DOC 55 **2317/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

19 novembre 2021

PROJET DE LOI

introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G

SOMMAIRE Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

19 november 2021

WETSONTWERP

tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten

INHOUD Blz.

05628

Le gouvernement a déposé ce projet de loi le 19 novembre 2021.	*De regering heeft dit wetsontwerp op 19 november 2021 ingediend.*
Le "bon à tirer" a été reçu à la Chambre le 24 novembre 2021.	*De "goedkeuring tot drukken" werd op 24 november 2021 door de Kamer ontvangen.*

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

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

RÉSUMÉ

Le 9 octobre 2019, le groupe de coopération NIS a publié un rapport sur l'évaluation coordonnée des risques liés à la cybersécurité des réseaux de cinquième génération (5G).

En janvier 2020, une boîte à outils commune contenant des mesures d'atténuation des risques a été publiée par le groupe de coopération NIS. Le but est de proposer des solutions concernant les risques identifiés dans le rapport précité.

La Commission européenne a apporté son soutien à la mise en œuvre de cette boîte à outils et l'a encouragée via la publication le 29 janvier 2020 de sa communication "Sécurité du déploiement de la 5G dans l'UE – Mise en œuvre de la boîte à outils de l'UE" au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions.

Afin de mettre en œuvre cette boîte à outils, il a été choisi d'insérer un nouvel article 105 dans la loi du 13 juin 2005 relative aux communications électroniques. En voici les grandes lignes:

— Les MNO (Mobile Network Operators) doivent obtenir une autorisation préalable (ou une autorisation de régularisation) pour pouvoir utiliser un élément de leur réseau 5G;

— Les MNO sont également tenus d'obtenir une autorisation préalable (ou une autorisation de régularisation) pour pouvoir faire appel à certains prestataires de services;

— Lorsqu'un MNO offre des services de communications électroniques en Belgique à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des États membres de l'Union européenne. En complément, les MNO peuvent se voir imposer des règles pour qu'ils exercent les activités qui sont absolument nécessaires pour le fonctionnement, la sécurité et la continuité de leur réseau sur le territoire des États membres de l'UE.

Tout ce qui précède peut être étendu à une ou plusieurs catégories de MVNO (Mobile Virtual Network Operators) et à certains fournisseurs de réseaux privés.

SAMENVATTING

Op 9 oktober 2019 heeft de NIS-samenwerkingsgroep een rapport gepubliceerd over de gecoördineerde risicobeoordeling betreffende de cyberbeveiliging van netwerken van de vijfde generatie (5G).

In januari 2020 werd een gemeenschappelijke toolbox voor risicobeperkende maatregelen gepubliceerd door de NIS-samenwerkingsgroep, met als doel oplossingen aan te reiken voor de risico's die geïdentificeerd zijn in het voormelde rapport.

De Europese Commissie heeft de uitvoering van deze toolbox gesteund en aangemoedigd via de publicatie op 29 januari 2020 van haar mededeling "Uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox" aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en aan het Comité van de Regio's.

Om deze toolbox uit te voeren werd ervoor gekozen om een nieuw artikel 105 in te voegen in de wet van 13 juni 2005 betreffende de elektronische communicatie. De grote lijnen hiervan zijn de volgende:

— MNO's (Mobile Network Operators) moeten een voorafgaande machtiging (of machtiging tot regularisatie) verkrijgen om een element van hun 5G-netwerk te mogen gebruiken;

— MNO's kunnen ook worden verplicht om een voorafgaande machtiging (of machtiging tot regularisatie) te verkrijgen om beroep te mogen doen op sommige dienstenaanbieders;

— Wanneer een MNO in België elektronischecommunicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuren van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. De MNO's kunnen bijkomstig regels worden opgelegd opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk uitoefenen binnen het grondgebied van de lidstaten van de EU.

Al het voorgaande kan worden uitgebreid naar één of meer categorieën van MVNO's (Mobile Virtual Network Operators) en naar bepaalde aanbieders van private netwerken.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

1. **Le déploiement de la 5G**

Le déploiement des réseaux de communications électroniques de cinquième génération (ci-après 5G) figure aujourd'hui au rang des priorités de l'agenda politique, des opérateurs mobiles et des entreprises.

La 5G présente des avantages considérables par rapport aux générations précédentes de réseaux mobiles: elle est plus rapide, elle a un temps de réaction plus court (ce qui est important pour les applications tributaires du temps) et elle peut connecter davantage d'objets différents. En outre, la 5G est plus efficace du point de vue énergétique et en termes d'utilisation du spectre, une ressource rare.

Concrètement il faut penser aux grues automatiques dans les ports, aux pilotes qui, par gros temps, manœuvrent un bateau dans un port au centimètre près depuis leur ordinateur chez eux, à l'automatisation sans fil dans l'industrie de l'assemblage ou de la logistique; dans les transports en commun, il s'agit des métros autonomes et dans le secteur médical, les données des patients seront transmises sans fil au sein des réseaux hospitaliers, les ambulances transmettront les données des patients en direct aux urgences et les médecins pourront établir leur diagnostic à distance. La 5G devient également de plus en plus importante pour les applications dans les villes intelligentes telles que la gestion des flux de trafic et l'indication des places de parking disponibles, et l'on peut également penser à des applications dans le domaine de l'environnement telles que la surveillance de la qualité de l'air à l'aide de compteurs de particules fines. La 5G est également considérée comme la pierre angulaire d'applications d'intelligence artificielle (AI).

La 5G améliorera aussi la couverture, ce qui permettra d'avoir une connexion de meilleure qualité, même en étant à l'intérieur.

2. **Les travaux concernant la sécurité de la 5G effectués au niveau de l'Union européenne**

Vu l'importance de pouvoir se reposer sur des infrastructures sûres et fiables et d'assurer une souveraineté et autonomie numérique européenne, divers travaux ont

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

1. **De 5G-uitrol**

De uitrol van de elektronische-communicatienetwerken van de vijfde generatie (hierna 5G) vormt vandaag een van de prioriteiten op de politieke agenda, alsook van de mobiele operatoren en de ondernemingen.

5G houdt aanzienlijke voordelen in ten opzichte van de vorige generaties van mobiele netwerken: het is sneller, heeft een kortere reactietijd (wat belangrijk is voor de tijdkritische applicaties) en kan een groter aantal verschillende objecten verbinden. Bovendien is 5G efficiënter in energieverbruik en in termen van gebruik van het spectrum, een schaarse hulpbron.

Concreet moet daarbij worden gedacht aan automatische kranen in havens, aan bestuurders die bij hevige weersomstandigheden van op hun computer thuis een schip in een haven tot op de centimeter kunnen manoeuvreren, aan de draadloze automatisering in de assemblage- of logistieke industrie; qua openbaar vervoer gaat het om zelfrijdende metrostellen en in de medische wereld zullen de patiëntengegevens draadloos worden verstuurd binnen de ziekenhuisnetwerken, ambulances zullen de patiëntengegevens live doorsturen naar de spoedafdelingen en artsen zullen hun diagnose van op een afstand kunnen stellen. 5G wordt ook alsmaar belangrijker voor toepassingen in slimme steden zoals het beheer van de verkeersstromen en de aanduiding van beschikbare parkeerplaatsen, en men kan ook denken aan toepassingen op het gebied van het milieu zoals de bewaking van de luchtkwaliteit met behulp van fijnstofmeters. Tevens wordt 5G beschouwd als de hoeksteen voor AI-toepassingen (artificiële intelligentie).

5G zal ook de dekking verbeteren, waardoor een verbinding van betere kwaliteit mogelijk zal worden, ook binnenshuis.

2. **De werkzaamheden betreffende de beveiliging van 5G binnen de Europese Unie**

Gelet op het belang om te kunnen steunen op veilige en betrouwbare infrastructuren en een Europese digitale soevereiniteit en autonomie te garanderen, zijn op het

été menés au niveau de l'Union européenne concernant la sécurité de la 5G.

Ces travaux ont été effectués entre autres par le groupe de coopération NIS. Ce groupe a été institué par l'article 11 de la directive "NIS" (directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union) et est composé de représentants des États membres, de la Commission et de l'ENISA (l'Agence de l'Union européenne pour la cybersécurité).

Le groupe de coopération NIS a publié le 9 octobre 2019 un rapport sur l'évaluation coordonnée des risques liés à la cybersécurité dans les réseaux de cinquième génération (5G) ("*CG Publication 02/2019 - Risk assessment of 5G networks*").

