft het tweede geval, is voor de opdrachten van toepassing en controle van de bepalingen van de telecomwet soms ook de verstrekking van metagegevens vereist. De daartoe noodzakelijke categorieën van gegevens zijn ook deze beoogd in de artikelen 122, 123, 126 en 127 van de telecomwet, met uitzondering van de gegevens bewaard op grond van het artikel 126/1.

In bepaalde gevallen, zoals bij de strijd tegen fraude (artikel 121/8 van de telecomwet), is het onontbeerlijk om ruwe metagegevens te verstrekken zodat de inachtneming door de operator van zijn verplichting om de gepaste maatregelen te treffen, kan worden geverifieerd. Net zoals op het stuk van netwerkveiligheid is het niet mogelijk om een correcte analyse te maken indien deze is gebaseerd op fictieve gegevens.

In andere gevallen zoals bij de controle of de operatoren hun verplichtingen naleven inzake bescherming van de gebruikers (bijv. gespecificeerde facturatie), zal het gebruik van pseudonieme, of zelfs anonieme, gegevens, deel kunnen uitmaken van de veiligheidswaarborgen waarin werd voorzien, zonder dat dat afbreuk doet aan het beoogde doel. Dat zal met name het geval kunnen zijn wanneer het doel enkel vereist dat samengevoegde gegevens kunnen worden verkregen (zoals de bepaling van de dekking van het nationale grondgebied door de mobiele netwerken).

Wat het eerste geval betreft (de opdracht van het BIPT als controleautoriteit voor de nationale bepalingen genomen in toepassing van Richtlijn 2002/58 (e-Privacy)), bepalen de ontwerpartikelen 15, § 3, en 25, § 3, dat het BIPT en zijn officieren van gerechtelijke politie de databanken die uitvoering verlenen aan de artikelen 122, 123, 126, 126/1 en 127 van de telecomwet mogen raadplegen teneinde de inachtneming van deze bepalingen door de operator te verifiëren.

Er dient te worden opgemerkt dat eenzelfde opdracht van het BIPT verscheidene doeleinden kan hebben. Zo kan de netwerkbeveiliging kaderen in de preventie van ernstige bedreigingen voor de openbare veiligheid en de controle van de telecomwet, boven op het doel van "netwerkveiligheid".

Paragraaf 1: verzoek om identificatiegegevens

In geval van een verzoek om identificatiegegevens, wordt bepaald dat het met redenen omkleed verzoek wordt verzonden door het Instituut, waarvan de beslissingsbevoegdheid collegiaal wordt uitgeoefend door zijn Raad. Omdat het gaat om een verzoek om gegevens die door de voormelde rechtspraak als "minder indringend" worden beschouwd, wordt de interne controle van het verzoek gewaarborgd door deze collectieve uitoefening van de beslissingsbevoegdheid.

Au considérant 95 de son avis n° 66/2022 du 1er avril 2022, l'APD a confirmé que les modalités prévues par la loi statut en projet pour la communication et l'accès aux données relatives à l'abonné ou à l'utilisateur habituel du service (dorénavant les demandes de données d'identification) sont conformes aux exigences énoncées par la Cour constitutionnelle dans son arrêt n° 158/2021.

Paragraphe 2: demande de métadonnées

Le paragraphe 2 vise l'application et le contrôle des mêmes normes que celles visées au paragraphe 1er lorsque ces mêmes missions nécessitent la communication de certaines métadonnées, autres que celles visées au paragraphe 1er et considérées comme "plus intrusives" par la jurisprudence précitée.

Dans son arrêt du 18 novembre 2021 précité, la Cour constitutionnelle a rappelé que, s'agissant de telles données, la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme exigent un contrôle judiciaire ou administratif préalable ("contrôle externe"). Dans ce contexte, et de manière à pouvoir rencontrer cette condition, le gouvernement a décidé de confier cette tâche à l'Autorité de protection des données. À cet effet, certaines modifications seront apportées à la loi du 3 décembre 2017 portant création de l'Autorité de protection des données de manière à préciser la procédure applicable.

Pour ce qui concerne l'accès à ces autres métadonnées ("plus intrusives"), l'APD a précisé aux considérants 66 et 67 de son avis n° 32/2021 du 16 février 2022 qu': "au vu de la gravité des risques d'abus, l'Autorité estime, conformément à la jurisprudence européenne, que les accès aux métadonnées de communication qui ont lieu dans le cadre de missions qui impliquent la prise de décisions coercitives à l'égard des personnes concernées ou qui impliquent une collecte massive de métadonnées de communications électroniques, doivent faire l'objet d'un contrôle indépendant par un organe qui dispose d'une expertise technique suffisante."

Dans son avis, l'APD précise également que "pour les missions de l'IBPT et du CCB qui n'impliquent ni de collecter les métadonnées de communications électroniques "en masse" ni la prise de décision coercitive à l'égard des personnes concernées, en lieu et place de prévoir un système d'autorisation préalable, c'est au législateur qu'il revient d'encadrer adéquatement cet accès en le limitant à des données anonymisées,

In considerans 95 van haar advies nr. 66/2022 van 1 april 2022 heeft de GBA bevestigd dat de nadere bepalingen vastgelegd in de ontwerpstatuutwet voor de communicatie en de toegang tot de gegevens met betrekking tot de abonnee of de gewoonlijke gebruiker van de dienst (voortaan de verzoeken om identificatiegegevens), in overeenstemming zijn met de vereisten die het Grondwettelijk Hof heeft vastgesteld in zijn arrest nr. 158/2021.

Paragraaf 2: verzoek om metagegevens

Paragraaf 2 beoogt de toepassing en de controle van dezelfde normen als diegene die beoogd worden in paragraaf 1, wanneer diezelfde opdrachten nopen tot de mededeling van sommige metagegevens, andere dan die welke in paragraaf 1 worden beoogd en die door de voormelde rechtspraak beschouwd worden als "indringender".

In zijn voormelde arrest van 18 november 2021 heeft het Grondwettelijk Hof eraan herinnerd dat wat dergelijke gegevens betreft het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens een voorafgaande gerechtelijke of administratieve controle ("externe controle") eisen. In die context en om aan die voorwaarden te kunnen voldoen heeft de regering beslist om die taak toe te vertrouwen aan de Gegevensbeschermingsautoriteit. Daartoe zullen een aantal wijzigingen worden aangebracht in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, om de toepasselijke procedure te verduidelijken.

Wat betreft de toegang tot deze andere ("meer indringende") metagegevens heeft de GBA in consideransen 66 en 67 van haar advies nr. 32/2021 van 16 februari 2022 verduidelijkt dat: "Gezien de ernst van de risico's op misbruik, is de Autoriteit bovendien, in overeenstemming met de Europese rechtspraak, van mening dat de toegangen tot de metagegevens van communicatie die plaatsvinden in het kader van opdrachten die het nemen van dwangbesluiten ten aanzien van betrokkenen impliceren of die een massale verzameling van metagegevens van elektronische communicatie impliceren, moeten worden onderworpen aan een onafhankelijke controle door een instantie die beschikt over toereikende technische expertise."

In haar advies preciseert de GBA eveneens: "Voor de opdrachten van het BIPT en het CCB die geen dwangbesluit impliceren ten aanzien van betrokkenen en die geen massale verzameling van metagegevens van elektronische communicatie impliceren, komt het daarentegen toe aan de wetgever om deze toegang passend te regelen door die te beperken tot geanonimiseerde gegevens, of ook gepseudonimiseerde

voire pseudonymisées tout en sécurisant l'utilisation de la clef de pseudonymisation et en prévoyant toute autre mesure adéquate" (cons. 67 et conclusion).

Cette proposition de l'APD (à savoir l'absence de contrôle préalable externe lorsqu'il n'y a pas de collecte de métadonnées "en masse" ni de prise de décision coercitive à l'égard des personnes concernées et que les données ont été rendues anonymes ou pseudonymes) n'a pas été suivie pour les raisons suivantes:

— ces éléments ne figurent pas, ou à tout le moins, pas expressément dans la jurisprudence de la Cour de Justice de l'Union européenne à ce jour et, par précaution, il semble préférable de faire preuve de réserve à cet égard;

— Les termes "en masse" ne sont par ailleurs pas définis et peuvent prêter à des interprétations divergentes.

Au point 92 de son avis, l'APD "souligne, en particulier, que s'il est possible que l'IBPT remplisse toutes ou certaines des missions énumérées ci-dessus à l'aide de données anonymisées ou pseudonymisées, le projet doit prévoir que seules des données anonymisées ou pseudonymisées pourront leur être transmises".

Pour tenir compte de ce point, l'article 15, § 2, prévoit que l'IBPT devra obtenir de l'opérateur des données anonymes ou pseudonymes lorsque cela ne nuit pas à l'objectif poursuivi. Par ailleurs, l'article 15, § 4, prévoit que lorsque l'IBPT estime que de telles données nuisent à cet objectif, il devra le justifier dans la demande adressée à l'APD.

Paragraphe 3: contrôle de la section "Secret des communications"

Le paragraphe 3 vise la situation spécifique dans laquelle l'IBPT agit en tant qu'autorité de contrôle des dispositions nationales prises en application de la directive 2002/58 ("e-privacy"), à savoir les dispositions prévues sous le Titre IV, Chapitre III, Section 2 de la loi télécom "Secret des communications, traitement des données et protection de la vie privée".

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

gegevens, en daarbij het gebruik van de pseudonimiseringssleutel te beveiligen en te voorzien in alle andere passende maatregelen, liever dan te voorzien in een systeem van voorafgaande toestemming." (cons. 67 en conclusie).

Dit voorstel van de GBA (met name geen externe voorafgaande controle wanneer er geen sprake is van een "massale" verzameling aan metagegevens en wanneer er geen dwangbesluit wordt genomen ten aanzien van de betrokkenen en de gegevens geanonimiseerd of gepseudonimiseerd werden), werd niet gevolgd om de volgende redenen:

— deze elementen zijn op heden niet opgenomen, of toch niet uitdrukkelijk, in de rechtspraak van het Europese Hof van Justitie en het lijkt verkieslijk om, uit voorzorg, enige behoedzaamheid aan de dag te leggen wat dit betreft;

— de term "massale" is overigens niet gedefinieerd en kan leiden tot uiteenlopende interpretaties.

In punt 92 van haar advies benadrukt de GBA dat "indien het mogelijk is dat het BIPT alle of sommige van de hierboven opgesomde taken uitvoert met behulp van geanonimiseerde of gepseudonimiseerde gegevens, het ontwerp moet bepalen dat alleen geanonimiseerde of gepseudonimiseerde gegevens aan hen kunnen worden doorgegeven".

Om rekening te houden met dat punt bepaalt artikel 15, § 2, dat het BIPT van de operator anonieme of pseudonieme gegevens zal moeten krijgen wanneer dat geen afbreuk doet aan het beoogde doel. Artikel 15, § 4, schrijft voor dat wanneer het BIPT meent dat dergelijke gegevens afbreuk doen aan dit doel, het dat zal moeten rechtvaardigen in de aanvraag gericht aan de GBA.

Paragraaf 3: controle van het deel "Geheimhouding van de communicatie"

Paragraaf 3 beoogt de specifieke situatie waarin het BIPT optreedt als controleoverheid van de nationale bepalingen genomen in toepassing van Richtlijn 2002/58 ("e-Privacy"), namelijk de bepalingen vastgesteld in Titel IV, Hoofdstuk III, Afdeling 2 van de telecomwet "Geheimhouding van de communicatie, verwerking van de gegevens en bescherming van de persoonlijke levenssfeer".

Artikel 15*bis*, § 3, van de richtlijn schrijft voor: "De lidstaten zorgen ervoor dat de bevoegde nationale instantie 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

respect des dispositions nationales adoptées en application de la présente directive."

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 puisse être exigé par l'IBPT, puisque ce contrôle vise précisément à rechercher et détecter l'existence d'infractions éventuelles.

Lorsque l'IBPT agit en tant qu'autorité de contrôle des dispositions nationales prises en application de la directive 2002/58 ("e-privacy"), soumettre la demande d'accès envers l'opérateur qui est nécessaire pour effectuer ce contrôle à un contrôle préalable par une juridiction ou une autre autorité administrative indépendante reviendrait dans ce cas-ci à contrôler le "contrôleur" du respect des dispositions protectrices de la vie privée et à s'immiscer dans la marge d'appréciation dont bénéficie l'IBPT pour l'exercice de son contrôle du respect de ces dispositions. Une telle logique ne peut être suivie. Cette analyse est confirmée par l'APD (cf. considérant 103 de son avis n° 66/2022 du 1er avril 2022).

Dès lors, dans ce cadre précis, le Conseil de l'IBPT peut collégialement décider d'effectuer un contrôle du respect de ces dispositions en exigeant d'un opérateur l'accès permettant de consulter les bases de données concernées à des fins de contrôle.

Les articles 126, 126/1, 126/2 et 127, qui sont des dispositions dont le non-respect est sanctionné pénalement (voir article 145, § 1er, de la loi télécom) sont repris dans le paragraphe 3 pour les raisons suivantes. Les officiers de police judiciaire (OPJ) de l'IBPT peuvent être amenés à contrôler le respect de ces articles et de leurs arrêtés d'exécution, en exigeant de l'opérateur contrôlé de pouvoir accéder à une base de données qui contient les données conservées en vertu d'un de ces articles ou d'un de leur arrêté d'exécution.

En cas d'infraction, un OPJ de l'IBPT rédigera un PV et enverra ce PV au procureur du Roi et une copie de ce PV au Conseil de l'IBPT. Sur base de l'article 21/1 de la loi IBPT-statut, en concertation avec le procureur du Roi, l'Institut peut se charger de poursuivre les manquements de l'opérateur repris dans le PV. La procédure d'infraction devient alors

deze richtlijn vastgestelde nationale bepalingen te monitoren en na te doen leven."

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 kan eisen, aangezien die controle net tot doel heeft het bestaan van eventuele inbreuken te onderzoeken en op te sporen.

Wanneer het BIPT optreedt als toezichthoudende autoriteit met betrekking tot de nationale bepalingen die genomen zijn overeenkomstig Richtlijn 2002/58 ("e-Privacy"), 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. Deze analyse wordt bevestigd door de GBA (cf. considerans 103 van haar advies 66/2022 van 1 april 2022).

In dit specifieke kader kan de Raad van het BIPT dan ook collegiaal beslissen om een controle te verrichten van de naleving van deze bepalingen door van een operator de toegang te eisen zodat de betreffende databanken voor controledoeleinden geraadpleegd kunnen worden.

De artikelen 126, 126/1, 126/2 en 127, welke bepalingen zijn waarvan de niet-naleving strafrechtelijk bestraft wordt (zie artikel 145, § 1, van de telecomwet) worden opgenomen in paragraaf 3 om de volgende redenen. Het kan gebeuren dat de officieren van gerechtelijke politie (OGP) van het BIPT de naleving van deze artikelen en van de uitvoeringsbesluiten ervan moeten controleren, waarbij van de gecontroleerde operator verlangd wordt om toegang te krijgen tot een databank die de krachtens een van die artikelen of een van de uitvoeringsbesluiten ervan bewaarde gegevens bevat.

In geval van een inbreuk zal een OGP van het BIPT een proces-verbaal opstellen en dat pv verzenden naar de procureur des Konings en een kopie van dat pv naar de Raad van het BIPT. Op grond van artikel 21/1 van de BIPT-statuutwet, kan het Instituut in overleg met de procureur des Konings de taak op zich nemen om de in het pv vermelde inbreuken van

administrative. On ne peut pas exclure que dans le cadre de cette procédure administrative, un nouvel accès à une base de données de l'opérateur soit nécessaire, par exemple pour contrôler que l'opérateur s'est mis en ordre avec la législation. Ce nouvel accès ne peut plus être autorisé par les OPJ de l'IBPT, vu que la procédure n'est plus pénale. Par conséquence, c'est l'IBPT (représenté par son Conseil) qui devra exiger ce nouvel accès à la base de données.

Paragraphe 4: la motivation des demandes et le registre

Le paragraphe 4 a pour objectif d'incorporer dans la loi-statut les exigences en termes de motivation posées par la Cour constitutionnelle dans son arrêt n° 158/2021 du 18 novembre 2021, point B.16.8.7, qui se lit comme suit: "B.16.8.7. Cela étant, la demande d'accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005 doit toujours être motivée in concreto par la démonstration du lien entre ces données et les éléments objectifs qui fondent la suspicion concrète initiale à l'égard de l'utilisateur final en question concernant une infraction spécifique. Il faut également motiver le fait que l'on ne demande pas davantage de données que celles qui sont strictement nécessaires dans le cadre de l'enquête en cours. Une telle motivation ne peut pas recourir à des formulations types ou à des formules de style."

En outre, suite à l'avis n° 66/2022 de l'APD du 1er avril 2022, il est ajouté au paragraphe 4 que seront précisées dans la motivation de la demande envers l'APD:

— la raison pour laquelle la communication par l'opérateur de données anonymisées ne permet pas de rencontrer l'objectif poursuivi (en cas demande de données anonymes, le demande envers l'opérateur n'est soumise au contrôle de l'APD), et;

— la raison pour laquelle la communication par l'opérateur de données pseudonymisées ne permet pas de rencontrer l'objectif poursuivi, lorsque la demande de métadonnées de l'IBPT ne précise pas que l'opérateur doit y répondre avec des données pseudonymisées.

Ceci permet de garantir que des données "brutes" ne seront pas demandées lorsque ce n'est pas nécessaire.

de operator te vervolgen. De inbreukprocedure wordt dan administratief. Er kan niet worden uitgesloten dat in het kader van deze administratieve procedure een nieuwe toegang tot een databank van de operator noodzakelijk is, bijvoorbeeld om te controleren of de operator zich naar de wetgeving geschikt heeft. Die nieuwe toegang mag niet meer worden toegestaan door de OGP's van het BIPT, aangezien de procedure niet langer strafrechtelijk is. Bijgevolg is het het BIPT (vertegenwoordigd door zijn Raad) dat deze nieuwe toegang tot de databank zal moeten eisen.

Paragraaf 4: de motivering van de verzoeken en de inventaris

Paragraaf 4 heeft tot doel in de statuutwet de eisen inzake motivering op te nemen die zijn gesteld door het Grondwettelijk Hof in zijn arrest nr. 158/2021 van 18 november 2021, punt B.16.8.7, dat luidt: "B.16.8.7. Wel dient het verzoek om toegang tot de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens steeds in concreto te worden gemotiveerd door het verband aan te tonen tussen die gegevens en de objectieve elementen die de initiële concrete verdenking van de betrokken eindgebruiker voor een specifiek misdrijf ondersteunen. Tevens dient te worden gemotiveerd dat er niet meer gegevens worden opgevraagd dan strikt noodzakelijk is in het licht van het lopende onderzoek. Een dergelijke motivering mag geen gebruik maken van standaardformuleringen of stijlformules."

Naar aanleiding van het advies nr. 66/2022 van de GBA van 1 april 2022 wordt in paragraaf 4 toegevoegd dat het volgende zal worden gepreciseerd in de motivering van het verzoek aan de GBA:

— de reden waarom het voor het beoogde doel niet volstaat dat de operator geanonimiseerde gegevens verstrekt (in geval van verzoek om geanonimiseerde gegevens, wordt het verzoek niet ter controle voorgelegd aan de GBA), en;

— de reden waarom het voor het beoogde doel niet volstaat dat de operator gepseudonimiseerde gegevens verstrekt wanneer het verzoek om metagegevens van het BIPT niet preciseert dat de operator moet antwoorden met gepseudonimiseerde gegevens.

Dit maakt het mogelijk dat er geen "ruwe" gegevens worden gevraagd wanneer dat niet nodig is.

Afin de permettre un contrôle interne des demandes que l'IBPT adresse aux opérateurs, un inventaire de ces demandes sera tenu auprès de l'IBPT.

Information de la personne concernée

Une information de la personne concernée n'est pas prévue car cette dernière n'aurait pas de sens pratique. Lorsque l'IBPT est confronté à un incident de sécurité qui affecte le réseau d'un opérateur, il n'a pas connaissance de l'identité de l'auteur de l'attaque, qu'il revient aux autorités judiciaires de rechercher.

Lorsque l'IBPT contrôle le respect des articles 122 et 123 de la loi télécom ou le respect des exigences en matière de facturation, il contrôle l'opérateur et non des individus.

En outre, conformément à l'article 14, § 5, b), du RGPD, il est permis de déroger au droit de la personne concernée d'être informée de chaque traitement de ses données à caractère personnel lorsque les moyens qui devraient être déployés par le responsable du traitement pour informer la personne concernée du traitement seraient disproportionnés.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Om een interne controle mogelijk te maken van de verzoeken die het BIPT aan de operatoren richt, zal bij het BIPT een inventaris van die verzoeken bijgehouden worden.

Inlichting van de betrokken persoon

Er wordt niet voorzien in een inlichting aan de betrokken persoon omdat dit praktisch gezien geen zin zou hebben. Wanneer het BIPT geconfronteerd wordt met een beveiligingsincident dat het netwerk van een operator treft, heeft het geen kennis van de identiteit van de dader van de aanval; het is de taak van de gerechtelijke autoriteiten om die te zoeken.

Wanneer het BIPT de naleving van de artikelen 122 en 123 van de telecomwet of de naleving van de eisen inzake facturering controleert, dan controleert het de operator en niet de individuen.

Overeenkomstig artikel 14, § 5, b), van de AVG is het bovendien toegestaan om af te wijken van het recht van de betrokken persoon om te worden ingelicht over elke verwerking van zijn persoonsgegevens wanneer de middelen die de verwerkingsverantwoordelijke zou moeten inzetten om de betrokken persoon in te lichten over de verwerking, onevenredig zouden zijn.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 11 **DU GOUVERNEMENT**

Art. 19

Remplacer cet article par ce qui suit:

"Art. 19. L'article 24 de la même loi, dont le texte actuel devient le paragraphe 1er, est complété par le paragraphe 2 suivant:

"§ 2. Le Roi désigne, parmi les officiers de police judiciaire de l'Institut visés au § 1er, ceux qui sont chargés du contrôle des demandes visées à l'article 25/1, §§ 1 et 3.

Sans préjudice de l'article 25, paragraphe 5, les officiers de police judiciaire de l'Institut désignés par le Roi en vertu de l'alinéa 1er, exécutent leur mission en toute indépendance. Ils ne peuvent être soumis à aucun lien de subordination à l'égard des autres officiers de police judiciaire de l'Institut."."

JUSTIFICATION

Un nouveau paragraphe 2 est ajouté à l'article 24 existant de la loi statut IBPT de manière à créer un mécanisme interne de contrôle de la régularité des demandes visées à l'article 25/1, §§ 1 et 3 formulées par les officiers de police judiciaire de l'IBPT dans le cadre de la recherche et la constatation des infractions pénales qui relèvent de leurs compétences en vertu de l'article 24 § 1er.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Nr. 11 **VAN DE REGERING**

Art. 19

Dit artikel vervangen als volgt:

"Art. 19. Artikel 24 van dezelfde wet, waarvan de huidige tekst paragraaf 1 word, wordt aangevuld met de volgende paragraaf 2:

"§ 2. De Koning wijst onder de in § 1 bedoelde officieren van gerechtelijke politie van het Instituut diegenen aan die belast worden met de controle van de in artikel 25/1, §§ 1 en 3 beoogde verzoeken.

Onverminderd artikel 25, paragraaf 5, voeren de officieren van gerechtelijke politie van het Instituut die krachtens het eerste lid door de Koning aangesteld zijn, hun opdracht volledig onafhankelijk uit. Zij mogen niet worden onderworpen aan een ondergeschikt verband ten opzichte van de andere officieren van gerechtelijke politie van het Instituut."."

VERANTWOORDING

In het bestaande artikel 24 van de BIPT-statuutwet wordt een nieuwe paragraaf 2 toegevoegd zodat een intern mechanisme wordt ingesteld voor de controle van de regelmatigheid van de verzoeken bedoeld in artikel 25/1, §§ 1 en 3, die geformuleerd zijn door de officieren van gerechtelijk politie van het BIPT in het kader van de opsporing en vaststelling van de strafbare feiten die krachtens artikel 24, § 1, onder hun bevoegdheid vallen.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 12 **DU GOUVERNEMENT**

Art. 19/1 *(nouveau)*

Dans le chapitre 4, insérer un article 19/1, rédigé comme suit:

"Art. 19/1. Dans l'article 25 de la même loi, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 1er, les mots "membres du personnel visés à l'article 24" sont remplacés par les mots "officiers de police judiciaire de l'Institut";

2° au paragraphe 1er, alinéa 1er, les mots ", dans l'exercice de leur mission de police judiciaire" sont supprimés;

3° au paragraphe 3, les mots "membres du personnel visés à l'article 24" sont remplacés par les mots "officiers de police judiciaire de l'Institut";

4° au paragraphe 3, les mots ",en leur qualité d'officier de police judiciaire," sont supprimés;

5° aux paragraphes 4, 5, 6 et 7 les mots "de l'Institut" sont insérés après les mots "officiers de police judiciaire".".

JUSTIFICATION

Les modifications visent à assurer une cohérence de la terminologie utilisée dans les articles 24 à 25/1. Lorsqu'il est fait mention des officiers de police judiciaire de l'IBPT (à savoir les officiers de police judiciaire désignés en vertu de l'article 24, § 1er, il est entendu que l'on vise les membres du personnel de l'IBPT ayant cette qualité qui agissent dans le cadre de l'exercice de leurs missions d'officiers de police judiciaire.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Nr. 12 **VAN DE REGERING**

Art. 19/1 *(nieuw)*

In hoofdstuk 4, een artikel 19/1 invoegen, luidende:

"Art. 19/1. In artikel 25 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de woorden "personeelsleden vermeld in artikel 24" vervangen door de woorden "officieren van gerechtelijke politie van het Instituut";

2° in paragraaf 1, eerste lid, worden de woorden "in hun hoedanigheid van officier van gerechtelijke politie" geschrapt;

3° in paragraaf 3, worden de woorden "personeelsleden vermeld in artikel 24" vervangen door de woorden "officieren van gerechtelijke politie van het Instituut";

4° in paragraaf 3, worden de woorden "in hun hoedanigheid van officier van gerechtelijke politie" geschrapt;

5° in de paragrafen 4, 5, 6 en 7 worden de woorden "van het Instituut" ingevoegd na de woorden "officieren van gerechtelijke politie".".