Ce rapport identifie un certain nombre de défis importants en matière de sécurité, qui vont apparaître avec la venue des réseaux 5G ou que ces derniers vont intensifier. Un de ces défis est, selon ce rapport (§ 2.36., p.22), le fait que "Le plus grand rôle joué par les logiciels et services fournis par des fournisseurs tiers au sein des réseaux 5G provoque une plus grande exposition à un certain nombre de vulnérabilités susceptibles de découler du profil de risque de fournisseurs individuels." (traduction libre)

Selon ce même rapport (§ 2.37, p.22), "Les profils de risque des fournisseurs individuels peuvent être évalués sur la base de plusieurs facteurs, notamment:

— La probabilité que le fournisseur subisse des ingérences d'un pays non européen. […]

— La capacité du fournisseur à garantir l'approvisionnement;

— La qualité globale des produits et pratiques de cybersécurité du fournisseur […]" (traduction libre)

En janvier 2020, le groupe de coopération NIS a publié la boîte à outils commune de mesures d'atténuation des risques. ("*CG Publication 01/2020: Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*"). Cette boîte à outils entend apporter des solutions par rapport aux risques qui ont été identifiés dans son rapport sur l'évaluation coordonnée des risques liés à la cybersécurité dans les réseaux de cinquième génération (5G).

niveau van de Europese Unie diverse werkzaamheden verricht wat de 5G-beveiliging betreft.

Dat werk is onder andere verricht door de NIS-samenwerkingsgroep. Deze groep is ingesteld door artikel 11 van de "NIS-richtlijn" (Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie) en is samengesteld uit vertegenwoordigers van de lidstaten, van de Commissie en van het ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging).

De NIS-samenwerkingsgroep heeft op 9 oktober 2019 een rapport gepubliceerd over de gecoördineerde risicobeoordeling betreffende de cyberbeveiliging van netwerken van de vijfde generatie (5G) ("*CG Publication 02/2019 - Risk assessment of 5G networks*").

Dit rapport identificeert een aantal belangrijke uitdagingen op het gebied van beveiliging die zullen opduiken met de komst van de 5G-netwerken of die door deze laatste groter zullen worden. Een van die uitdagingen ligt, volgens het rapport (§ 2.36., p. 22), in het volgende feit: "De grotere rol die binnen de 5G-netwerken zal worden gespeeld door de software en diensten die worden verstrekt door derde leveranciers brengt een grotere blootstelling aan een aantal kwetsbaarheden die kunnen voortvloeien uit het risicoprofiel van individuele leveranciers met zich mee." (vrije vertaling).

Volgens datzelfde rapport (§ 2.37, p. 22) kunnen de risicoprofielen van de individuele leveranciers worden beoordeeld op basis van verschillende factoren, met name:

— de kans dat de leverancier inmenging van een niet-Europees land ondervindt. […]

— het vermogen van de leverancier om de bevoorrading te garanderen;

— de algemene kwaliteit van de producten en praktijken inzake cyberbeveiliging van de leverancier […]" (vrije vertaling)

In januari 2020 heeft de NIS-samenwerkingsgroep de gemeenschappelijke toolbox voor risicobeperkende maatregelen gepubliceerd. ("*CG Publication 01/2020: Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*"). De bedoeling van deze toolbox is om oplossingen aan te reiken voor de risico's die geïdentificeerd zijn in zijn rapport over de gecoördineerde risicobeoordeling betreffende de cyberbeveiliging van netwerken van de vijfde generatie (5G).

Selon cette boîte à outils (page 18), les États membres “devraient:

— renforcer les exigences de sécurité pour les opérateurs de réseau mobile (contrôles d’accès stricts, règles concernant la sécurité de l’exploitation et de la surveillance, limitation de l’externalisation de certaines fonctions, etc.);

— évaluer les profils de risque des fournisseurs; en conséquence, appliquer des restrictions pertinentes pour les fournisseurs considérés comme à haut risque – y compris les exclusions nécessaires pour atténuer effectivement les risques – pour les actifs essentiels définis comme critiques et sensibles dans l’évaluation coordonnée des risques pour l’UE (par exemple, les fonctions de réseau de base, les fonctions de gestion et d’orchestration et les fonctions de réseau d’accès);

— veiller à ce que chaque opérateur se dote d’une stratégie multifournisseurs appropriée pour éviter ou limiter toute dépendance majeure à l’égard d’un seul fournisseur (ou de fournisseurs présentant un profil de risque similaire), garantir un équilibre suffisant entre les fournisseurs au niveau national et éviter la dépendance à l’égard des fournisseurs considérés comme à haut risque; cela nécessite également d’éviter toute situation d’enfermement propriétaire, notamment en promouvant une interopérabilité accrue des équipements.” (traduction libre)

La Commission européenne a soutenu et encouragé la mise en œuvre de cette boîte à outils, en publiant le 29 janvier 2020 sa communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Sécurité du déploiement de la 5G dans l’UE – Mise en œuvre de la boîte à outils de l’UE.

3. **La sécurité des communications dans le cadre du déploiement de la 5G en Belgique**

Un incident de sécurité affectant les réseaux 5G pourrait avoir un impact négatif significatif sur la sûreté, l’économie, les citoyens, les services publics belges ou les organisations internationales situées sur le territoire belge. Il convient à cet égard de rappeler que la Belgique occupe une situation particulière par rapport à d’autres États vu qu’elle accueille plusieurs institutions européennes ainsi que plusieurs sites militaires de l’OTAN. Cet impact peut être significatif tant en cas d’actes malveillants – espionnage, sabotage, attaque informatique dirigée contre des services – qu’en cas de graves problèmes techniques non intentionnels.

Volgens die toolbox (pagina 18) zouden de lidstaten het volgende moeten doen:

— “de beveiligingseisen voor exploitanten van mobiele netwerken aanscherpen (bv. strenge toegangscontroles, regels voor veilige exploitatie en monitoring, beperkingen op het uitbesteden van specifieke functies enz.);

— het risicoprofiel van leveranciers beoordelen; en dus relevante beperkingen toepassen voor leveranciers die worden geacht een hoog risico te vormen – met inbegrip van de nodige uitsluitingen om de risico’s effectief te beperken – voor essentiële activa die als kritiek en gevoelig worden gedefinieerd in de gecoördineerde EU-risicobeoordeling (bv. functies van het kernnetwerk, netwerkbeheers- en orkestratiefuncties, en toegangsnetwerkfuncties);

— ervoor zorgen dat elke operator een passende multivendor-strategie heeft om verregaande afhankelijkheid van individuele leveranciers (of leveranciers met een vergelijkbaar risicoprofiel) te voorkomen of te beperken, een passend evenwicht van leveranciers op nationaal niveau te garanderen en afhankelijkheid van leveranciers die worden geacht een hoog risico te vormen te vermijden; dit betekent ook dat een lock-in door bepaalde leveranciers moet worden voorkomen, onder andere door een grotere interoperabiliteit van apparatuur te bevorderen.” (vrije vertaling)

De Europese Commissie heeft de uitvoering van deze toolbox gesteund en aangemoedigd via de publicatie op 29 januari 2020 van haar mededeling aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en aan het Comité van de Regio’s, Uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox.

3. **De beveiliging van de communicatie in het kader van de 5G-uitrol in België**

Een beveiligingsincident dat de 5G-netwerken treft zou een aanzienlijke negatieve impact kunnen hebben op de veiligheid, de economie, de burgers, de Belgische overheidsdiensten of de internationale organisaties op het Belgische grondgebied. Daarbij dient eraan te worden herinnerd dat België in een bijzondere situatie verkeert ten opzichte van andere staten, aangezien het verscheidene Europese instellingen alsook verschillende militaire sites van de NATO huisvest. Deze impact kan aanzienlijk zijn zowel in geval van kwaadwillige handelingen – spionage, sabotage, cyberaanval gericht tegen diensten – als in geval van onopzettelijke ernstige technische problemen.

La crise sanitaire due au COVID-19 a montré la grande dépendance de la société aux communications électroniques. Cette dépendance va être décuplée par l'émergence de systèmes connectés rendant essentielle la sécurité des communications électroniques.

Par ailleurs, il est essentiel de préserver la sécurité et la discrétion des interceptions effectuées par les autorités judiciaires et les services de renseignement et de sécurité conformément à leur législation, ainsi que la capacité de ces services à effectuer de telles interceptions.

4. **La solution retenue: un système d'autorisation préalable introduit dans la loi du 13 juin 2005 relative aux communications électroniques**

Tout comme c'est le cas en Belgique, d'autres pays européens (France, Pays-Bas, Italie, Royaume-Uni, Suède, etc.) ont pris ou ont l'intention de prendre des mesures par rapport aux équipementiers à haut risque dans le cadre de la 5G.

Pour mettre en œuvre ces mesures, le présent avant-projet de loi met en place un système d'autorisation préalable des ministres concernés dans le cadre du déploiement de la 5G, comme c'est le cas dans d'autres pays (par exemple en France).

Cependant, dans un souci de transparence, les restrictions imposées aux opérateurs, à l'exception de la liste des zones sensibles et de l'identité des fournisseurs qui seraient considérés comme à haut risque, seront détaillées dans un arrêté royal, dont les ministres concernés tiendront compte lors de l'octroi de leur autorisation.

Le système d'autorisation préalable est introduit dans la loi du 13 juin 2005 relative aux communications électroniques, vu qu'il concerne en premier lieu les opérateurs télécom et qu'il touche, en tout cas en ce qui concerne la qualité des produits et pratiques des fournisseurs en termes de sécurité, à la sécurité des réseaux et services des opérateurs. Cette dernière est définie comme suit dans l'article 2, 21), de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen: "la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées ou des services connexes offerts par ces

De gezondheidscrisis die door COVID-19 is veroorzaakt, heeft aangetoond dat de maatschappij sterk afhankelijk is van elektronische communicatie. Deze afhankelijkheid zal nog veel groter worden door de opkomst van geconnecteerde systemen, die de beveiliging van de elektronische communicatie essentieel maken.

Bovendien is het van fundamenteel belang om de veiligheid en de discretie van de onderscheppingen verricht door de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten overeenkomstig hun wetgeving, alsook het vermogen van deze diensten om dergelijke onderscheppingen te doen, te vrijwaren.

4. **De gekozen oplossing: een systeem van voorafgaande machtiging ingevoerd in de wet van 13 juni 2005 betreffende de elektronische communicatie**

Net zoals het geval is in België hebben andere Europese landen (Frankrijk, Nederland, Italië, Verenigd Koninkrijk, Zweden, enz.) maatregelen genomen of zijn ze van plan dat te doen ten opzichte van producenten van netwerkelementen die een hoog risico vormen in het kader van 5G.

Om deze maatregelen uit te voeren stelt het onderhavige voorontwerp van wet een systeem in van voorafgaande machtiging van de betrokken ministers in het kader van de 5G-uitrol, zoals dat ook het geval is in andere landen (bijvoorbeeld in Frankrijk).

Omwille van de transparantie zullen de restricties die worden opgelegd aan de operatoren, met uitzondering van de lijst van de gevoelige zones en van de identiteit van de leveranciers die zouden worden geacht een hoog risico te vormen, niettemin worden gedetailleerd in een koninklijk besluit, waarmee de betrokken ministers rekening zullen houden bij het geven van hun machtiging.

Het systeem van voorafgaande machtiging wordt ingevoerd in de wet van 13 juni 2005 betreffende de elektronische communicatie, aangezien het op de eerste plaats betrekking heeft op de telecomoperatoren en, althans wat betreft de kwaliteit van de producten en praktijken van de leveranciers in termen van beveiliging, raakt aan de beveiliging van de netwerken en diensten van de operatoren. Deze laatste wordt als volgt gedefinieerd in artikel 2, 21), van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie: "het vermogen van elektronischecommunicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van die netwerken en

réseaux ou services de communications électroniques ou rendus accessibles via de tels réseaux ou services".

Dès lors que certains opérateurs ont déjà commencé à déployer la 5G et afin de minimiser l'impact de la présente loi sur leur stratégie de déploiement 5G, il importe de fixer rapidement les exigences en la matière.

5. **Explications techniques relatives au réseau 5G**

On peut considérer que le réseau 5G est composé de trois parties, à savoir le réseau d'accès radioélectrique (qui comprend les stations de base), le réseau de transport et la partie centrale du réseau (qui comprend entre autres le cœur du réseau, en ce compris les OSS ("*operations support system*") et BSS ("*business support system*")). Ces différentes parties du réseau sont elles-mêmes composées de différents éléments, qu'il s'agisse de dispositifs matériels (en anglais "hardware") ou de logiciels (en anglais "software").

L'arrêté royal qui exécutera l'article 105 précisera ce que chaque partie du réseau comprend.

diensten, van de opgeslagen, verzonden of verwerkte gegevens of van de daaraan gerelateerde diensten die via die elektronischecommunicatienetwerken en -diensten worden aangeboden of toegankelijk zijn, in gevaar brengen".

Omdat sommige operatoren reeds 5G zijn beginnen uit te rollen en om de impact van de onderhavige wet op hun strategie inzake 5G-uitrol tot een minimum te beperken, is het belangrijk om snel de eisen ter zake vast te stellen.

5. **Technische uitleg betreffende het 5G-netwerk**

Men kan stellen dat het 5G-netwerk uit drie delen bestaat, namelijk het radiotoegangsnetwerk (dat de basisstations omvat), het transportnetwerk en het centrale deel van het netwerk (dat onder andere het corenetwerk omvat, waaronder het OSS ("*operations support system*") en het BSS ("*business support system*") vallen). Deze verschillende delen van het netwerk bestaan zelf uit verschillende elementen, hetzij hardware, hetzij software.

Het koninklijk besluit dat uitvoering zal geven aan artikel 105 zal preciseren wat elk deel van het netwerk omvat.

COMMENTAIRE ARTICLE PAR ARTICLE

TOELICHTING BIJ DE ARTIKELEN

CHAPITRE 2

HOOFDSTUK 2

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

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

Art. 2

L'article 2 définit dorénavant les notions de MNO (Mobile Network Operator ou un opérateur de réseaux mobile) et de MVNO (*Mobile Virtual Network Operator* ou opérateur de réseau mobile virtuel). Un opérateur de réseau mobile (MNO) dispose d'un réseau d'accès radioélectrique propre (réseau RAN), ainsi que de tous les éléments utiles à l'exploitation du réseau. Contrairement à un MNO, un opérateur de réseau mobile virtuel (MVNO) ne dispose ni d'un réseau d'accès radioélectrique propre ni d'une licence de spectre.

Art. 2

Artikel 2 definieert voortaan de begrippen van MNO (Mobile Network Operator of mobiel-netwerkoperator) en van MVNO (*Mobile Virtual Network Operator* of virtuele mobiel-netwerkoperator). Een mobiel-netwerkoperator (MNO) beschikt over zijn eigen radiotoegangsnetwerk (RAN-netwerk), alsook over alle nuttige elementen voor de exploitatie van het netwerk. In tegenstelling tot een MNO, beschikt een virtuele mobiel-netwerkoperator (MVNO) noch over een eigen radiotoegangsnetwerk, noch over een spectrumvergunning.

Art. 3

Cet article remplace l'article 105 de la loi du 13 juin 2005 relative aux communications électroniques qui est devenu obsolète.

Paragraphe 1er

L'alinéa 1er du paragraphe 1er introduit le système de l'autorisation préalable, étant donné que les éléments du réseau 5G sont en principe produits par un équipementier, qui peut avoir un profil à haut risque. L'autorisation est une autorisation commune des ministres concernés. Il s'agit donc d'un seul et unique acte juridique auquel les ministres concernés consentent formellement dans le cadre d'une seule et même procédure.

L'obligation d'autorisation préalable est nécessaire pour la préservation des intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, à savoir:

— la défense de l'intégrité du territoire national et des plans de défense militaire;

— l'accomplissement des missions des forces armées;

— la sûreté intérieure de l'État, y compris dans le domaine de l'énergie nucléaire, et la pérennité de l'ordre démocratique et constitutionnel;

— la sûreté extérieure de l'État et les relations internationales de la Belgique;

— le potentiel scientifique et économique du pays;

— tout autre intérêt fondamental de l'État. Cela comprend notamment la préservation de la sécurité et de la discrétion des interceptions effectuées par les autorités judiciaires et les services de renseignement et de sécurité;

— la sécurité des ressortissants belges à l'étranger;

— le fonctionnement des organes décisionnels de l'État;

— la sécurité des personnes auxquelles, en vertu du Code d'instruction criminelle, des mesures de protection spéciales sont octroyées.

Art. 3

Dit artikel vervangt het achterhaalde artikel 105 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Paragraaf 1

Het eerste lid van paragraaf 1 introduceert het systeem van voorafgaande machtiging, aangezien de elementen van het 5G-netwerk in principe worden vervaardigd door een producent van netwerkelementen, die een hoog risicoprofiel kan hebben. De machtiging is een gemeenschappelijke machtiging van de betrokken ministers. Het gaat dus om één enkele rechtshandeling waarmee de betrokken ministers formeel instemmen in het kader van één en dezelfde procedure.