VERANTWOORDING

De wijzigingen zijn erop gericht een coherentie te waarborgen van de terminologie die wordt gebruikt in de artikelen 24 tot 25/1. Wanneer sprake is van de officieren van gerechtelijke politie van het BIPT (namelijk de officieren van gerechtelijke politie die aangewezen zijn krachtens artikel 24, § 1, wordt daaronder verstaan de personeelsleden van het BIPT die deze hoedanigheid hebben en die optreden in het kader van de uitoefening van hun opdrachten als officieren van gerechtelijke politie.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 13 **DU GOUVERNEMENT**

Art. 19/2 *(nouveau)*

Dans le chapitre 4, insérer un article 19/2, rédigé comme suit:

"Art. 19/2. Dans le chapitre III, section 4, sous-section 1e de la même loi est inséré un article 25/1, rédigé comme suit:

"Art. 25/1. § 1er. Afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3bis, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°, un officier de police judiciaire de l'Institut peut, par écrit:

1° exiger d'un opérateur de répondre à une demande de données d'identification qui est nécessaire à ces fins;

2° requérir la collaboration des personnes et institutions visées à l'article 46quater, § 1er, du Code d'instruction criminelle et d'associations les représentant, sur la base de la référence de paiement en ligne spécifique à un service de communications électroniques qui a préalablement été communiquée par un opérateur conformément au 1°, afin d'identifier la personne qui a payé le service;

3° requérir la collaboration des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, où la souscription de l'abonné à un service de communications électroniques a été effectué, sur la base des coordonnées du centre ou du lieu d'hébergement qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné;

4° requérir la collaboration de toute autre personne morale qui est l'abonnée d'un opérateur ou qui souscrit à un service de communications électroniques au nom

Nr. 13 **VAN DE REGERING**

Art. 19/2 *(nieuw)*

In hoofdstuk 4, een artikel 19/2 invoegen luidende:

"Art. 19/2. In hoofdstuk III, afdeling 4, onderafdeling 1, van dezelfde wet wordt een artikel 25/1 ingevoegd, luidende:

"Art. 25/1. § 1. Om een inbreuk bedoeld in artikel 145, § 3 of § 3bis, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen, kan een officier van gerechtelijke politie van het Instituut, schriftelijk:

*1° van een operator eisen om te antwoorden op een verzoek om identificatiegegevens, d*at voor deze doeleinden noodzakelijk is*;*

2° de medewerking vorderen van de personen en instellingen bedoeld in artikel 46quater, § 1, van het Wetboek van Strafvordering en van verenigingen die hen vertegenwoordigen, op basis van het kenmerk van de onlinebetaling specifiek voor een elektronische-communicatiedienst die voorafgaand meegedeeld is door een operator overeenkomstig de bepaling onder 1°, om de persoon te identificeren die de dienst heeft betaald;

3° de medewerking vorderen van de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, waar de inschrijving van de abonnee op een elektronische-communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaand meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee te identificeren;

4° de medewerking vorderen van alle andere rechtspersonen die abonnee zijn van een operator, of die intekenen in naam en voor rekening van natuurlijke

et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné ou l'utilisateur habituel du service.

Une demande visée à l'alinéa 1er ne peut être transmise à un acteur visé à l'alinéa 1er qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée adressée à cet officier conformément au § 5.

§ 2. Pour les besoins de l'accomplissement de ses missions, un officier de police judiciaire de l'Institut peut exiger d'un opérateur, par écrit, de répondre à une demande de métadonnées, qui est nécessaire afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3, ou § 3bis, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°.

Sauf en cas d'urgence dûment justifié, l'officier de police judiciaire ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée au juge d'instruction et après autorisation écrite de ce dernier.

En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande et la justification de l'urgence. Un contrôle ultérieur est effectué par le juge d'instruction.

§ 3. Par dérogation aux paragraphes 1 et 2, afin de contrôler le respect des articles 126, 126/1, 126/2 ou 127 de la loi du 13 juin 2005 relative aux communications électroniques et de leurs arrêtés d'exécution et à la demande écrite et motivée d'un officier de

personen op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaand meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee of de gewoonlijke gebruiker van de dienst te identificeren.

Een in het eerste lid bedoeld verzoek mag aan een in het eerste lid bedoelde actor pas worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek gericht aan deze officier overeenkomstig § 5.

§ 2. Ten behoeve van de vervulling van zijn opdrachten kan een officier van gerechtelijke politie van het Instituut van een operator schriftelijk eisen om te antwoorden op een verzoek om metagegevens, die nodig zijn om een inbreuk bedoeld in artikel 145, § 3, of § 3bis, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid, mag de officier van gerechtelijke politie het verzoek aan de operator pas richten na het voorleggen van een schriftelijk en met redenen omkleed verzoek aan de onderzoeksrechter en na schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dit verzoek, de motivering van het verzoek alsook de rechtvaardiging van de hoogdringendheid mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.

§ 3. In afwijking van de paragrafen 1 en 2, teneinde de naleving te controleren van de artikelen 126, 126/1, 126/2 of 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van de uitvoeringsbesluiten ervan en op schriftelijk en met redenen omkleed

police judiciaire de l'Institut, un opérateur fournit, dans le délai fixé dans le réquisitoire, un accès permettant de consulter ses bases de données qui mettent en œuvre un de ces articles ou un de ces arrêtés d'exécution.

Une demande visée à l'alinéa 1er ne peut être transmise à un opérateur qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, paragraphe 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée conformément au § 5.

La demande adressée à l'opérateur précise les noms des officiers de police judiciaire de l'Institut qui peuvent consulter la base de données.

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.

§ 4. Pour l'application des paragraphes 1er et 2, les acteurs visés au paragraphe 1er, alinéa 1er, 1° à 4°, auxquels un officier de police judiciaire de l'Institut a demandé des données lui communiquent ces données en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire.

Pour l'application des paragraphes 1 à 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 communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

Toute personne qui refuse de permettre la consultation de la base de données conformément au paragraphe 3 ou qui ne permet pas cette consultation dans

verzoek van een officier van gerechtelijke politie van het Instituut, verleent een operator binnen de termijn die vastgesteld is in de vordering toegang zodat zijn databanken die een van deze artikelen of een van deze uitvoeringsbesluiten uitvoeren, geraadpleegd kunnen worden.

Een in het eerste lid bedoeld verzoek mag pas naar een operator worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, paragraaf 2, bedoelde officier van gerechtelijke politie. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek overeenkomstig § 5.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de officieren van gerechtelijke politie van het Instituut die de databank kunnen raadplegen.

Deze officieren mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

§ 4. Voor de toepassing van de paragrafen 1 en 2, delen de actoren bedoeld in paragraaf 1, eerste lid, 1° tot 4°, aan wie een officier van gerechtelijke politie van het Instituut gegevens gevraagd heeft, de gevraagde gegevens mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

Voor de toepassing van de paragrafen 1 tot 3, is iedere persoon die uit hoofde van zijn functie kennis krijgt van de maatregel of daaraan zijn medewerking verleent, tot geheimhouding verplicht. Iedere schending van de geheimhoudingsplicht wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

Iedere persoon die weigert de raadpleging van de databank mogelijk te maken overeenkomstig paragraaf 3 of die deze raadpleging niet mogelijk maakt

le délai fixé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

§ 5. Pour l'application des paragraphes 1 à 3, la motivation de la demande adressée à l'officier de police judiciaire visé à l'article 24, § 2, ou au juge d'instruction doit être développée au regard des circonstances de l'enquête.

Pour l'application des paragraphes 1 et 2, cette motivation doit indiquer:

1° le lien entre les données demandées et l'objectif de recherche, de constat ou de poursuite de l'infraction spécifique qui justifie la demande;

2° le caractère strictement nécessaire des données demandées dans le cadre de l'enquête.

§ 6. Les officiers de police judiciaire de l'Institut consignent dans un registre:

1° l'ensemble des demandes visées aux paragraphes 1, 2 et 3;

2° la motivation de la demande et la justification de l'urgence communiquées au juge d'instruction conformément au paragraphe 2, alinéa 3;

3° les autorisations prévues aux paragraphes 1, 2 et 3."."

binnen de termijn bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

§ 5. Voor de toepassing van de paragrafen 1 tot 3 moet de motivering van het verzoek gericht aan de officier van gerechtelijke politie bedoeld in artikel 24, § 2, of aan de onderzoeksrechter uitgewerkt zijn in het licht van de omstandigheden van het onderzoek.

Voor de toepassing van de paragrafen 1 en 2 moet deze motivering vermelden:

1° het verband tussen de gevraagde gegevens en het doel van de opsporing, vaststelling of de vervolging van de specifieke inbreuk dat het verzoek rechtvaardigt;

2° de strikt noodzakelijke aard van de gegevens die worden gevraagd in het kader van het onderzoek.

§ 6. De officieren van gerechtelijke politie van het Instituut nemen op in een inventaris:

1° alle verzoeken waarvan sprake in de paragrafen 1, 2 en 3;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de onderzoeksrechter overeenkomstig paragraaf 2, derde lid;

3° de in de paragrafen 1, 2 en 3 bedoelde toestemmingen."."

JUSTIFICATION

Introduction pour les paragraphes 1 et 2

Les paragraphes 1 et 2 du nouvel article 25/1 visent les infractions suivantes:

— les infractions à l'article 145, § 3, de la loi du 13 juin 2005 relative aux communications électroniques, qui prévoit ce qui suit: "§ 3. Est punie d'une amende de 500 à 50 000 euros et d'une peine d'emprisonnement d'un

VERANTWOORDING

Inleiding voor de paragrafen 1 en 2

De paragrafen 1 en 2 van het nieuwe artikel 25/1 doelen op de volgende inbreuken:

— de inbreuken waarvan sprake in artikel 145, § 3, van de wet van 13 juni 2005 betreffende de elektronische communicatie, dat het volgende bepaalt: "§ 3. Met een geldboete van 500 tot 50 000 euros en met een gevangenisstraf van één

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;

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.";

— Les infractions à l'article 145, § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques, qui prévoit ce qui suit: "§ 3*bis*. Est punie d'une amende de 50 euros à 300 euros 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."

— les infractions visées à l'article 24, § 1er, alinéa 1er, 2°, de la loi IBPT-statut, à savoir "des infractions au Code pénal et aux lois spéciales lorsque les infractions sont commises 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."

Toutes ces infractions ont en commun qu'elles sont commises à l'aide d'un réseau ou service de communications électroniques.

Ces infractions incluent notamment les cas de 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 25/1, paragraphes 1 et 2, il convient de rappeler que le Code pénal est assimilé à une loi.

Les procédures prévues aux paragraphes 1 et 2 de l'article 25/1 de la loi IBPT-statut en cas d'infraction à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°,

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;

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.";

— De inbreuken waarvan sprake in artikel 145, § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie, dat het volgende bepaalt: "§ 3*bis*. Met een geldboete van 50 euros tot 300 euros 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."

— de inbreuken bedoeld in artikel 24, § 1, eerste lid, 2°, van de BIPT-statuutwet, namelijk "inbreuken op het Strafwetboek en op de bijzondere wetten wanneer die inbreuken worden gepleegd door middel van apparatuur, netwerken of diensten van elektronische communicatie of radiocommunicatie in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie."

Al deze inbreuken hebben met elkaar gemeen dat ze worden gepleegd met behulp van een netwerk of dienst voor elektronische communicatie.

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 25/1, de paragrafen 1 en 2, moet eraan worden herinnerd dat het Strafwetboek wordt gelijkgesteld met een wet.

De procedures die zijn vastgesteld in de paragrafen 1 en 2 van artikel 25/1 van de BIPT-statuutwet in geval van inbreuk op artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie

de la loi IBPT-statut, sont sans préjudice de l'application des règles classiques du Code d'instruction criminelle.

En effet, il reste toujours possible pour ce type d'infraction de mettre en œuvre le Code d'instruction criminelle (réquisitoire du procureur du Roi pour ce qui concerne les demandes de données d'identification et réquisitoire du juge d'instruction pour ce qui concerne les demandes de métadonnées). Cela se comprend dès lors que les OPJ de l'IBPT ne sont pas les seuls à pouvoir dresser un procès-verbal pour les infractions précitées.

Dans un souci d'efficacité et lorsqu'un opérateur informe l'IBPT d'une infraction potentielle à une loi visée à l'article 24, paragraphe 1er, il est essentiel que l'opérateur lui communique dès le départ les données d'identification et les métadonnées qui sont nécessaires pour que les officiers de police judiciaire de l'IBPT puissent rechercher, constater ou poursuivre cette infraction.

Paragraphe 1: la demande de données d'identification

Selon l'article 46*bis* du Code d'instruction criminelle, une demande de données d'identification envers un opérateur télécom doit faire l'objet d'un réquisitoire du procureur du Roi. L'article 25/1, paragraphe 1er, de la loi IBPT-statut prévoit une procédure différente, qui est la suivante.

Il y a deux groupes d'officiers de police judiciaires (OPJ) parmi les officiers de police judiciaire de l'IBPT:

— les officiers de police judiciaire qui sont chargés de rédiger les demandes pour les opérateurs et autres acteurs concernés;

— les officiers de police judiciaire qui sont chargés de contrôler ces demandes.

Un OPJ de l'IBPT qui est chargé de rédiger les demandes pour les opérateurs et les autres acteurs concernés adresse une demande écrite et motivée à un officier de police judiciaire de l'IBPT qui est chargé de contrôler ces demandes. Après approbation écrite de ce dernier officier, la demande pourra être envoyée à l'acteur concerné.

La procédure différente prévue dans la loi IBPT-statut par rapport à l'article 46*bis* du Code d'instruction criminelle se justifie comme suit.

of op artikel 24, § 1, 2°, van de BIPT-statuutwet, doen geen afbreuk aan de toepassing van de klassieke regels van het Wetboek van Strafvordering.

Voor dit soort van inbreuken blijft het immers altijd mogelijk om een beroep te doen op het Wetboek van Strafvordering (vordering van de procureur des Konings wat betreft de verzoeken om identificatiegegevens en vordering van de onderzoeksrechter wat betreft de verzoeken om metagegevens). Dat is te begrijpen doordat de OGP's van het BIPT niet de enigen zijn die een proces-verbaal mogen opstellen voor de voormelde inbreuken.

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, paragraaf 1, is het van fundamenteel belang dat de operator meteen de identificatie- en metagegevens eraan meedeelt die nodig zijn opdat de officieren van gerechtelijke politie van het BIPT die inbreuk kunnen opsporen, vaststellen of vervolgen.

Paragraaf 1: verzoek om identificatiegegevens

Volgens artikel 46*bis* van het Wetboek van Strafvordering moet een verzoek om identificatiegegevens aan een telecomoperator het voorwerp uitmaken van een vordering van de procureur des Konings. Artikel 25/1, paragraaf 1, van de BIPT-statuutwet voorziet in een andere procedure, die als volgt is.

Er zijn twee groepen van officieren van gerechtelijke politie (OGP) onder de officieren van gerechtelijke politie van het BIPT:

— de officieren van gerechtelijke politie die belast zijn met het opstellen van de verzoeken voor de operatoren en andere betrokken actoren;

— de officieren van gerechtelijke politie die belast zijn met de controle van die verzoeken.

Een OGP van het BIPT die ermee belast is de verzoeken voor de operatoren en de andere betrokken actoren op te stellen richt een schriftelijk en met redenen omkleed verzoek aan een officier van gerechtelijke politie van het BIPT die belast is met de controle van die verzoeken. Na schriftelijke goedkeuring van die laatste officier zal het verzoek mogen worden verzonden naar de betrokken actor.

De procedure waarin de BIPT-statuutwet voorziet en die verschilt van artikel 46*bis* van het Wetboek van Strafvordering wordt als volgt gerechtvaardigd.

Une première justification est la nature particulière des infractions visées aux paragraphes 1er et 2 du nouvel article 25/1.

Comme il a été indiqué ci-dessus, toutes ces infractions ont en commun qu'elles sont commises à l'aide d'un réseau ou service de communications électroniques.

Par conséquent, la recherche de l'auteur de ces infractions ne sera possible qu'au moyen des "traces numériques" que cet auteur laisse en utilisant le réseau ou le service de communications électroniques.

La tâche des officiers de police judiciaire de l'IBPT consistera d'abord à vérifier que l'infraction est bien établie. Ces officiers sont bien placés pour examiner la matérialité des faits, vu leur expertise technique dans le secteur des communications électroniques.

En pratique, il apparaît facilement si un fait est ou pas une infraction aux dispositions précitées (smishing, spoofing, etc.).

Les seules actions que les OPJ de l'IBPT peuvent entreprendre par rapport à ce type d'infraction est essayer d'exploiter les "traces numériques" qu'elles laissent.

La mesure la moins intrusive au niveau de la vie privée est d'essayer d'identifier l'auteur de la communication à l'origine de l'infraction. Pour ce faire, les OPJ de l'IBPT auront besoin de pouvoir demander à l'opérateur concerné de répondre à une demande de données d'identification. S'agissant de la poursuite d'une finalité pénale, il va de soi que l'utilisation de données anonymes ou pseudonymes n'aurait aucun sens.

Il en résulte que pour retrouver l'auteur de l'infraction, la marge de manœuvre des officiers de police judiciaires de l'IBPT est très limitée.

Une deuxième justification est que le paragraphe 1er du nouvel article 25/1 de la loi IBPT-statut ne permet aux officiers de police judiciaire de l'IBPT que d'adresser une demande de données d'identification (demande de données qui n'est pas considérée comme constituant une ingérence grave dans la vie privée des individus) et que l'autorisation du juge d'instruction est nécessaire conformément au paragraphe 2 pour obtenir des métadonnées (demande constituant une ingérence grave dans la vie privée des individus).

Een eerste rechtvaardiging is de bijzondere aard van de inbreuken bedoeld in de paragrafen 1 en 2 van het nieuwe artikel 25/1.

Zoals hierboven vermeld, hebben al deze inbreuken met elkaar gemeen dat ze worden gepleegd met behulp van een netwerk of dienst voor elektronische communicatie.

Bijgevolg zal naar de dader van deze inbreuken maar gezocht kunnen worden door middel van de "digitale sporen" die deze dader achterlaat bij het gebruik van het netwerk of de dienst voor elektronische communicatie.

De taak van de officieren van gerechtelijke politie van het BIPT zal er eerst in bestaan na te gaan of de inbreuk vaststaat. Deze officieren zijn, gelet op hun technische expertise in de elektronische-communicatiesector, aangewezen om de werkelijkheid van de feiten te onderzoeken.

In de praktijk is snel duidelijk of een feit al dan niet een inbreuk vormt op de voormelde bepalingen (smishing, spoofing, enz.).

De enige acties die de OGP's van het BIPT mogen ondernemen ten aanzien van dergelijke inbreuken is te proberen om zich de "digitale sporen" die ze achterlaten, ten nutte te maken.

De maatregel die het minst in de privacy indringt, bestaat erin om te proberen de auteur van de communicatie aan de oorsprong van de inbreuk te identificeren. Daartoe is het nodig dat de OGP's van het BIPT aan de betrokken operator kunnen vragen om te antwoorden op een verzoek om identificatiegegevens. Wat betreft de vervolging van een strafrechtelijk doeleinde, spreekt het voor zich dat het gebruik van geanonimiseerde of gepseudonimiseerde gegevens geen enkel nut zou hebben.

Daaruit vloeit voort dat om de pleger van de inbreuk te vinden, de bewegingsruimte van de officieren van gerechtelijke politie van het BIPT erg beperkt is.

Een tweede rechtvaardiging is dat paragraaf 1 van het nieuwe artikel 25/1 van de BIPT-statuutwet het aan de officieren van gerechtelijke politie van het BIPT enkel toestaat om een verzoek om identificatiegegevens te doen (verzoek om gegevens dat niet beschouwd wordt als een ernstige inmenging in de persoonlijke levenssfeer van de individuen) en dat overeenkomstig paragraaf 2 de toestemming van de onderzoeksrechter nodig is om metagegevens te verkrijgen (verzoek dat wel een ernstige inmenging in de persoonlijke levenssfeer van de individuen vormt).

Une troisième justification est qu'il ressort de la pratique que du fait de la charge de travail très élevée des procureurs du Roi, un temps considérablement long peut être nécessaire avant qu'un officier de police judiciaire de l'IBPT n'obtienne un réquisitoire du procureur du Roi. Or, il est important que les autorités répressives agissent rapidement en cas de fraudes, qui par ailleurs connaissent une forte augmentation ces dernières années (par exemple le smishing). Les mesures et efforts pour combattre les fraudes ne doivent pas uniquement venir des opérateurs (voir le nouvel article 121/8 de la loi télécom et les modifications aux articles 122 et 123 de cette même loi dans le cadre du 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) mais également des autorités.

Concernant la justification de pouvoir requérir des données du secteur bancaire, des centres fermés ou lieux d'hébergements ou d'autres personnes morales, il est renvoyé à l'amendement nr. 6 qui remplace l'article 127 de la loi télécom (voir en particulier le paragraphe 9 de cet article) .

Lorsque l'opérateur a mis en œuvre la méthode d'identification de l'abonné par conservation de la référence de paiement en cas de paiement en ligne (voir article 127 de la loi télécom), l'OPJ de l'IBPT obtiendra d'abord cette référence de paiement de l'opérateur (par exemple 11 chiffres relatifs à la recharge d'une carte prépayée et la date et l'heure de paiement). À l'heure actuelle, il conviendra alors de demander à un organisme de paiement de fournir à l'OPJ le numéro de la carte bancaire qui a été utilisée pour effectuer le paiement. Une aide de l'ASBL Febelfin est parfois nécessaire car le numéro de carte bancaire ne permet pas toujours de déduire directement la banque concernée (certains chiffres de la carte bancaire peuvent être cachés). Après avoir été requise, la banque donnera à l'OPJ alors les informations suivantes:

— Le nom, le prénom, l'adresse et la date de naissance du titulaire du compte;

— Le numéro du compte bancaire du titulaire;

— Les coordonnées des co-titulaires, mandataires si existants.

Il convient de rappeler que les démarches auprès des fournisseurs de services de paiement et de Febelfin visent à déterminer l'identité civile de l'abonné qui est une personne

Een derde rechtvaardiging is dat uit de praktijk blijkt dat wegens de erg hoge werklast van de procureurs des Konings aanzienlijk veel tijd nodig kan zijn voordat een officier van gerechtelijke politie van het BIPT vanwege de procureur des Konings een vordering ontvangt. Welnu, het is belangrijk dat de rechtshandhavingsautoriteiten snel optreden in fraudegevallen, die de jongste jaren trouwens sterk toenemen (bijvoorbeeld smishing). De maatregelen en inspanningen om de fraude te bestrijden, moeten niet enkel komen van de operatoren (zie het nieuwe artikel 121/8 van de telecomwet en de wijzigingen in de artikelen 122 en 123 van diezelfde wet in het kader van het 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), maar ook van de autoriteiten.

Voor de rechtvaardiging om gegevens te mogen vorderen van de banksector, de gesloten centra of woonunits of van andere rechtspersonen, wordt verwezen naar amendement nr. 6, dat artikel 127 van de telecomwet vervangt (in het bijzonder paragraaf 9 van dat artikel).

Wanneer de operator de methode van identificatie van de abonnee via bewaring van de referentie van de betalingstransactie in geval van onlinebetaling heeft toegepast (zie artikel 127 van de telecomwet), zal de OGP van het BIPT eerst die referentie van de betaling krijgen van de operator (bijvoorbeeld 11 cijfers voor het herladen van de voorafbetaalde kaart en de datum en het tijdstip van de betaling). Momenteel past het dan om aan een betalingsorganisme te vragen om aan de OGP het nummer te verstrekken van de bankkaart die gebruikt werd om de betaling te verrichten. Soms is de hulp van de VZW Febelfin nodig omdat het niet altijd mogelijk is om aan de hand van het bankkaartnummer de bank in kwestie rechtstreeks daarvan af te leiden (sommige cijfers van de bankkaart kunnen verborgen zijn). Na daartoe te zijn gevorderd zal de bank aan de OGP dan de volgende inlichtingen verstrekken:

— de naam, de voornaam, het adres en de geboortedatum van de rekeninghouder;

— het bankrekeningnummer van de titularis;

— de contactgegevens van de medetitularissen, volmachthouders, indien ze bestaan.

Er dient aan te worden herinnerd dat de stappen bij de aanbieders van betalingsdiensten en bij Febelfin erop gericht zijn de burgerlijke identiteit te bepalen van de abonnee die

physique ou l'identité de l'abonné qui est une personne morale.

Ces démarches sont limitées à une transaction bancaire spécifique, à savoir celle qui a permis d'acheter (ou de recharger) une carte prépayée ou l'abonnement.

À l'aide de ces démarches, les OPJ recueillent des données d'identification, mais pas des métadonnées.

Paragraphe 2: la demande de métadonnées

Lorsque, pour les besoins de l'accomplissement de sa mission, un OPJ de l'IBPT adresse une demande de métadonnées, il soumet sa demande motivée au préalable à l'autorisation du juge d'instruction, sauf cas d'urgence dûment justifié.

Au point 111 de son avis, l'Autorité de protection des données "constate qu'il n'y pas de précision concernant les métadonnées de communications électroniques auxquelles l'officier de police judiciaire de l'IBPT peut accéder. La disposition en projet est formulée de manière très large et permet a priori de demander un accès à toutes les données conservées par les opérateurs, y compris les données conservées en exécution du nouvel article 126/1 de la loi télécom."

Dans son avis, le Conseil d'État indique qu'"Il appartient à l'auteur de l'amendement d'être en mesure d'établir les éléments qui permettent de justifier la nécessité et le caractère proportionné de la possibilité d'accéder à l'ensemble de ces données (ou une partie d'entre elles), et ce mission par mission dans le respect de la jurisprudence de la Cour de justice.

La justification de l'amendement sera utilement complétée à cet égard.

La même observation vaut mutatis mutandis en ce qui concerne l'amendement n° 15 qui entend autoriser, à l'article 25/1 en projet de la loi du 17 janvier 2003, les officiers de police judiciaire de l'IBPT à accéder aux mêmes données afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 ou à l'article 24, § 1er, 2°, de la loi du 17 janvier 2003."

een natuurlijke persoon is of de identiteit van de abonnee die een rechtspersoon is.

Deze stappen zijn beperkt tot een specifieke banktransactie, namelijk die waardoor het abonnement of een prepaid kaart kon worden aangekocht (of herladen in het tweede geval).

Dankzij deze stappen verzamelen de OGP's identificatiegegevens, maar geen metagegevens.

Paragraaf 2: het verzoek om metagegevens

Wanneer een OGP van het BIPT, ten behoeve van de vervulling van zijn opdracht, een verzoek om metagegevens doet, legt hij zijn gemotiveerde verzoek op voorhand voor machtiging voor aan de onderzoeksrechter, behalve in een geval van naar behoren gerechtvaardigde hoogdringenheid.

In punt 111 van haar advies merkt de Gegevensbeschermingsautoriteit op "dat niet wordt gespecificeerd tot welke metagegevens van de elektronische communicatie de officier van gerechtelijke politie van het BIPT toegang kan hebben. De ontwerpbepaling is zeer ruim geformuleerd en maakt het mogelijk a priori toegang te vragen tot alle door operatoren opgeslagen gegevens, met inbegrip van gegevens die zijn opgeslagen op grond van het nieuwe artikel 126/1 van de telecomwet."

In zijn advies stelt de Raad van State: "Het staat aan de steller van het amendement om de elementen te kunnen vaststellen die de noodzaak en de evenredigheid kunnen rechtvaardigen van de mogelijkheid om toegang te krijgen tot al die gegevens (of een deel ervan), en dat opdracht per opdracht met inachtneming van de rechtspraak van het Hof van Justitie.

Het verdient aanbeveling de verantwoording van het amendement in dat opzicht aan te vullen.

Dezelfde opmerking geldt mutatis mutandis voor wat betreft amendement 15, dat ertoe strekt om in het ontworpen artikel 25/1 van de wet van 17 januari 2003 de officiers van gerechtelijke politie van het BIPT toegang te verlenen tot dezelfde gegevens met het oog op het onderzoek, de vaststelling of de vervolging van een inbreuk zoals bedoeld in artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 of in artikel 24, § 1, 2° van de wet van 17 januari 2003."

Il convient de relever que la définition de demande de métadonnées exclut les données conservées en vertu de l'article 126/1 de la loi télécom. L'opérateur devra donc répondre aux OPJ de l'IBPT sur base des métadonnées conservées en vertu des articles 122, 123 et 126 de la loi télécom. Par ailleurs, il n'est pas possible de déterminer dans le projet d'amendement toutes les métadonnées dont auraient besoin les OPJ de l'IBPT pour exercer leurs missions dans le futur.

Afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°, il est nécessaire que les OPJ de l'IBPT puissent se voir communiquer par l'opérateur concerné certaines métadonnées. Tel est le cas, par exemple, des données de localisation des équipements terminaux à partir desquels sont envoyés les messages de *phishing*, *smishing* ou autres types de messages frauduleux. Une telle donnée permet fréquemment de remonter la chaîne de transmission des messages frauduleux et ainsi identifier la ou les personnes à l'origine de celles-ci. S'agissant de la poursuite d'une finalité pénale, il va de soi que l'utilisation de données anonymes ou pseudonymes n'aurait aucun sens.

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.

Paragraphe 3: le contrôle des obligations à charge de l'opérateur

Pour pouvoir faire un contrôle efficace de l'obligation d'un opérateur de conserver les données et copies de document d'identification prévues aux articles 126, 126/1, 126/2 et 127, de la loi télécom 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.

Etant 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

Er dient te worden op gewezen dat de definitie van een verzoek om metagegevens de gegevens bewaard op basis artikel 126/1 van de telecomwet uitsluit. De operator zal dus de OGP's van het BIPT moeten antwoorden op basis van metagegevens bewaard krachtens de artikelen 122, 123 en 126 van de telecomwet. Verder is het niet mogelijk om in het ontwerpamendement alle metagegevens te bepalen die de OGP's van het BIPT nodig zouden hebben om hun opdrachten in de toekomst uit te voeren.

Teneinde een inbreuk bedoeld in artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te onderzoeken, vast te stellen of te vervolgen, is het noodzakelijk dat de OGP's van het BIPT van de betrokken operator bepaalde metagegevens kunnen krijgen. Dat is bijvoorbeeld het geval voor locatiegegevens van de eindapparatuur waarmee de *phishing*- of *smishing*berichten of andere soorten van frauduleuze berichten werden verstuurd. Aan de hand van een dergelijk gegeven kan vaak de verzendingsketen van frauduleuze berichten worden getraceerd en aldus de persoon (personen) aan de basis ervan worden geïdentificeerd. Wat betreft de vervolging van een strafrechtelijk doeleinde, spreekt het voor zich dat het gebruik van geanonimiseerde of gepseudonimiseerde gegevens geen enkel nut zou hebben.

In de gevallen van naar behoren gerechtvaardigde hoogdringendheid waarin de voorafgaande controle door de onderzoeksrechter niet mogelijk was, voert de onderzoeksrechter daarna een controle uit.

Paragraaf 3: de controle van de verplichtingen die op de operator rusten

Om de verplichting van een operator om de in de artikelen 126, 126/1, 126/2 en 127 van de telecomwet bepaalde identificatiegegevens en de kopieën van identificatiedocumenten te bewaren, 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 officieren 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 officieren 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

officiers de police judiciaire doit dorénavant être précédée d'une autorisation par un OPJ de l'IBPT désigné par le Roi pour effectuer ce contrôle.

Même si à l'occasion de leur contrôle, les officiers de police judiciaire de l'IBPT sont amenés à prendre 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.

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 par l'opérateur. Afin de limiter le traitement de données à caractère personnel, ils ne peuvent pas garder de copie dans d'autres cas.

Paragraphe 4: le délai pour répondre à la demande et les sanctions applicables

Concernant la justification de ce nouveau paragraphe, il est renvoyé à l'amendement n° 14 qui complète l'article 46*bis* du Code d'instruction criminelle.

Paragraphe 5: la motivation des demandes

Le paragraphe 5 a pour objectif d'incorporer dans la loi-statut les exigences posées par la Cour constitutionnelle dans son arrêt n° 158/2021 du 18 novembre 2021, point B.16.8.7. (cf. supra).

Les OPJ de l'IBPT doivent toujours disposer, à cet effet, d'indices concrets que l'identification de l'abonné est nécessaire dans le cadre de leurs missions.

Ces exigences ne sont pas applicables dans le cadre de la consultation par un OPJ de l'IBPT d'une base de données de l'opérateur afin de contrôler que ce dernier respecte bien la législation télécom. En effet, dans ce cadre, il n'y a pas de demande de données qui seraient communiquées de l'opérateur à l'OPJ dans le cadre d'une enquête pénale mais plutôt une consultation de cet OPJ de la base de données, afin de contrôler l'opérateur sur base d'échantillons représentatifs. Cependant, l'exigence de la Cour constitutionnelle concernant la motivation in concreto est reprise pour le contrôle de l'opérateur, étant donné qu'il s'agit d'un principe général.

deze officieren van gerechtelijke politie voortaan worden voorafgegaan door een toestemming vanwege een OGP van het BIPT, die door de Koning aangewezen is om die controle te verrichten.

Hoewel de officieren van gerechtelijke politie van het BIPT ter gelegenheid van hun controle ertoe gebracht 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.

Het is van fundamenteel belang dat de officieren 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 door de operator. Om de verwerking van persoonsgegevens te beperken, mogen ze in andere gevallen geen kopie bewaren.

Paragraaf 4: de termijn om op het verzoek te antwoorden en de toepasselijke sancties

Voor de verantwoording van deze nieuwe paragraaf wordt verwezen naar amendement nr. 14, dat artikel 46*bis* van het Wetboek van Strafvordering aanvult.

Paragraaf 5: de motivering van de verzoeken

Paragraaf 5 heeft tot doel in de statuutwet de eisen op te nemen die zijn gesteld door het Grondwettelijk Hof in zijn arrest nr. 158/2021 van 18 november 2021, punt B.16.8.7. (zie hierboven).

De OGP's van het BIPT moeten daartoe steeds over concrete aanwijzingen beschikken dat de identificatie van de abonnee noodzakelijk is in het kader van hun opdrachten.

Die eisen gelden niet wanneer een OGP van het BIPT een databank van de operator raadpleegt om te controleren of deze laatste wel degelijk de telecomwetgeving naleeft. In dat kader is er immers geen verzoek om gegevens die door de operator aan de OGP zouden worden meegedeeld als deel van een strafonderzoek, maar wel een raadpleging door die OGP van de databank, met als doel de operator te controleren op basis van representatieve steekproeven. De eis van het Grondwettelijk Hof in verband met de motivering in concreto is evenwel overgenomen voor de controle van de operator, aangezien het om een algemeen principe gaat.

Paragraphe 6: le registre

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, aux fournisseurs de services de paiement, à Felbefin, aux centres fermés ou lieux d'hébergement ou aux personnes morales, ces OPJ 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.

Dans le cadre des paragraphes 1 et 2, la motivation de la demande est communiquée à l'OPJ de l'IBPT qui est chargé du contrôle des demandes ou au juge d'instruction mais pas à l'opérateur. Cela s'explique par le fait que la motivation de la demande doit être faite in concreto et peut comprendre des éléments délicats dont n'a pas à connaître l'opérateur. Cela permet donc de protéger le secret de l'enquête.

Le registre comprend les demandes internes et externes. Les demandes internes sont les demandes envers l'OPJ de l'IBPT qui est chargé de contrôler les demandes ou le juge d'instruction (demande avec la motivation). Les demandes externes sont les demandes adressées aux opérateurs et aux autres acteurs concernés.

Information de la personne concernée

La loi-statut ne prévoit pas une information de la personne concernée dans le cadre des paragraphes 1, 2 et 3 de l'article 25/1 et ce pour les raisons suivantes. Dans le cadre des paragraphes 1 et 2, les OPJ de l'IBPT préparent le dossier pour le parquet et informer la personne concernée pourrait nuire à l'enquête que le parquet peut démarrer sur base des informations que les OPJ de l'IBPT lui fournissent. L'information de la personne concernée se fera donc conformément aux règles du Code d'instruction criminelle.

L'information de la personne concernée dans le cadre du paragraphe 3 de l'article 25/1 serait très lourd à mettre en place, dès lors qu'un contrôle d'une base de données peut aboutir à un contrôle de (plusieurs) milliers d'enregistrements dans cette base de données. Vu que le contrôle porte sur l'opérateur et non pas sur les personnes dont les données se trouvent dans la base de données, informer ces personnes

Paragraaf 6: de inventaris

Om een interne controle en een controle door de procureur-generaal mogelijk te maken van de verzoeken die de officieren van gerechtelijke politie van het BIPT richten aan de operatoren, aan de aanbieders van betalingsdiensten, aan Febelfin, aan de gesloten centra, aan de woonunits of aan de rechtspersonen, houden deze OGP's 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 officieren van gerechtelijke politie van het Instituut onder het toezicht van de procureur-generaal staan.

In het kader van de paragrafen 1 en 2 wordt de motivering van het verzoek meegedeeld aan de OGP van het BIPT die belast is met de controle van de verzoeken ofwel aan de onderzoeksrechter, maar niet aan de operator. De verklaring daarvoor is dat de motivering van het verzoek in concreto moet gebeuren en gevoelige elementen kan bevatten waarvan de operator geen weet moet hebben. Daardoor kan het geheim van het onderzoek beschermd worden.

De inventaris bevat de interne en externe verzoeken. Interne verzoeken zijn verzoeken aan de OGP van het BIPT die belast is met de controle van de verzoeken ofwel aan de onderzoeksrechter (verzoek samen met de motivering). Externe verzoeken zijn verzoeken die gericht zijn aan de operatoren en aan de andere betrokken actoren.

Inlichten van de betrokken persoon

De statuutwet schrijft niet voor dat de betrokken persoon ingelicht moet worden in het kader van de paragrafen 1, 2 en 3 van artikel 25/1 en dat om de volgende redenen. In het kader van de paragrafen 1 en 2 bereiden de OGP's van het BIPT het dossier voor het parket voor en de betrokken persoon inlichten zou het onderzoek kunnen schaden dat het parket kan starten op basis van de informatie die de OGP's van het BIPT eraan verstrekken. De betrokken persoon zal dus worden ingelicht overeenkomstig de regels van het Wetboek van Strafvordering.

Het inlichten van de betrokken persoon in het kader van paragraaf 3 van artikel 25/1 zou heel zwaar zijn om in te voeren, omdat een controle van een databank kan uitmonden in een controle van (ettelijke) duizenden registraties in deze databank. Doordat de controle betrekking heeft op de operator en niet op de personen van wie de gegevens zich in de databank bevinden, zou die betrokken personen inlichten het

concernées risqueraient de créer de la confusion auprès de ces dernières et n'auraient pas de plus-value pour ces dernières.

En outre, comme indiqué précédemment quant à l'article 15, le RGPD permet de déroger au droit de la personne concernée d'être informée de chaque traitement de ses données à caractère personnel lorsque les moyens qui devraient être déployés par le responsable du traitement pour informer la personne concernée du traitement seraient disproportionnés.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

risico inhouden dat die laatsten in verwarring worden gebracht en dat zou voor hen geen meerwaarde hebben.

Bovendien, zoals eerder al aangegeven in verband met artikel 15, staat de AVG het toe om af te wijken van het recht van de betrokken persoon om te worden ingelicht over elke verwerking van zijn persoonsgegevens wanneer de middelen die de verwerkingsverantwoordelijke zou moeten inzetten om de betrokken persoon in te lichten over de verwerking, onevenredig zouden zijn.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 14 **DU GOUVERNEMENT**

Art. 20/1 *(nouveau)*

Insérer un article 20/1, libellé comme suit:

"Art. 20/1. Dans l'article 46bis du même Code, modifié en dernier lieu par la loi du 25 décembre 2016, les modifications suivantes sont apportées:

1° dans le paragraphe 1er un alinéa rédigé comme suit est inséré entre les alinéas 2 et 3:

"Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, il peut également requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:

— des personnes et institutions visées à l'article 46quater, § 1er, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, en application du paragraphe 1er.

— des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectué, et qui ont préalablement été communiquées par un des acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, en application du paragraphe 1er;

— des autres personnes morales qui sont l'abonné d'un des acteurs visés au paragraphe 2, premier ou deuxième tiret, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, en application du paragraphe 1er."

Nr. 14 **VAN DE REGERING**

Art. 20/1 *(nieuw)*

Een artikel 20/1 invoegen, luidende:

"Art. 20/1. In artikel 46bis van hetzelfde Wetboek, laatst gewijzigd door de wet van 25 december 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt tussen het tweede en het derde lid een lid ingevoegd, luidende:

"Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid, tweede streepje, kan hij ook, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— de personen of instellingen bedoeld in artikel 46quater, § 1, op basis van de referentie van een elektronische banktransactie die voorafgaand meegedeeld is door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, in toepassing van het eerste lid;

— de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden, die voorafgaand meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, in toepassing van het eerste lid;

— andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, eerste of tweede streepje, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaand meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, in toepassing van het eerste lid."

2° dans le paragraphe 2, les alinéas 3 et 4 sont abrogés;

3° l'article est complété par les paragraphes 3 et 4, rédigés comme suit:

§ 3. Les acteurs visés au § 1er, alinéa 3, 1er à 3e tirets, requis de communiquer l'identification de l'abonné ou de l'utilisateur habituel d'un service visé au paragraphe 1er, l'alinéa 2, deuxième tiret, communiquent au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition.

§ 4. 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 communiquer les données ou qui ne les communique 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."."

JUSTIFICATION

Il convient tout d'abord de se référer à la justification de l'amendement n° 6, amendement qui remplace l'article 127 de la loi relative aux communications électroniques à la suite de l'arrêt de la Cour constitutionnelle n° 158/2021 du 18 novembre 2021. La Cour a annulé l'article 2 de la loi du 1er septembre 2016 "portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité", uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération.

En résumé, la Cour étais d'avis que les données d'identification et les documents d'identification qui doivent être conservés par les opérateurs en vertu de l'article 127 doivent être énumérés dans la loi elle-même, et que cette énumération

2° in paragraaf 2 worden het derde en het vierde lid opgeheven;

3° het artikel wordt aangevuld met de paragrafen 3 en 4, luidende:

"§ 3. De actoren bedoeld in § 1, derde lid, eerste tot derde streepje, van wie de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in § 1, tweede lid, tweede streepje gevorderd wordt, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

§ 4. 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 de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro."."

VERANTWOORDING

Er kan eerst en vooral verwezen worden naar de toelichting bij amendement nr. 6, amendement dat artikel 127 van de wet betreffende de elektronische communicatie vervangt als gevolg van arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof. Het Hof heeft artikel 2 van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst vernietigd, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen.