De verplichting tot voorafgaande machtiging is noodzakelijk voor de vrijwaring van de belangen bedoeld in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, namelijk:

— de verdediging van de onschendbaarheid van het nationaal grondgebied en van de militaire defensieplannen;

— de vervulling van de opdrachten van de strijdkrachten;

— de inwendige veiligheid van de Staat, met inbegrip van het domein van de kernenergie, en het voortbestaan van de democratische en grondwettelijke orde;

— de uitwendige veiligheid van de Staat en de internationale betrekkingen van België;

— het wetenschappelijk en economisch potentieel van het land;

— elk ander fundamenteel belang van de Staat. Dit omvat onder andere het vrijwaren van de veiligheid en de discretie van de onderscheppingen door de gerechtelijke overheden en de inlichtingen- en veiligheidsdiensten;

— de veiligheid van de Belgische onderdanen in het buitenland;

— de werking van de besluitvormingsorganen van de Staat;

— de veiligheid van de personen aan wie, krachtens het Wetboek van Strafvordering, bijzondere beschermingsmaatregelen worden toegekend.

La portée de ces intérêts est exposée dans une directive du 25 mai 2001 du Comité ministériel du renseignement et de sécurité (aujourd'hui: le Conseil national de sécurité) relative aux modalités de classification, de déclassification et de modification du degré de classification (DIFFUSION RESTREINTE).

En application du paragraphe 1er, alinéa 1er, de l'article 105, un MNO qui fournit un réseau mobile 5G devra obtenir une nouvelle autorisation, lorsqu'il souhaite utiliser un élément de réseau et que cette utilisation n'est pas couverte par l'autorisation qu'il a reçue. A titre d'exemple, une nouvelle autorisation doit être demandée si:

— un opérateur veut avoir recours à un autre équipementier que ceux qu'il a mentionnés dans sa demande initiale;

— il veut utiliser d'autres éléments de réseau d'un équipementier que ceux qui sont couverts par l'autorisation ou, en cas d'éléments de réseaux fournis par un équipementier à haut risque, il veut augmenter le nombre de sites dans lesquels ils sont utilisés.

Dans son avis, le Conseil d'État indique que la situation des fournisseurs de services n'est pas claire pour lui. Pour tenir compte de cette remarque, la loi précise que le Roi peut soumettre les MNO à une autorisation préalable avant qu'ils puissent bénéficier de toute une série de services d'un fournisseur (intervention ponctuelle dans la gestion du réseau, notamment en cas d'incident ou de modification majeure du réseau ou gestion ou supervision quotidienne des éléments du réseau ou pour certains de ces fournisseurs) ou de certains de ces services. En d'autres termes, le Roi sera amené à identifier les services fournis au MNO par un tiers qui nécessitent une autorisation préalable.

L'extension aux fournisseurs de services ne pourra être effectuée par arrêté royal que pour autant que ce même arrêté contienne les mesures de restriction pour le recours à de tels fournisseurs.

Lors de l'examen de la demande d'autorisation préalable et sur base des avis des services de renseignement et de sécurité et de l'Institut, les ministres concernés devront déterminer si le fournisseur de services auquel le MNO souhaite faire appel doit être qualifié de fournisseur à haut risque. Les restrictions applicables dans l'arrêté royal ne s'appliqueront que pour le recours de MNO à des fournisseurs de services à haut risque.

De draagwijdte van deze belangen wordt uiteengezet in een richtlijn van 25 mei 2001 van het Ministerieel Comité voor Inlichting en Veiligheid (nu: Nationale Veiligheidsraad) betreffende de nadere regels voor classificatie, declassificatie en wijziging van het classificatieniveau (BEPERKTE VERSPREIDING).

Overeenkomstig paragraaf 1, eerste lid, van artikel 105 zal een MNO die een mobiel 5G-netwerk aanbiedt een nieuwe machtiging moeten krijgen, wanneer hij een netwerkelement wenst te gebruiken en dit gebruik niet onder de machtiging valt die hij gekregen heeft. Er moet bijvoorbeeld een nieuwe machtiging worden gevraagd als:

— een operator een beroep wil doen op een andere producent van netwerkelementen dan diegene die hij in zijn aanvankelijke aanvraag heeft vermeld;

— hij andere netwerkelementen van een producent van netwerkelementen wil gebruiken dan diegene die onder de machtiging vallen of, in geval van netwerkelementen die geleverd zijn door een producent die een hoog risico vormt, hij het aantal sites wil verhogen waarin die worden gebruikt.

In zijn advies geeft de Raad van State aan dat de situatie van de dienstenaanbieders voor hem niet duidelijk is. Rekening houdend met deze opmerking, preciseert de wet dat de Koning de MNO's kan onderwerpen aan een voorafgaande machtiging voordat zij een hele reeks diensten van een aanbieder kunnen genieten (gerichte ingreep in het beheer van het netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks beheer van of toezicht op de elementen van het netwerk of voor sommige van die aanbieders) of sommige van deze diensten. De Koning zal met andere woorden moeten bepalen voor welke door een derde aan de MNO aangeboden diensten een voorafgaande machtiging is vereist.

De uitbreiding naar aanbieders van diensten kan via koninklijk besluit maar gebeuren voor zover datzelfde besluit de beperkende maatregelen bevat voor het beroep op dergelijke aanbieders.

Bij het onderzoek van het verzoek om voorafgaande machtiging en op basis van de adviezen van de inlichtingen- en veiligheidsdiensten en van het Instituut, zullen de betrokken ministers moeten bepalen of de dienstenaanbieder op wie de MNO een beroep wil doen, aangeduid moet worden als een aanbieder die een hoog risico vormt. De beperkingen die toepasselijk zijn in het koninklijk besluit zullen enkel gelden voor het beroep dat een MNO doet op dienstenaanbieders die een hoog risico vormen.

La présente loi vise les réseaux mobiles de cinquième génération (5G). Afin de répondre à l'avis du Conseil d'État, une définition de la 5G a été introduite dans la présente loi. Cette définition fait référence à la recommandation ITU-R M.2150 de l'Union internationale de télécommunication (ci-après "la recommandation UIT-R"). Une première version de cette recommandation a été publiée en février 2021 et est disponible à l'adresse suivante: *https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-0-202102-I*!!PDF-E.pdf. Il convient de souligner que la définition de réseau 5G n'exige pas que le réseau d'accès radioélectrique soit 100 % conforme à chaque élément de cette recommandation. Cependant, en pratique, un équipementier soit suit l'ensemble des éléments obligatoires d'un standard, soit il ne le suit pas.

L'alinéa 5 du paragraphe 1er exclut du champ d'application de l'article 105 les éléments suivants.

Sont exclus les éléments passifs du réseau, qui sont par exemple des antennes passives, des prismes ou des filtres. Ils sont exclus étant donné que le risque en termes de sécurité pour ces éléments est très faible. En effet, ils ne sont pas programmables et donc leur fonctionnement est connu d'avance.

Sont également exclus les points de terminaison, pour autant qu'ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications. Pour rappel, la notion de "point de terminaison du réseau" est définie à l'article 2, 16°, de la loi du 13 juin 2005 relative aux communications électroniques.

Enfin, sont exclus les éléments de réseaux mobiles de quatrième génération et des générations antérieures, pour autant qu'ils ne soient pas nécessaires à la fourniture de réseaux 5G. En revanche, les éléments de ces réseaux qui sont nécessaires à la fourniture de réseaux 5G tombent sous le régime de l'autorisation préalable. Concrètement, si un réseau mobile utilise une technologie radio 5G, il doit être considéré comme un réseau 5G, même si certaines parties de ce réseau (par exemple le réseau cœur) ressortent encore de la quatrième génération des réseaux mobiles. A cet égard, la recommandation UIT-R M.2150 de l'Union internationale des télécommunications identifie trois interfaces radios dont une qui est basée sur l'utilisation d'un réseau 4G/LTE. L'autorisation préalable couvre cette interface radio et tous les éléments nécessaires à sa mise en œuvre.