Samengevat komt het erop neer dat het Hof van oordeel was dat de identificatiegegevens en de identificatiedocumenten die door operatoren op grond van artikel 127 bewaard moeten worden, opgesomd moeten worden in de wet zelf, en

ne peut être laissée au pouvoir exécutif par le biais d'une délégation au Roi.

Le gouvernement a donc décidé de donner suite à cet arrêt en énumérant les données d'identification et les documents d'identification à l'article 127 de la loi.

L'article 127 de la loi contient des méthodes d'identification directes et indirectes.

Par "méthode d'identification directe", on entend la méthode par laquelle l'opérateur collecte et conserve des données fiables relatives à l'identité civile d'une personne physique qui est son abonné ou qui agit pour le compte de son abonné qui est une personne morale afin de remplir les obligations d'identification de la personne morale et, le cas échéant, une copie du document d'identité de cette personne physique.

En revanche, la "méthode indirecte d'identification" désigne la méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés.

Le nouvel article 127 comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés (méthode d'identification directe) ou à tout le moins de rendre cette identification possible (méthode d'identification indirecte).

L'article 46*bis* du Code d'instruction criminelle est la base légale qui permet aux autorités judiciaires de procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique, ou bien du moyen de communication électronique utilisé, ou à l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

L'article 46*bis*, en combinaison ou non avec d'autres bases légales, peut envisager à la fois la méthode d'identification directe et indirecte.

L'article peut être considéré comme une méthode d'identification directe lorsque le procureur du Roi requiert la collaboration des opérateurs ou des fournisseurs de services de communication électronique à cette fin, et obtient ensuite l'identification directement de ces opérateurs ou fournisseurs de services.

dat die opsomming niet via een delegatie aan de Koning aan de uitvoerende macht kunnen worden overgelaten.

Daarom heeft de regering beslist om gevolg te geven aan dit arrest door de identificatiegegevens en de identificatiedocumenten op te sommen in artikel 127 van de wet.

Artikel 127 van de wet bevat directe en indirecte identificatiemethodes.

Onder "directe identificatiemethode" dient te worden verstaan de methode waarbij de operator betrouwbare gegevens verzamelt en bewaart met betrekking tot de burgerlijke identiteit van een natuurlijke persoon die zijn abonnee is of die optreedt voor rekening van zijn abonnee die een rechtspersoon is om de verplichtingen inzake identificatie van de rechtspersoon te vervullen en, in voorkomend geval, een kopie van het identiteitsstuk van deze natuurlijke persoon.

De "indirecte identificatiemethode" daarentegen, doelt op de methode waarbij de operator gegevens verzamelt en bewaart aan de hand waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen.

Het nieuwe artikel 127 bevat nu een positieve verplichting voor de operatoren om hun abonnees te identificeren (directe identificatiemethode) of op zijn minst deze identificatie mogelijk te maken (indirecte identificatiemethode).

Artikel 46*bis* van het Wetboek van strafvordering is de wettelijke basis die de gerechtelijke autoriteiten de mogelijkheid geeft om over te gaan tot de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel, of tot de identificatie van de elektronische communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

Artikel 46*bis*, al dan niet in combinatie met andere wettelijke basissen, kan zowel de directe als de indirecte identificatiemethode beogen.

Het artikel kan beschouwd worden als directe identificatiemethode wanneer de procureur des Konings daarvoor de medewerking vordert van operatoren of verstrekkers van elektronische communicatiediensten, en daarop volgend de identificatie rechtstreeks van deze operator of dienstenverstrekkers verkrijgt.

Toutefois, il est également possible que le procureur du Roi reçoive d'autres informations d'un opérateur, avec lesquelles il doit ensuite faire appel à d'autres personnes ou institutions pour obtenir une identification. L'article 46*bis* vise également à fournir ce moyen d'identification: l'article stipule que le procureur du Roi peut procéder à l'identification visée au § 1er, premier alinéa, "sur la base de toutes données détenues par lui". Il peut s'agir, par exemple, d'une opération de paiement, sur la base de laquelle le procureur du Roi peut s'adresser à une institution financière pour obtenir l'identification de l'abonné visé. Il s'agit alors de la méthode indirecte d'identification.

L'APD a constaté dans la note de bas de page n° 50 de l'avis n° 66/2022 du 1er avril 2022, que la lecture de l'article 46*bis* du Code d'instruction criminelle ne laisse pas clairement entrevoir le pouvoir du Procureur du Roi d'exiger des institutions financières de révéler l'identité de la personne "derrière" la référence d'une transaction bancaire électronique. Il a déjà été indiqué ci-dessus que l'article 46*bis* permet au procureur du Roi de procéder à l'identification "sur la base de toutes données détenues par lui". En pratique, cela se fait souvent par une réquisition combinée fondée sur les articles 46*bis* et 46*quater* du Code d'instruction criminelle. En outre, l'article XII.20 du Code de droit économique fournit déjà aux autorités judiciaires une base pour demander aux prestataires de services toutes les informations dont ils disposent et utiles à la recherche et à la constatation des infractions commises par leur intermédiaire. Enfin, sur la base de l'article 28*ter* du Code d'instruction criminelle, le procureur du Roi dispose d'un droit général d'information.

Ainsi, le Code d'instruction criminelle fournit déjà une base légale pour procéder à l'identification indirecte visée à l'article 127 de la loi relative aux communications électroniques.

Le gouvernement est d'avis que cette possibilité doit être précisée dans les lois organiques des autorités qui souhaitent faire usage de ces méthodes d'identification indirecte. L'article 46*bis* du Code d'instruction criminelle sera donc également modifié et précisé dans ce sens.

Les modifications prévues à l'article 46*bis* par le présent amendement sont parfaitement conformes à ce qui est prévu à l'article 127, § 9, de la loi relative aux communications électroniques.

La méthode d'identification indirecte sur base de la référence d'une opération de paiement était déjà prévue à

Het is echter ook mogelijk dat de procureur des Konings van een operator andere informatie krijgt waarmee hij vervolgens een beroep moet doen op andere personen of instellingen om de identificatie te verkrijgen. Ook deze manier om tot identificatie over te gaan wordt beoogd door artikel 46*bis*: het artikel bepaalt immers dat de procureur des Konings kan overgaan tot de identificatie bedoeld in § 1, eerste lid "op basis van ieder gegeven in zijn bezit". Het zou hier bijvoorbeeld kunnen gaan om een betalingsverrichting, op basis waarvan de procureur des Konings zich tot een financiële instelling kan wenden om de identificatie van de beoogde abonnee te verkrijgen. Dit is dan de indirecte identificatiemethode.

De GBA heeft in voetnoot nr. 50 van advies nr. 66/2022 van 1 april 2022 vastgesteld, dat uit de lezing van artikel 46*bis* van het Wetboek van strafvordering niet duidelijk blijkt dat de procureur des Konings bevoegd is om financiële instellingen te verplichten de identiteit bekend te maken van de persoon "achter" de referentie van een elektronische bankverrichting. Hierboven werd al aangegeven dat artikel 46*bis* de procureur des Konings toelaat over te gaan tot identificatie "op basis van ieder gegeven in zijn bezit". In de praktijk wordt hier vaak gewerkt met een gecombineerde vordering op basis van de artikelen 46*bis* en 46*quater* van het Wetboek van strafvordering. Ook artikel XII.20 van het Wetboek Economisch recht biedt de gerechtelijke autoriteiten al een basis om bij dienstverleners alle informatie te kunnen opvragen waarover zij beschikken en die nuttig is voor de opsporing en de vaststelling van de inbreuken gepleegd door hun tussenkomst. Tot slot beschikt de procureur des Konings op basis van artikel 28*ter* van het Wetboek van strafvordering over een algemeen opsporingsrecht.

Het Wetboek van strafvordering biedt dus nu al een wettelijke basis om tot een indirecte identificatie zoals bedoeld in artikel 127 van de wet betreffende de elektronische communicatie over te gaan.

De Regering is van mening dat deze mogelijkheid verduidelijkt dient te worden in de organieke wetten van alle autoriteiten die een beroep wensen te doen op deze indirecte identificatiemethodes. Ook artikel 46*bis* van het Wetboek van strafvordering wordt dientengevolge aangepast en verduidelijkt in die zin.

De aanpassingen die door huidig amendement voorzien worden in artikel 46*bis*, liggen volledig in de lijn van wat in artikel 127, § 9, van de wet betreffende de elektronische communicatie wordt voorzien.

De indirecte identificatiemethode via het kenmerk van een betalingsverrichting was al voorzien in artikel 17 van

l'article 17 de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée, et est désormais reprise à l'article 127, § 9, premier alinéa, 3°. Le point 5° du même paragraphe prévoit que, sur la base des informations reçues de l'opérateur, les autorités judiciaires peuvent s'adresser au centre fermé ou au lieu d'hébergement, pour obtenir plus d'information sur l'identité de l'abonné. Ces deux options sont désormais également prévues à l'article 46*bis*, ainsi qu'une catégorie résiduelle.

L'amendement insère donc un nouvel alinéa entre les deuxième et troisième alinéas de l'article 46*bis*, § 1er, afin de permettre au procureur du Roi de requérir la collaboration de certaines personnes et/ou institutions, en vue de l'identification (indirecte) de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques.

La première catégorie (article 46*bis*, § 1er, troisième alinéa, premier tiret) concerne les banques et les établissements financiers. Pour déterminer le champ d'application, il est fait référence aux personnes et institutions visées à l'article 46*quater*, § 1er. Plus précisément, dans l'article 46*quater*, § 1er, il s'agit:

1° des personnes et institutions visées à l'article 5, § 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de payement réglementés en valeurs virtuelles.

La loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social a élargi le champ d'application de l'article 46*quater*. Le champ d'application matériel, qui était limité jusqu'alors aux prestataires qui offrent des services qui se retrouvent dans l'énumération limitative des "comptes bancaires, coffres bancaires ou instruments financiers de la loi du 2 août 2017 et des opérations bancaires", a été remplacé et étendu à l'ensemble du secteur financier. L'article 5, § 1er de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces reprend l'énumération la plus claire et complète du secteur financier. Les différentes entités y sont décrites légalement, intégralement, clairement et de

het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een vooraf betaalde kaart, en wordt nu opgenomen in artikel 127, § 9, eerste lid, 3°. In punt 5° van datzelfde lid wordt bepaald dat gerechtelijke autoriteiten op basis van de informatie die ontvangen is van de operator zich kunnen wenden tot een gesloten centrum of een woonunit om meer informatie te krijgen over de identiteit van de abonnee. Beide opties worden nu ook voorzien in artikel 46*bis*, samen met een restcategorie.

Het amendement voegt dus een nieuw lid in tussen het tweede en derde lid van artikel 46*bis*, § 1, teneinde het mogelijk te maken voor de procureur des Konings om de medewerking te vorderen van bepaalde personen en/of instellingen, met het oog op de (indirecte) identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst.

De eerste categorie (artikel 46*bis*, § 1, derde lid, eerste streepje) betreft de banken en de financiële instellingen. Om het toepassingsgebied te bepalen wordt verwezen de personen en instellingen bedoeld in artikel 46*quater*, § 1. Het gaat in artikel 46*quater*, § 1 meer bepaald om:

1° de personen en instellingen als bedoeld in artikel 5, § 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, en

2° personen en instellingen die binnen het Belgisch grondgebied diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld.

De wet van 5 mei 2019 houdende diverse bepalingen in strafzaken en inzake erediensten, en tot wijziging van de wet van 28 mei 2002 betreffende de euthanasie en van het Sociaal Strafwetboek heeft het toepassingsgebied van artikel 46*quater* verruimd. Het materiële toepassingsgebied, tot dan beperkt tot de aanbieders die diensten aanbieden die voorkomen in de limitatieve opsomming van "bankrekeningen, bankkluizen en de financiële instrumenten wet van 2 augustus 2002 en bankverrichtingen" werd vervangen en uitgebreid tot de volledige financiële sector. Artikel 5, § 1 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten biedt de meest duidelijke en volledige oplijsting van de financiële sector. De verschillende entiteiten worden er op een wettelijke, volledige,

manière connue. Ceci favorise dès lors la sécurité juridique (ce qui est important étant donné les sanctions pénales introduites en cas de non-collaboration desdites institutions).

Il y a lieu d'entendre par "des personnes et institutions qui mettent à disposition ou proposent des services en lien avec des valeurs virtuelles" des plateformes, des échangeurs (traders), des prestataires de services de paiement qui proposent des cartes de débit et de crédit reliées à des monnaies virtuelles, etc. Il peut être renvoyé à l'exposé des motifs de la loi du 5 mai 2019 (Doc. Parl., Chambre, DOC 54 3515/001, p. 14 et suivants).

Il est explicitement prévu dans l'amendement que le procureur du Roi ne peut faire appel à ces personnes et institutions que lorsqu'il dispose de la référence d'une transaction bancaire électronique préalablement communiquée par un opérateur ou un fournisseur d'un service de communications électroniques en application de l'article 46*bis*, § 1er.

La deuxième catégorie (article 46*bis*, § 1er, troisième alinéa, deuxième tiret) concerne les des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers. Il s'agit ici des cas de souscription d'un abonné qui réside dans un tel centre fermé ou un lieu d'hébergement à un service de communications électroniques mobiles fourni au moyen d'une carte prépayée. Là encore, l'amendement prévoit que le procureur du Roi ne peut faire appel à ces institutions que s'il dispose des coordonnées du centre fermé ou du lieu d'hébergement où la souscription à un service de communications électroniques mobiles a eu lieu et qui ont été communiquées préalablement par un opérateur ou un fournisseur d'un service de communications électroniques en application de l'article 46*bis*, § 1er.