De onderhavige wet doelt op de mobiele netwerken van de vijfde generatie (5G). Om aan het advies van de Raad van State te beantwoorden is in de onderhavige wet een definitie van 5G ingevoerd. Die definitie verwijst naar de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie (verder "de ITU-R-aanbeveling"). Een eerste versie van deze aanbeveling is gepubliceerd in februari 2021 en is beschikbaar op het volgende adres: *https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-0-202102-I*!!PDF-E.pdf. Er dient te worden benadrukt dat de definitie van 5G-netwerk niet vereist dat het radiotoegangsnetwerk voor 100 % voldoet aan elk element van deze aanbeveling. In de praktijk is het echter zo dat een producent van netwerkelementen ofwel alle verplichte elementen van een norm volgt, ofwel deze niet volgt.

Het vijfde lid van paragraaf 1 sluit de volgende elementen uit van het toepassingsgebied van artikel 105.

Uitgesloten worden de passieve elementen van het netwerk, zoals passieve antennes, prisma's of filters. Zij worden uitgesloten omdat het risico in termen van veiligheid voor deze elementen erg klein is. Ze zijn immers niet programmeerbaar en dus is de werking ervan vooraf bekend.

Ook uitgesloten zijn de netwerkaansluitpunten, voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie. Ter herinnering, het begrip "netwerkaansluitpunt" is gedefinieerd in artikel 2, 16°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Ten slotte zijn uitgesloten de elementen van mobiele netwerken van de vierde generatie en van de vorige generaties, voor zover ze niet nodig zijn voor de verstrekking van 5G-netwerken. De elementen van die netwerken die nodig zijn voor de verstrekking van 5G-netwerken vallen daarentegen wel onder het stelsel van de voorafgaande machtiging. Concreet, wanneer een mobiel netwerk gebruikmaakt van een 5G-radiotechnologie, moet het als een 5G-netwerk worden beschouwd, zelfs wanneer bepaalde delen van dat netwerk (bijvoorbeeld het corenetwerk) nog deel uitmaken van de vierde generatie van mobiele netwerken. In dat opzicht identificeert de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie drie radio-interfaces waaronder een die gebaseerd is op het gebruik van een 4G/LTE-netwerk. De voorafgaande machtiging slaat op deze radio-interface en op alle elementen die nodig zijn voor de toepassing ervan.

Les réseaux mobiles de quatrième génération et des générations antérieures sont exclus étant donné que le risque en termes de sécurité est moins élevé que celui qui naîtra avec la 5G. En effet, comme il a été expliqué ci-dessus, avec la 5G, la société deviendra de plus en plus dépendante des réseaux mobiles de communications électroniques.

Les technologies de 2e, 3e ou 4e génération sont respectivement la technologie GSM, la technologie UMTS et les technologies LTE conformément aux normes publiées par l'ETSI. Ne sont également pas visés par l'avant-projet de loi les réseaux TETRA (*Terrestrial Trunked Radio*) et les réseaux reposant sur le standard de transmission sans fil IEEE 802.11 (Wi-Fi).

L'alinéa 6 du paragraphe 1er s'explique comme suit. Le système que l'avant-projet de loi entend mettre en place est un système d'autorisation préalable. Cependant, en pratique, certains opérateurs auront déjà commencé à utiliser des dispositifs matériels ou des logiciels d'équipementier pour développer un réseau 5G, et auront déjà recours aux fournisseurs de services au moment de l'entrée en vigueur de l'arrêté royal qui exécutera l'article 105 de la loi du 13 juin 2005. Pour ces opérateurs, l'autorisation ne sera par définition pas préalable mais consistera en une autorisation de régularisation (sur base d'une demande de régularisation).

Dans le cas où l'arrêté royal qui fixe les restrictions pour l'utilisation d'éléments de réseau fournis par les équipementiers et l'arrêté royal qui fixe les restrictions pour le recours aux fournisseurs de services ne sont pas adoptés au même moment, la demande de régularisation concernant les éléments de réseau et la demande de régularisation concernant le recours aux fournisseurs de services peuvent être introduites à des moments différents.

Paragraphe 2

En fonction de positions futures du Conseil national de sécurité et en plus de l'extension du recours aux fournisseurs de services (cf. *supra*), le champ d'application de l'article 105 pourrait être étendu comme expliqué ci-après.

Premièrement, le Roi pourrait étendre l'obligation visée au paragraphe 1er d'obtenir les autorisations visées à ce paragraphe à une ou plusieurs catégories d'opérateurs de réseaux mobiles virtuels mobiles (en anglais *Mobile Virtual Network Operator* ou MVNO). En effet, cette extension n'a pas beaucoup de sens pour les catégories

De mobiele netwerken van de vierde en vroegere generaties worden uitgesloten aangezien het veiligheidsrisico niet zo hoog is als het risico dat door 5G zal ontstaan. Zoals immers hierboven is uitgelegd, zal de maatschappij met 5G meer en meer afhankelijk zijn van de mobiele elektronische-communicatienetwerken.

De technologieën van de 2e, 3e of 4e generatie zijn respectievelijk de gsm-technologie, de UMTS-technologie en de technologieën LTE overeenkomstig de door het ETSI gepubliceerde normen. Evenmin beoogd door het voorontwerp van wet zijn de TETRA-netwerken (*Terrestrial Trunked Radio*) en de netwerken die berusten op de norm voor draadloze transmissie IEEE 802.11 (wifi).

Het zesde lid van paragraaf 1 wordt als volgt verklaard. Het systeem dat het voorontwerp van wet wil invoeren is een systeem van voorafgaande machtiging. In de praktijk zullen bepaalde operatoren echter al begonnen zijn met het gebruik van hard- of software van producenten van netwerkelementen om een 5G-netwerk te ontwikkelen en zullen zij reeds een beroep doen op dienstenaanbieders op het ogenblik van inwerkingtreding van het koninklijk besluit dat artikel 105 van de wet van 13 juni 2005 ten uitvoer zal leggen. Voor die operatoren zal de machtiging per definitie niet voorafgaand zijn, maar bestaan uit een machtiging tot regularisatie (op basis van een verzoek om regularisatie).

Ingeval het koninklijk besluit dat de beperkingen vaststelt voor het gebruik van netwerkelementen die worden geleverd door producenten van netwerkelementen en het koninklijk besluit dat de beperkingen vaststelt voor het beroep op dienstenaanbieders niet op hetzelfde moment worden aangenomen, mogen het verzoek om regularisatie betreffende de netwerkelementen en het verzoek om regularisatie betreffende het beroep op de dienstenaanbieders op een verschillend moment worden ingediend.

Paragraaf 2

Afhankelijk van de toekomstige standpunten van de Nationale Veiligheidsraad en bovendien van de uitbreiding van het beroep op de dienstenaanbieders (zie hierboven) zou het toepassingsgebied van artikel 105 kunnen worden uitgebreid zoals hierna wordt uitgelegd.

Ten eerste zou de Koning de in paragraaf 1 bedoelde verplichting om de in deze paragraaf bedoelde machtigingen te krijgen kunnen uitbreiden naar een of meer categorieën van virtuele mobiel-netwerkoperatoren (in het Engels *Mobile Virtual Network Operators* of MVNO). Die uitbreiding heeft immers niet veel zin voor

de MVNO qui ne disposent pas ou très peu d'éléments d'infrastructure. Il s'agit de trois types d'autorisations, à savoir l'autorisation préalable concernant les éléments du réseau 5G (paragraphe 1er, alinéa 1er), l'autorisation préalable pour bénéficier des services de fournisseurs (paragraphe 1er, alinéa 2), ainsi que l'autorisation à la suite d'une demande de régularisation (paragraphe 1er, alinéa 6). Il va de soi que ces autorisations doivent se comprendre dans le cadre du champ d'application du paragraphe 1er et sont donc limitées à un réseau 5G.

Deuxièmement, le Roi pourrait étendre l'obligation visée au paragraphe 1er d'obtenir les autorisations visées à ce paragraphe à certaines entreprises qui déploient un réseau 5G privé. Il s'agit:

— d'ASTRID (pour autant qu'elle déploie un tel réseau);

— des fournisseurs qui seraient exploitants d'infrastructures critiques au sens de la loi "infrastructures critiques" ou opérateurs de services essentiels au sens de la loi NIS (loi du 7 avril 2019);

— d'autres fournisseurs de réseaux privés qui sont désignés par une autorité que le Roi charge de cette tâche.

Il est à noter que dans son avis, le Conseil d'État demande de définir les réseaux privés mobiles. Ceci n'a pas été fait, dès lors que l'article 105 n'utilise plus cette notion. L'article 105, § 2, 2°, fait référence aux réseaux privés et ces derniers n'entrent dans le champ d'application de la loi que pour autant qu'il s'agisse de réseaux 5G. Or, la loi définit dorénavant les réseaux 5G. Un réseau privé est un réseau autre qu'un réseau public. Un réseau public de communications électroniques est défini à l'article 2, 10°, de la loi du 13 juin 2005 relative aux communications électroniques.

Enfin, le paragraphe 2, 4° précise également que le Roi peut préciser les hypothèses dans lesquelles une autorisation est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau.

Dans son avis, le Conseil d'État propose de viser à l'article 105, § 2, 5°, un "dispositif matériel d'un système informatique constituant un élément de réseau" à la place d'un dispositif matériel relatif à un élément de réseau. Cette suggestion n'est pas suivie car un réseau de communications électroniques se distingue d'un système informatique. Les dispositifs logiciels

de categorieën van MVNO's die over heel weinig of geen infrastructuurelementen beschikken. Het gaat om drie soorten van machtigingen, namelijk de voorafgaande machtiging betreffende de 5G-netwerkelementen (paragraaf 1, eerste lid), de voorafgaande machtiging om de diensten van aanbieders te genieten (paragraaf 1, tweede lid), alsook de machtiging volgend op een verzoek om regularisatie (paragraaf 1, zesde lid). Het spreekt vanzelf dat deze machtigingen moeten worden opgevat binnen het kader van het toepassingsgebied van paragraaf 1 en dus beperkt zijn tot een 5G-netwerk.

Ten tweede zou de Koning de in paragraaf 1 bedoelde verplichting om de in deze paragraaf bedoelde machtigingen te krijgen kunnen uitbreiden naar bepaalde ondernemingen die een privaat 5G-netwerk uitrollen. Het gaat om:

— ASTRID (voor zover deze zo'n netwerk uitrolt);

— de aanbieders die exploitant van kritieke infrastructuren zouden zijn in de zin van de wet "kritieke infrastructuren" of operatoren van essentiële diensten in de zin van de NIS-wet (wet van 7 april 2019);

— andere aanbieders van private netwerken die worden aangewezen door een overheid die door de Koning met deze taak is belast.

Er moet worden opgemerkt dat de Raad van State in zijn advies vraagt om een definitie te geven van private mobiele netwerken. Dat is niet gebeurd, omdat artikel 105 dat begrip niet meer gebruikt. Artikel 105, § 2, 2°, verwijst naar de private netwerken en die laatste vallen maar in het toepassingsgebied van de wet voor zover het om 5G-netwerken gaat. Welnu, de wet bevat voortaan een definitie van de 5G-netwerken. Een privaat netwerk is een netwerk dat geen openbaar netwerk is. Een openbaar elektronische-communicatienetwerk wordt gedefinieerd in artikel 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Ten slotte, preciseert paragraaf 2, 4° ook dat de Koning de hypothesen mag preciseren waarin een machtiging noodzakelijk is in geval van een update van de software of hardware van het netwerk.

In zijn advies stelt de Raad van State voor om in de Franse versie in artikel 105, § 2, 5°, te verwijzen naar een "dispositif matériel d'un système informatique constituant un élément de réseau" in plaats van een "dispositif matériel relatif à un élément de réseau". Deze suggestie is niet gevolgd omdat een elektronische-communicatienetwerk zich onderscheidt van een computersysteem. Ook in de

et matériels renvoient aux notions de hardware et de software employés également dans la version néerlandaise de cette disposition.

Paragraphe 3

En pratique, une autorisation ne doit pas être demandée pour chaque élément actif du réseau, mais un dossier peut être introduit pour l'ensemble ou une partie des éléments du réseau.

Le dossier est introduit par l'entreprise délivrant pour elle-même ou pour une tierce partie des services mobiles auprès de l'Institut, selon les modalités que l'Institut fixe sur son site internet.

Dans son avis, le Conseil d'État se demande si une seule demande doit être introduite, et si oui, auprès de quel ministre. Vu que la décision est prise de manière conjointe par les différents ministres, une demande pour l'ensemble des ministres suffit (et non une demande par ministre). Cette demande sera introduite auprès de l'Institut.

Il revient à un MNO de déterminer s'il souhaite introduire une demande pour l'utilisation d'un élément de son réseau 5G et une demande séparée pour le recours à des fournisseurs de services ou une seule demande pour les deux.

Dans son avis, le Conseil d'État se demande également si chacun des ministres doit traiter de manière individuelle le dossier et demander l'avis de l'Institut et des services de renseignement et de sécurité. Ces questions seront réglées dans l'arrêté royal d'exécution de la loi.

Les ministres concernés, l'Institut et les services de renseignement et de sécurité pourront demander des informations ou des documents complémentaires au demandeur ou à toute personne physique ou morale pouvant contribuer utilement à leur information.

Paragraphe 4

Tout d'abord, il est à noter que ce paragraphe a subi plusieurs révisions afin de tenir compte de l'avis du Conseil d'État. Les ministres concernés examineront la demande d'autorisation préalable ou de régularisation qui leur est soumise ou reverront d'initiative leur décision lorsqu'un nouvel élément de nature à remettre en cause cette décision le justifiera. Une révision de la décision

Nederlandstalige versie van deze bepaling is er sprake van hardware en software.

Paragraaf 3

In de praktijk hoeft een machtiging niet te worden aangevraagd voor elk actief element van het netwerk, maar er kan wel een dossier worden ingediend voor alle of een deel van de elementen van het netwerk.

Het dossier moet door de onderneming die voor zichzelf of voor een derde partij mobiele diensten levert, worden ingediend bij het Instituut volgens de werkwijze die het Instituut vaststelt op zijn website.

In zijn advies vraagt de Raad van State zich af of slechts één verzoek moet worden ingediend en zo ja, bij welke minister. Aangezien de beslissing gemeenschappelijk wordt genomen door de verschillende ministers volstaat één verzoek voor alle ministers (dus geen verzoek per minister). Dat verzoek zal worden ingediend bij het Instituut.

Het komt aan een MNO toe om te bepalen of hij een verzoek wenst in te dienen voor het gebruik van een element van zijn 5G-netwerk en een apart verzoek voor het beroep op dienstenaanbieders, dan wel één verzoek voor allebei.

In zijn advies vraagt de Raad van State zich eveneens af of elk van de ministers afzonderlijk het dossier moet behandelen en het advies moet aanvragen van het Instituut en van de inlichtingen- en veiligheidsdiensten. Deze kwesties zullen worden geregeld in het koninklijk besluit ter uitvoering van de wet.

De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten zullen informatie of aanvullende documenten kunnen vragen aan de verzoeker of aan iedere natuurlijke of rechtspersoon die op nuttige wijze kan bijdragen tot hun informatie.

Paragraaf 4

Allereerst moet worden opgemerkt dat deze paragraaf al meermaals is herzien om rekening te houden met het advies van de Raad van State. De betrokken ministers zullen het verzoek om voorafgaande machtiging of regularisatie dat hun wordt voorgelegd onderzoeken, of zullen op eigen initiatief hun beslissing herzien wanneer dat wordt gerechtvaardigd door een nieuw element dat

sera justifiée lorsqu'un élément non connu lors de la prise de décision aurait mené à une décision différente.

Parmi les nouveaux éléments justifiant une révision figurent par exemple une modification des zones sensibles, une plus grande possibilité d'ingérence faisant que le profil de risque du fournisseur doit être réévalué, une diminution ou perte de capacité du fournisseur à garantir l'approvisionnement.

Les ministres concernés mettront en œuvre dans leur décision l'arrêté royal exécutant l'article 105, paragraphe 4, alinéa 1er.

Cette disposition permet au Roi de restreindre le recours aux fournisseurs à haut risque en fonction de la partie du réseau et en tenant compte de zones sensibles.

Les fournisseurs dont il est question dans l'alinéa 1er sont les équipementiers et les fournisseurs de services. Un équipementier est considéré comme un type de fournisseur de l'opérateur. En effet, les éléments de réseau développés par l'équipementier sont fournis à l'opérateur, afin de lui permettre de construire et d'exploiter son réseau de communications électroniques. Les fournisseurs de services comprennent les fournisseurs de services gérés (en anglais "*managed services providers*") et les partenaires de soutien (en anglais "*supporting partners*").

En pratique, la tâche du partenaire de soutien est prise en charge par l'équipementier, l'opérateur lui-même, le groupe dont il fait partie, un fournisseur de services gérés ou une autre entreprise. Un équipementier peut être le fournisseur de services gérés.

De telles restrictions sont nécessaires dès lors que les autres mesures de sécurité qui pourraient être imposées ne sont pas suffisantes pour réduire suffisamment les risques en jeu.