La troisième catégorie (article 46*bis*, § 1er, troisième alinéa, troisième tiret) est une catégorie résiduelle: elle concerne les autres personnes morales qui sont l'abonné d'un des acteurs visés à l'article 46*bis*, paragraphe 2, premier ou deuxième tiret, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques. Là encore, le procureur ne peut requérir la collaboration de ces personnes morales que sur la base des données qui sont communiquées préalablement par un opérateur ou un fournisseur d'un service de communications électroniques en application de l'article 46*bis*, § 1er.

duidelijke en gekende wijze omschreven. Dit bevordert aldus de rechtszekerheid (wat belangrijk is, gelet op de strafsancties die ingevoerd worden voor niet-medewerking van de bedoelde instellingen).

Met "personen en instellingen die diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden" wordt onder meer gedoeld op platformen, exchangers (handelaars), betalingsdienstenaanbieders die debet- en creditkaarten gekoppeld aan virtuele munten aanbieden. Er kan verwezen worden naar de memorie van toelichting bij de wet van 5 mei 2019 (Parl. St., Kamer, DOC 54 3515/001, blz. 14 en volgende).

Er wordt expliciet voorzien in het amendement dat de procureur des Konings slechts een beroep kan doen op deze personen en instellingen wanneer hij beschikt over de referentie van een elektronische banktransactie die voorafgaand meegedeeld is door een operator of een verstrekker van een elektronische communicatiedienst in toepassing van artikel 46*bis*, § 1.

De tweede categorie (artikel 46*bis*, § 1, derde lid, tweede streepje) betreft de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen. Hier gaat het om gevallen van een intekening van een abonnee die in een dergelijk gesloten centrum of woonunit verblijft op een mobiele elektronische communicatiedienst verstrekt door middel van een voorafbetaalde kaart. Ook hier voorziet het amendement dat de procureur des Konings slechts een beroep kan doen op deze instellingen wanneer hij beschikt over de contactgegevens van het gesloten centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden en die voorafgaand meegedeeld zijn door een operator of een verstrekker van een elektronische communicatiedienst in toepassing van artikel 46*bis*, § 1.

De derde categorie (artikel 46*bis*, § 1, derde lid, derde streepje) is een restcategorie: het gaat om andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in artikel 46*bis*, tweede lid, eerste of tweede streepje, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst. Opnieuw, de procureur kan slechts de medewerking vorderen van deze rechtspersonen op basis van gegevens die voorafgaand meegedeeld zijn door een operator of een verstrekker van een elektronische communicatiedienst in toepassing van artikel 46*bis*, § 1.

Les points 2° et 3° de cet amendement concernent l'obligation de collaboration et l'obligation de secret des personnes et institutions visées. À cet égard, il convient de distinguer, d'une part, les opérateurs et les fournisseurs visés à l'article 46*bis*, § 1er, alinéa 2, premier et deuxième tirets, et, d'autre part, les autres institutions "tierces" visées au nouvel alinéa 3 de l'article 46*bis*, § 1er.

L'article 46*bis*, § 2, s'applique aux opérateurs: ils doivent communiquer au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition, et ce selon les modalités fixées par le Roi. Ces modalités sont fixées dans 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.

Cet arrêté royal ne s'applique qu'aux opérateurs visés à l'article 46*bis*, § 1er, deuxième alinéa. Il n'est nullement dans l'intention de cet amendement de rendre cet arrêté royal également applicable aux institutions "tierces" auxquelles le procureur peut faire appel sur la base du nouvel alinéa 3 de l'article 46*bis*, § 1er. C'est la raison pour laquelle un nouvel paragraphe 3 est introduit dans l'article 46*bis* pour ces institutions, dans lequel on attend d'elles qu'elles fournissent au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition. Ils ne sont pas soumis à d'autres obligations de collaboration que celle-ci.

Le Conseil d'État, dans son avis n° 71 184/4 du 25 avril 2022, a recommandé de remplacer les mots "en temps réel" à l'article 46*bis*, §§ 3 et 4 par les mots "sans délai", en raison du fait que "la notion de "temps réel" peut prêter à confusion dès lors qu'elle peut revêtir une signification particulière dans le cadre de traitements de données dans le domaine des communications électroniques".

Le gouvernement ne reprend pas cette suggestion, car la notion de "en temps réel" est un concept bien connu, défini dans l'arrêté royal du 9 janvier 2003 précité déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques. L'arrêté royal définit la notion de "temps réel" comme la "durée minimale nécessaire à l'exécution d'une prestation déterminée, selon les règles de l'art, sans interruption et en mettant en œuvre les moyens et le personnel adéquats".

De punten 2° en 3° in dit amendement betreffen de medewerkingsplicht en de geheimhoudingsplicht van de beoogde personen en instellingen. Wat dit betreft dient een onderscheid gemaakt te worden tussen enerzijds de operatoren en dienstenverstrekkers bedoeld in artikel 46*bis*, § 1, tweede lid, eerste en tweede streepje, en anderzijds de andere "derde" instellingen bedoeld in het nieuwe derde lid van artikel 46*bis*, § 1.

Artikel 46*bis*, § 2, is van toepassing op de operatoren: zij dienen de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering mee te delen, en dat volgens de nadere regels vastgesteld door de Koning. Die nadere regels zijn opgenomen in het koninklijk besluit van 9 januari 2003 Koninklijk besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie.

Dit koninklijk besluit is uitsluitend van toepassing op operatoren als bedoeld in artikel 46*bis*, § 1, tweede lid. Het is geenszins de bedoeling van dit amendement om dit KB ook van toepassing te maken op de "derde" instellingen waarop de procureur des Konings een beroep kan doen op basis van het nieuwe derde lid van artikel 46*bis*, § 1. Daarom wordt voor deze instellingen een nieuwe paragraaf 3 ingevoerd in artikel 46*bis* waarin van deze instellingen wordt verwacht dat zij de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, meedelen. Zij zijn aan geen verdere medewerkingsverplichtingen onderworpen dan deze.

De Raad van State heeft in advies nr. 71 184/4 van 25 april 2022 aanbevolen om de woorden "in werkelijke tijd" in artikel 46*bis*, §§ 3 en 4 te vervangen door het woord "onverwijld", omwille van het feit dat "het begrip "werkelijke tijd" verwarrend kan zijn, aangezien dit een bijzondere betekenis kan hebben in de context van gegevensverwerking op het gebied van elektronische communicatie."

De Regering gaat niet in op deze suggestie, aangezien het begrip "in werkelijke tijd" een gekend begrip is dat gedefinieerd is in het hierboven vermelde Koninklijk besluit van 9 januari 2003 Koninklijk besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie. Onder werkelijke tijd wordt in het Koninklijk besluit verstaan de "minimum tijdsduur nodig voor de uitvoering van een bepaalde prestatie volgens de regels van de kunst, zonder onderbreking en waarvoor aangepaste middelen en personeel werden ingezet".

La notion “en temps réel” est également utilisée dans les actuels articles 46*bis*, § 2 et 88*bis*, § 4 du Code d’instruction criminelle. Il ne serait pas logique d’utiliser aux §§ 3 et 4 de l’article 46*bis* une autre terminologie que celle déjà prévue au § 2 du même article et dans d’autres articles du Code. Cela soulèverait immédiatement la question de savoir si les opérateurs visés à l’article 46*bis*, § 2, sont traités différemment des institutions visées aux §§ 3 et 4. Bien qu’il n’y ait pas de différence identifiable entre les termes “en temps réel” et “sans délai”, il convient d’utiliser la même terminologie dans tout le Code.

Enfin, le paragraphe 2 de l’article 46*bis* actuel prévoit également des sanctions en cas de non-collaboration ou de communication tardive des données, et prévoit une obligation de secret pour les personnes qui, du chef de ses fonctions, ont connaissance de la mesure ou y prêtent leur concours. Il est logique de supprimer ces deux alinéas du paragraphe 2 et de les insérer dans un nouveau paragraphe 4: de cette manière, ces règles deviennent applicables tant aux opérateurs visés à l’article 46*bis*, § 1er, deuxième alinéa, qu’aux personnes tiers et institutions visées à l’article 46*bis*, § 1er, troisième alinéa nouveau. Les alinéas 3 et 4 du paragraphe 2 seront donc supprimés, mais immédiatement réintégrés dans le nouveau paragraphe 4.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

Het begrip “in werkelijke tijd” wordt ook gebruikt in de huidige artikelen 46*bis*, § 2 en 88*bis*, § 4 van het Wetboek van strafvordering. Het zou niet logisch zijn om in de §§ 3 en 4 van artikel 46*bis* een andere terminologie te gebruiken dan deze die al voorzien is in § 2 van hetzelfde artikel en in andere artikelen van het Wetboek. Het zou meteen de vraag doen rijzen of de operatoren bedoeld in artikel 46*bis*, § 2, een andere behandeling krijgen dan de instellingen bedoeld in de §§ 3 en 4. Hoewel er geen aanwijsbaar verschil is tussen de termen “in werkelijke tijd” en “onverwijld” is het aangewezen om overal in het Wetboek dezelfde terminologie te gebruiken.

Tot slot, paragraaf 2 van huidig artikel 46*bis* voorziet ook sancties voor niet-medewerking of niet tijdige aanlevering van de gegevens, en voorziet in een geheimhoudingsplicht voor personen die uit hoofde van hun bediening kennis krijgen van de maatregel of daaraan hun medewerking verlenen. Het is logisch om deze twee leden uit paragraaf 2 te halen en in te schrijven in een nieuwe paragraaf 4: op die manier worden deze regels toepasbaar op zowel de operatoren bedoeld in het tweede lid van artikel 46*bis*, § 1 als op de derde personen en instellingen bedoeld in het nieuwe derde lid van artikel 46*bis*, § 1. Het derde en vierde lid van paragraaf 2 worden dan ook opgeheven, maar direct opnieuw opgenomen in de nieuwe paragraaf 4.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 15 **DU GOUVERNEMENT**

Art. 32/1 *(nouveau)*

Dans le chapitre 8, insérer un article 32/1, rédigé comme suit:

"Art. 32/1. Dans l'article 81 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, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 3, les mots "visée à l'alinéa 1er" sont insérés entre les mots "dans sa décision" et les mots "les circonstances de fait";

2° le paragraphe 1er est complété par un alinéa, rédigé comme suit:

"Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, 2°, l'auditeur ou, en son absence, l'auditeur adjoint peut également requérir la collaboration:

— des personnes et institutions visées à l'article 5, § 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er;

— des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectuée, et qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er;

Nr. 15 **VAN DE REGERING**

Art. 32/1 *(nieuw)*

In hoofdstuk 8, een artikel 32/1 invoegen, luidende:

"Art. 32/1. In artikel 81 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, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden in het derde lid de woorden "bedoeld in het eerste lid" ingevoegd tussen de woorden "in zijn beslissing" en de woorden "opgave van";

2° paragraaf 1 wordt aangevuld met een lid, luidende:

"Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een in het tweede lid, 2°, bedoelde dienst, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, ook de medewerking vorderen van:

— de personen of instellingen bedoeld in artikel 5, § 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op basis van de referentie van een elektronische banktransactie die voorafgaand meegedeeld is door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid;

— de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden, die voorafgaand meegedeeld zijn door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid;

— des autres personnes morales qui sont l'abonné d'un des acteurs visés à l'alinéa 2, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er.";

3° au paragraphe 2, alinéa 2, les mots "les acteurs visés à l'alinéa 1er" sont remplacés par les mots "les acteurs visés au § 1er, alinéa 2, ainsi que les personnes et institutions visées au § 1er, alinéa 4,"."

JUSTIFICATION

L'amendement vise à prévoir explicitement que l'auditeur de la FSMA peut requérir la collaboration de certaines personnes et institutions en vue de procéder à l'identification (indirecte) de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques. Il faut en effet savoir que l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, tel que remplacé par l'amendement n° 6, comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés (méthode d'identification directe) ou à tout le moins de rendre cette identification possible (méthode d'identification indirecte). Dans le cas d'une identification directe, l'opérateur collecte et conserve des données fiables relatives à l'identité civile de l'abonné. Dans le cas d'une identification indirecte, l'opérateur collecte et conserve uniquement des données qui permettent d'obtenir d'un tiers l'identité de l'abonné.

Conformément à l'actuel article 81 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ("loi du 2 août 2002"), l'auditeur de la FSMA peut requérir les opérateurs d'un réseau de communications électroniques ainsi que 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") d'identifier l'abonné ou l'utilisateur habituel d'un tel service ou réseau. Par analogie avec ce que l'amendement n° 14 prévoit de faire (conformément à l'article 127, § 9, de la loi du 13 juin 2005 relative aux communications électroniques, tel qu'inséré par l'amendement n° 6) à l'article 46*bis* du Code d'instruction criminelle pour les autorités judiciaires, il est ajouté à l'article 81 de la loi du 2 août 2002 une disposition précisant que l'auditeur de la

— andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaand meegedeeld zijn door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid.";

3° in paragraaf 2, tweede lid, worden de woorden "de in het eerste lid bedoelde actoren" vervangen door de woorden "de actoren bedoeld in § 1, tweede lid en de personen en instellingen bedoeld in § 1, vierde lid"."

VERANTWOORDING

Het amendement heeft tot doel om uitdrukkelijk te voorzien dat de auditeur van de FSMA de medewerking kan vorderen van bepaalde personen en instellingen met het oog op de (indirecte) identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst. Het is immers zo dat artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zoals vervangen bij amendement nr. 6, een positieve verplichting voor de operatoren voorziet om hun abonnees te identificeren (directe identificatiemethode) of op zijn minst deze identificatie mogelijk te maken (indirecte identificatiemethode). In geval van directe identificatie verzamelt en bewaart de operator betrouwbare gegevens met betrekking tot de burgerlijke identiteit van de abonnee. In geval van indirecte identificatie verzamelt en bewaart de operator enkel gegevens aan de hand waarvan bij een derde de identiteit van de abonnee kan worden verkregen.