Ce paragraphe reprend les critères pour définir un fournisseur à haut risque tels que décrits dans le paragraphe 2.37 de l'évaluation coordonnée des risques au niveau de l'UE par le groupe de coopération NIS (cf. *supra*). Pour satisfaire aux remarques du Conseil d'État, des explications sont données sur la portée du concept d'ingérence et la liste non exhaustive de facteurs pouvant indiquer une possibilité d'ingérence.

hun beslissing ter discussie stelt. Een herziening van het besluit is gerechtvaardigd wanneer iets dat niet bekend was op het tijdstip waarop het besluit werd genomen, tot een ander besluit zou hebben geleid.

Nieuwe elementen die een herziening rechtvaardigen, zijn bijvoorbeeld een verandering van de gevoelige zones, een gegroeide kans op inmenging waardoor het risicoprofiel van de leverancier moet worden geherevalueerd, een vermindering of verlies van vermogen van de leverancier om bevoorrading te garanderen.

De betrokken ministers zullen in hun beslissing het koninklijk besluit ter uitvoering van artikel 105, paragraaf 4, eerste lid ten uitvoer brengen.

Op basis van deze bepaling kan de Koning het beroep op leveranciers met een hoog risicoprofiel beperken op grond van het deel van het netwerk en rekening houdende met gevoelige zones.

De leveranciers waarvan sprake in het eerste lid, zijn de producenten van netwerkelementen en de dienstenaanbieders. Een producent van netwerkelementen wordt beschouwd als een soort van leverancier van de operator. De netwerkelementen die door de producent van netwerkelementen worden ontwikkeld, worden immers geleverd aan de operator, opdat deze zijn elektronischecommunicatienetwerk kan opbouwen en exploiteren. De dienstenaanbieders omvatten de aanbieders van beheerde diensten (in het Engels "*managed services providers*") en de ondersteunende partners (in het Engels "*supporting partners*").

In de praktijk wordt de taak van ondersteunende partner op zich genomen door de producent van netwerkelementen, de operator zelf, de groep waarvan hij deel uitmaakt, een aanbieder van beheerde diensten of een andere onderneming. Een producent van netwerkelementen kan de aanbieder van beheerde diensten zijn.

Dergelijke beperkingen zijn noodzakelijk omdat de overige veiligheidsmaatregelen die opgelegd zouden kunnen worden, niet voldoende zijn om de risico's voldoende te beperken.

Deze paragraaf neemt de criteria over om leverancier die een hoog risico vormt te definiëren, zoals die beschreven zijn in paragraaf 2.37 van de gecoördineerde risicobeoordeling op EU-niveau door de NIS-samenwerkingsgroep (cf. *supra*). Om tegemoet te komen aan de opmerkingen van de Raad van State wordt toelichting verschaft over de draagwijdte van het begrip inmenging en de niet exhaustieve lijst van factoren die op een kans op inmenging kunnen wijzen.

Le terme “ingérence” doit s’entendre au sens le plus large et pas uniquement au sens de l’article 8, 1°, g, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. En effet, la possibilité d’ingérence ou de facilitation de celle-ci ne se limite pas aux tentatives d’influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins. Ainsi, l’ingérence (ou sa possibilité) visée porte sur toutes les mesures, les atteintes ou les interventions (ou leur possibilité) du pays concerné à l’encontre de la souveraineté interne et externe de l’État belge, en ce compris les atteintes aux intérêts à préserver dont il est question à l’article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Cette souveraineté comprend notamment le droit de l’État belge de choisir librement son système politique, économique, social et culturel ainsi que de choisir sa politique étrangère. Ce principe de souveraineté est d’ailleurs repris dans les résolutions 2625 (1970) et 2131 (1965) de l’Assemblée générale des Nations Unies. La possibilité d’ingérence inclut également *a fortiori* le risque de violations du droit international comme le principe de non-intervention et l’interdiction de recourir à la menace ou à l’emploi de la force, comme défini dans la Charte des Nations Unies.

En outre, l’ingérence visée (y compris les formes possibles d’espionnage) n’est pas limitée aux actes éventuels du pays d’implantation, mais comprend également l’ingérence par des pays tiers ou par le biais de l’utilisation d’acteurs non étatiques. Les facteurs visés à l’alinéa 3, 1°, et qui ont été repris de l’évaluation coordonnée des risques au niveau de l’UE, ne sont ni cumulatifs ni limitatifs. La présence d’un seul facteur peut déjà indiquer une possibilité d’ingérence.

Un premier facteur renvoie au lien ou à l’interaction entre l’entreprise et les services publics du pays en question qui est de nature à créer une possibilité d’ingérence. Ainsi, un contrôle formel ou informel, direct ou indirect du gouvernement ou des services publics (y compris les autorités militaires) sera pris en considération lors de l’analyse de la possibilité d’ingérence.

Le deuxième facteur indique les risques inhérents au système politique au sein duquel le fournisseur opère, notamment concernant le niveau de protection juridique, les principes de l’État de droit, les droits de l’homme, la protection de la propriété intellectuelle et les secrets de fabrication, etc. Il ne s’agit pas uniquement de la situation de jure, mais aussi de la manière dont on

Het begrip “inmenging” dient gelezen te worden in de ruimst mogelijke betekenis en niet louter in de zin van artikel 8, 1°, g, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. De kans op inmenging of op de facilitering van de inmenging is immers niet beperkt tot de pogingen om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden. Aldus slaat de bedoelde (kans op) inmenging op alle (kansen op) maatregelen, aantastingen of ingrepen van het desbetreffende land tegen de interne en externe soevereiniteit van de Belgische staat, met inbegrip van aantastingen van de te vrijwaren belangen waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Deze soevereiniteit bestaat onder meer uit het recht voor de Belgische staat om vrij haar eigen politiek, economisch, sociaal en cultureel systeem te kiezen alsook de eigen keuze omtrent haar buitenlands beleid. Dit soevereiniteitsbeginsel wordt trouwens hernomen in de resoluties 2625 (1970) en 2131 (1965) van de Algemene Vergadering van de Verenigde Naties. De kans op inmenging omvat *a fortiori* ook de kans op schendingen van het internationaal recht, zoals het beginsel van non-interventie en het verbod op het gebruik van of het dreigen met geweld zoals bepaald in het Charter van de Verenigde Naties.

Daarnaast is de bedoelde inmenging (met inbegrip van alle mogelijke vormen van spionage) niet beperkt tot de mogelijke handelingen van het land van vestiging zelf, maar omvat deze ook inmenging door derde landen of via het gebruik van niet-statelijke actoren. De factoren, bedoeld in het derde lid, 1° en die overgenomen werden uit de gecoördineerde risicobeoordeling op EU-niveau, zijn niet-cumulatief en niet-limitatief. De aanwezigheid van slechts één factor kan reeds wijzen op de kans op inmenging.

De eerste factor verwijst naar de band of verwevenheid tussen de onderneming en de overheidsdiensten van het desbetreffende land die van dien aard is om een kans op inmenging te creëren. Zo zal een formele of informele, directe of indirecte controle van de regering of overheidsdiensten (met inbegrip van de militaire overheden) bij de analyse van de kans op inmenging in overweging genomen worden.

De tweede factor duidt op de risico’s inherent aan het staatkundig systeem waarin de leverancier zich bevindt, onder andere aangaande de mate van rechtsbescherming, de principes van de rechtstaat, de mensenrechten, de bescherming van de intellectuele eigendom en fabrieksgeheimen, etc. Het betreft niet enkel de ‘de iure’ situatie, maar ook hoe ‘*de facto*’ invulling gegeven

interprète *de facto* le système politique ou la protection des données et juridique.

Les caractéristiques de la propriété renvoient à l'organisation, à la transparence, aux structures de gestion, à l'actionnariat et au modèle de financement de l'entreprise. En outre, un contrôle de l'entreprise du fournisseur par une autre entreprise, qui est elle-même sujette à une possibilité d'ingérence, constituera également un facteur d'évaluation.

Le quatrième facteur indique la possibilité d'un pays d'exercer des pressions sur ou d'imposer des obligations à l'entreprise, de façon formelle ou informelle, pour qu'elle agisse de manière non conforme à la sécurité nationale ou à l'ordre public d'autres pays. Cela inclut également la possibilité d'imposer à l'entreprise de collaborer à des activités d'ingérence, d'espionnage ou de sabotage (indépendamment de leur licéité dans le pays d'origine) ou d'intervenir dans la liberté d'établissement de l'entreprise.