Overeenkomstig het bestaande artikel 81 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten ("wet van 2 augustus 2002"), kan de auditeur van de FSMA de identificatie van de abonnee of gewoonlijke gebruiker vorderen van 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). Naar analogie met wat amendement nr. 14 (in lijn met artikel 127, § 9, van de wet van 13 juni 2005 betreffende de elektronische communicatie, zoals ingevoegd bij amendement nr. 6) voorziet in artikel 46*bis* van het W. Sv. voor de gerechtelijke autoriteiten, wordt in artikel 81 van de wet van 2 augustus 2002 toegevoegd dat de auditeur van

FSMA peut également requérir la collaboration de certaines personnes et institutions pour procéder à l'identification (indirecte) de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques. Ces personnes et institutions seront elles aussi tenues de communiquer les données en question dans le délai fixé par l'auditeur (voir le paragraphe 2, alinéa 2, de l'article 81).

Cette nouvelle disposition permet d'assurer également pour l'auditeur de la FSMA que la méthode d'identification indirecte n'empêchera pas que l'abonné ou l'utilisateur habituel soit identifié. Pour davantage de précisions sur les catégories de personnes/institutions dont il peut requérir la collaboration et sur les conditions auxquelles il peut le faire, l'on se reportera à l'exposé des motifs portant sur l'amendement n° 14 pour les autorités judiciaires.

La collaboration de ces personnes/institutions, qui ne peut également être requise que par l'auditeur (ou, en son absence, par l'auditeur adjoint) de la FSMA, bénéficie des mêmes garanties matérielles et procédurales que la collaboration des opérateurs. Cela résulte du fait que leur collaboration ne s'avèrera nécessaire qu'après que l'auditeur aura requis et obtenu la collaboration des opérateurs.

La demande de collaboration adressée à ces personnes/institutions sera donc toujours nécessairement précédée d'une décision motivée et écrite de l'auditeur, par laquelle il requiert la collaboration des opérateurs. Dans cette décision, l'auditeur indique les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver sa décision, des principes de proportionnalité et de subsidiarité. À cet égard, il doit notamment mentionner le service de communications électroniques dont il souhaite identifier l'abonné ou l'utilisateur habituel, et motiver la raison pour laquelle cette identification est nécessaire aux fins visées à l'article 35, § 1er, alinéa 1er, de la loi du 2 août 2002. La même motivation vaut alors d'emblée aussi (sans devoir être réitérée) si, par la suite, la collaboration d'autres personnes/institutions est nécessaire en cas d'identification indirecte. L'autorisation préalable obligatoire délivrée par une juridiction ou une autorité administrative indépendante, laquelle constitue une garantie importante que le projet de loi portant dispositions diverses en matière financière prévoit d'inscrire également à l'article 81 de la loi du 2 août 2002 pour requérir des opérateurs de procéder à l'identification de l'abonné ou de l'utilisateur habituel, comporte d'emblée aussi l'autorisation de requérir par la suite, le cas échéant, la collaboration d'autres personnes /institutions en cas d'identification indirecte (sans que cette autorisation ne doive à nouveau être donnée). Enfin, le paragraphe 3 de l'article 81, en vertu duquel toute personne qui, du chef de sa fonction, a connaissance d'une demande de communication

de FSMA ook de medewerking kan vorderen van bepaalde personen en instellingen, met het oog op de (indirecte) identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst. Ook zij dienen deze gegevens te verschaffen binnen de door de auditeur bepaalde termijn (zie paragraaf 2, tweede lid, van artikel 81).

Zo wordt ook voor de auditeur van de FSMA verzekerd dat de indirecte identificatiemethode niet belet dat de abonnee of de gewoonlijke gebruiker wordt geïdentificeerd. Voor een toelichting bij de categorieën van personen/instellingen waarvan hij de medewerking kan vorderen en de voorwaarden waaronder hij dat kan doen, kan worden verwezen naar de memorie van toelichting bij amendement nr. 14 voor de gerechtelijke autoriteiten.

Voor de medewerking van deze personen/instellingen, die ook enkel kan worden gevorderd door de auditeur (of, in zijn afwezigheid, de adjunct-auditeur) van de FSMA, gelden dezelfde materiële en procedurele waarborgen als voor de medewerking van de operatoren. Dit volgt uit het feit dat hun medewerking pas nodig zal blijken nadat de auditeur de medewerking van de operatoren heeft gevorderd en bekomen.

Aan het vorderen van de medewerking van deze personen/instellingen gaat dus steeds noodzakelijkerwijze een gemotiveerde en schriftelijke beslissing van de auditeur vooraf, waarbij hij de medewerking van de operatoren vordert. In deze beslissing doet de auditeur opgave van de feitelijke omstandigheden die de maatregel rechtvaardigen en hij houdt rekening met het evenredigheids- en subsidiariteitsbeginsel bij de motivering van zijn beslissing. Daarbij dient hij met name de elektronische communicatiedienst waarvan hij de abonnee of gewoonlijke gebruiker wenst te identificeren te vermelden en te motiveren waarom deze identificatie nodig is voor de in artikel 35, § 1, eerste lid, van de wet van 2 augustus 2002 beoogde doeleinden. Dezelfde motivering geldt dan meteen ook (zonder dat deze moet worden herhaald) indien vervolgens de medewerking van andere personen/instellingen nodig is in geval van indirecte identificatie. De vereiste van een voorafgaande toestemming door een rechterlijke instantie of onafhankelijke administratieve autoriteit, een belangrijke waarborg die via het wetsontwerp houdende diverse bepalingen inzake financiën ook in artikel 81 van de wet van 2 augustus 2002 wordt voorzien om van de operatoren te vorderen tot identificatie van de abonnee of gewoonlijke gebruiker over te gaan, impliceert ook meteen de toestemming om nadien desgevallend de medewerking van andere personen/instellingen te vorderen in geval van indirecte identificatie (zonder dat deze toestemming opnieuw moet worden gegeven). Ten slotte geldt paragraaf 3 van

de données d'identification ou y prête son concours, est tenue de garder le secret, s'applique également à ces autres personnes/institutions.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

artikel 81, dat bepaalt dat iedere persoon die uit hoofde van zijn bediening kennis krijgt van een vordering tot mededeling van identificatiegegevens of daaraan zijn medewerking verleent, tot geheimhouding verplicht is, ook voor deze andere personen/instellingen.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

N° 16 **DU GOUVERNEMENT**

Art. 36/1 *(nouveau)*

Dans le chapitre 10, insérer un article 36/1, libellé comme suit:

"Art. 36/1. L'article 11, § 1er, de la même loi, remplacé par la loi du 10 avril 2014, est complété par un alinéa rédigé comme suit:

"Pour procéder à l'identification de la personne concernée, le chef du service Inspection produits de consommation peut requérir la collaboration des personnes ou institutions visées à l'article 5, § 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un opérateur au sens de l'article 2, 11° de la loi du 13 juin 2005 relative aux communications électroniques."."

JUSTIFICATION

Il convient tout d'abord de se référer à la justification de l'amendement n° 6, amendement qui remplace l'article 127 de la loi relative aux communications électroniques à la suite de l'arrêt de la Cour constitutionnelle n° 158/2021 du 18 novembre 2021. La Cour a annulé l'article 2 de la loi du 1er septembre 2016 "portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité", uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération.

En résumé, la Cour étais d'avis que les données d'identification et les documents d'identification qui doivent être conservés par les opérateurs en vertu de l'article 127 doivent être énumérés dans la loi elle-même, et que cette énumération ne peut être laissée au pouvoir exécutif par le biais d'une délégation au Roi.

Nr. 16 **VAN DE REGERING**

Art. 36/1 *(nieuw)*

In hoofdstuk 10, een artikel 36/1 invoegen, luidende:

"Art. 36/1. Artikel 11, § 1, van dezelfde wet, vervangen bij de wet van 10 april 2014, wordt aangevuld met een lid, luidende:

"Met het oog op de identificatie van de betrokkene kan het diensthoofd van de inspectiedienst consumptieproducten de medewerking vorderen van de personen of instellingen, bedoeld in artikel 5, § 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een operator in de zin van artikel 2, 11° van de wet van 13 juni 2005 betreffende de elektronische communicatie."."

VERANTWOORDING

Er kan eerst en vooral verwezen worden naar de toelichting bij amendement nr. 6, amendement dat het artikel 127 van de wet betreffende de elektronische communicatie vervangt als gevolg van arrest nr. 158/2021 van 18 november 2021 van het Grondwettelijk Hof. Het Hof heeft artikel 2 van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst vernietigd, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen.

Samengevat komt het erop neer dat het Hof van oordeel was dat de identificatiegegevens en de identificatiedocumenten die door operatoren op grond van artikel 127 bewaard moeten worden, opgesomd moeten worden in de wet zelf, en dat die opsomming niet via een delegatie aan de Koning aan de uitvoerende macht kunnen worden overgelaten.

Le gouvernement a donc décidé de donner suite à cet arrêt en énumérant les données d'identification et les documents d'identification à l'article 127 de la loi.

L'article 127 de la loi contient des méthodes d'identification directes et indirectes.

Par "méthode d'identification directe", on entend la méthode par laquelle l'opérateur collecte et conserve des données fiables relatives à l'identité civile d'une personne physique qui est son abonné ou qui agit pour le compte de son abonné qui est une personne morale afin de remplir les obligations d'identification de la personne morale et, le cas échéant, une copie du document d'identité de cette personne physique.

En revanche, la "méthode indirecte d'identification" désigne la méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés.

Le nouvel article 127 comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés (méthode d'identification directe) ou à tout le moins de rendre cette identification possible (méthode d'identification indirecte).

Ce projet de loi modifie également 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 et introduit la base juridique de l'identification des personnes physiques et morales sur la base du numéro de téléphone de la personne concernée ou l'adresse IP de la source de la communication électronique.

Étant donné qu'il n'est pas certain à l'avance si une telle identification est une forme d'identification directe ou indirecte, la disposition de modification doit être adaptée de manière à ce qu'une identification indirecte soit également possible. Cette dernière forme nécessite une base juridique explicite.

Il est question d'identification directe lorsque le service inspection requiert la collaboration des opérateurs ou des fournisseurs de services de communications électroniques, et obtient ensuite l'identification directement de ces opérateurs ou fournisseurs de services.

Toutefois, il est également possible que le service inspection reçoive d'autres informations d'un opérateur, avec lesquelles il doit ensuite faire appel à d'autres personnes ou

Daarom heeft de regering beslist om gevolg te geven aan dit arrest door de identificatiegegevens en de identificatiedocumenten op te sommen in artikel 127 van de wet.

Artikel 127 van de wet bevat directe en indirecte identificatiemethodes.

Onder "directe identificatiemethode" dient te worden verstaan de methode waarbij de operator betrouwbare gegevens verzamelt en bewaart met betrekking tot de burgerlijke identiteit van een natuurlijke persoon die zijn abonnee is of die optreedt voor rekening van zijn abonnee die een rechtspersoon is om de verplichtingen inzake identificatie van de rechtspersoon te vervullen en, in voorkomend geval, een kopie van het identiteitsstuk van deze natuurlijke persoon.

De "indirecte identificatiemethode" daarentegen, doelt op de methode waarbij de operator gegevens verzamelt en bewaart aan de hand waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen.

Het nieuwe artikel 127 bevat nu een positieve verplichting voor de operatoren om hun abonnees te identificeren (directe identificatiemethode) of op zijn minst deze identificatie mogelijk te maken (indirecte identificatiemethode).

Het wetsontwerp wijzigt artikel 11 van de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere produkten en voert de wettelijke basis in 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

Omdat het op voorhand niet zeker is of dergelijke identificatie een vorm van directe of indirecte identificatie is, dient de wijzigingsbepaling te worden aangepast zodat indirecte identificatie ook mogelijk is. Voor deze laatste vorm is immers een uitdrukkelijke wettelijke basis nodig.

Er is sprake van directe identificatiemethode wanneer de inspectiedienst daarvoor de medewerking vordert van operatoren of verstrekkers van elektronische communicatiediensten, en daarop volgend de identificatie rechtstreeks van deze operator of dienstenverstrekkers verkrijgt.

Het is echter ook mogelijk dat de inspectiedienst van een operator andere informatie krijgt waarmee hij vervolgens een beroep moet doen op andere personen of instellingen om de

institutions pour obtenir une identification. L'article 11 vise également à fournir ce moyen d'identification.

Le gouvernement est d'avis que cette possibilité doit être plus précisée dans les lois organiques des autorités qui souhaitent faire usage de ces méthodes d'identification indirecte. L'article 11 de la loi du 24 janvier 1977 doit donc être complétée.

Le présent amendement introduit la possibilité d'une identification indirecte par les banques et les établissements financiers. Pour déterminer le champ d'application, il est fait référence aux personnes et institutions visées à l'article 5, § 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces

Les modifications prévues à l'article 11 par le présent amendement sont parfaitement conformes à ce qui est prévu à l'article 127, § 9, de la loi relative aux communications électroniques.

Il est explicitement prévu dans l'amendement que le service inspection ne peut faire appel aux établissements financiers que s'il dispose d'une référence d'une transaction électronique bancaire.

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

Petra DE SUTTER

identificatie te verkrijgen. Ook deze manier om tot identificatie over te gaan wordt beoogd door artikel 11.

De regering is van mening dat deze mogelijkheid verder gepreciseerd dient te worden in de organieke wetten van de autoriteiten die een beroep wensen te doen op deze indirecte identificatiemethodes. Artikel 11 van de wet van 24 januari 1977 dient bijgevolg te worden aangevuld.

Het huidig amendement voegt de mogelijkheid tot indirecte identificatie in via de banken en de financiële instellingen. Om het toepassingsgebied te bepalen wordt verwezen naar de personen en instellingen als bedoeld in artikel 5, § 1, 3° tot 22°, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.

De aanpassingen die door huidig amendement voorzien worden in artikel 11, liggen volledig in de lijn van wat in artikel 127, § 9, van de wet betreffende de elektronische communicatie wordt voorzien.

Er wordt expliciet voorzien in het amendement dat de inspectiedienst slechts een beroep kan doen op de financiële instellingen wanneer hij beschikt over de referentie van een elektronische banktransactie.

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

Petra DE SUTTER

Imprimerie centrale – Centrale drukkerij