Le seul facteur ajouté aux critères concerne la conduite de ou l'implication dans une cyberpolitique offensive dans le pays dont un fournisseur est originaire. Pour un pays avec une cyberpolitique offensive, posséder ou contrôler une entreprise fournissant des éléments de réseau représente un atout majeur pour faciliter les activités de cybersécurité offensives. Au lieu de devoir hacker des cibles d'espionnage ou d'intrusion afin d'obtenir certaines informations, le pays peut recourir à son contrôle sur le fournisseur pour, par exemple via une porte dérobée ("*backdoor*") prévue au préalable dans le matériel du réseau, obtenir l'accès souhaité. En cas de conflits importants, le pays en question pourrait également utiliser cette emprise sur le fournisseur pour déconnecter (partiellement) le réseau ou perturber certains processus (par exemple des véhicules autonomes) dépendant du bon fonctionnement du réseau de télécommunications. La cyberpolitique ne renvoie donc pas uniquement aux activités du passé, mais également à la capacité et à la volonté d'un pays de déployer des cyberactivités susceptibles de menacer la sécurité nationale, la sécurité de l'information ou l'ordre public d'un pays.

D'autres facteurs non précisés qui ont une influence sur les intérêts à préserver visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité peuvent également entrer en ligne de compte lors de l'évaluation du profil de risque du fournisseur.

Il est noté qu'à l'instar du paragraphe 2.37 de l'évaluation coordonnée des risques au niveau de l'UE par le

wordt aan het staatkundig systeem of de gegevens- en rechtsbescherming.

De karakteristieken van eigendom verwijzen naar de organisatie, transparantie, beleidsstructuren, het aandeelhouderschap en financieringsmodel van de onderneming. Daarnaast zal een controle op de onderneming van de leverancier door een andere onderneming, die zelf een kans op inmenging ondervindt, ook een factor voor beoordeling vormen.

De vierde factor duidt op de mogelijkheid van een land om, op formele of informele wijze, druk uit te oefenen of verplichtingen op te leggen aan de onderneming om te handelen in strijd met de nationale veiligheid of openbare orde van andere landen. Dit omvat tevens de mogelijkheid om de onderneming op te leggen om mee te werken aan activiteiten van inmenging, spionage of sabotage (onafhankelijk van de rechtmatigheid ervan in het land van herkomst) of om tussen te komen in de vrijheid van vestiging van de onderneming.

De enige factor die aan de criteria is toegevoegd, betreft het voeren van of de betrokkenheid bij een offensief cyberbeleid in het land waarvan een leverancier afkomstig is. Voor een land met een offensief cyberbeleid is het beschikken over, of een greep hebben op, een onderneming die netwerkelementen levert een grote troef om de offensieve cyberactiviteiten te faciliteren. In plaats van de spionage- of inbraakdoelwitten te moeten hacken teneinde aan bepaalde informatie te komen, kan het land zijn greep op de leverancier gebruiken om, bijvoorbeeld via een vooraf ingebouwde achterdeur ("*backdoor*") in het netwerkmateriaal, de gewenste toegang te verkrijgen. In geval van grote conflicten, zou het land in kwestie zijn greep op de leverancier ook kunnen aanwenden om (delen van) het netwerk uit te schakelen, of om bepaalde processen (bijvoorbeeld zelfrijdende voertuigen) die afhankelijk zijn van de goede werking van het telecommunicatienetwerk te verstoren. Het cyberbeleid verwijst aldus niet enkel naar de activiteiten uit het verleden, maar ook naar de capaciteit en bereidheid van een land om cyberactiviteiten te ontplooien die een bedreiging kunnen vormen voor de nationale veiligheid, informatieveiligheid of de openbare orde van een land.

Bovendien kunnen ook andere, niet nader bepaalde factoren die een invloed hebben op de te vrijwaren belangen bedoeld in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, mee in rekening worden genomen bij de beoordeling van het risicoprofiel van de leverancier.

Er wordt opgemerkt dat, naar analogie van paragraaf 2.37 van de gecoördineerde evaluatie van

groupe de coopération NIS (groupe qui est instauré par la directive NIS, voir *supra*), le paragraphe 4, alinéa 4, 1°, de l'article 105 de la présente loi concerne l'ingérence d'un pays tiers à l'Union européenne ("UE") et non l'ingérence d'un pays tiers à la Belgique. Il convient de rappeler que ce document constitue une approche coordonnée entre les États membres et que le choix a été fait de ne pas dévier de cette approche sur ce point.

Il convient également de noter que l'Union européenne s'est dotée de nombreuses normes visant à assurer un socle minimum commun de protection des citoyens, tels que le Traité sur le fonctionnement de l'Union européenne, la Charte fondamentale des droits de l'Union européenne, le RGPD (règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), la directive vie privée et communications électroniques (directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques), le code des communications électroniques européen (directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen), la directive NIS (directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union) et le règlement sur la cybersécurité (Règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications). Ce socle commun propre au fonctionnement de l'Union européenne permet de distinguer les États membres de l'Union européenne des pays tiers en matière de sécurité des réseaux et des données en ce compris les données à caractère personnel.

En outre, comme indiqué *supra* le présent projet fait suite à la "*Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*" dont le but ultime est de créer un cadre commun aux États membres, solide et objectif de mesures de sécurité qui garantira un niveau adéquat de cybersécurité des réseaux 5G dans toute l'UE.

Ce sont les ministres concernés qui évalueront, lors de l'examen de la demande, le profil de risque du fournisseur,

de risico's op het niveau van de EU door de NIS-samenwerkingsgroep (groep die is opgericht krachtens de NIS-richtlijn, zie hierboven), paragraaf 4, vierde lid, 1°, van artikel 105 van deze wet, betrekking heeft op de inmenging van een land dat niet tot de Europese Unie ("EU") behoort en niet de inmenging van een ander land dan België. Er dient te worden opgemerkt dat dit document het voorwerp uitmaakt van een gecoördineerde aanpak vanwege de lidstaten en dat ervoor werd geopteerd om niet af te wijken van die aanpak voor dit punt.

Er dient eveneens te worden opgemerkt dat de Europese Unie zich heeft voorzien van tal van normen bedoeld om te zorgen voor een gemeenschappelijke minimale basis voor bescherming van de burgers, zoals het Verdrag betreffende de werking van de Europese Unie, het Handvest van de grondrechten van de Europese Unie, de GDPR (EU-verordening 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens), de richtlijn persoonlijke levenssfeer en elektronische communicatie (Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie), het Europees wetboek voor elektronische communicatie (Richtlijn (EU) 2018/1972 van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie), de NIS-richtlijn (Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie) en de cyberbeveiligingsverordening (Verordening (EU) 2019/881 van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie). Aan de hand van deze gemeenschappelijke basis eigen aan de werking van de Europese Unie kunnen de lidstaten van de Europese Unie onderscheiden worden van de derde landen op het gebied van veiligheid van netwerken en gegevens, persoonsgegevens inbegrepen.

Zoals overigens hierboven aangegeven, geeft dit ontwerp gevolg aan de "*Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*" waarvan het ultieme doel erin bestaat een degelijk en objectief gemeenschappelijk kader van beveiligingsmaatregelen te creëren voor de lidstaten dat een gepast niveau van cyberbeveiliging van de 5G-netwerken zal garanderen in de ganse EU.

Het zijn de betrokken ministers die tijdens het onderzoek van het verzoek het risicoprofiel van de leverancier

sur base d'un avis des services de renseignement et de sécurité et d'un avis de l'Institut. Selon l'article 2, § 1er, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les deux services de renseignement et de sécurité du Royaume sont la Sûreté de l'État, Service civil de Renseignement et de Sécurité, et le Service Général du Renseignement et de la Sécurité, Service militaire de Renseignement et de Sécurité.

Les avis des services de renseignement et de sécurité peuvent être classifiés conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Il importe de souligner que l'avis des services de renseignement de sécurité et l'avis de l'Institut ne sont pas contraignants pour les ministres. Comme l'avis de l'IBPT est rendu dans le cadre d'un dossier individuel, il ne présente en principe pas de caractère d'utilité publique.

Une zone sensible est une zone déterminée par le Roi, sur base d'un avis du Conseil national de sécurité. La zone est déterminée en tenant compte de la sensibilité des sites qui s'y trouvent. Un site peut être considéré comme sensible lorsqu'il est lié à l'un des intérêts énumérés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité dans cette zone.

Lorsque les ministres concernés revoient leur décision d'initiative, ils fixent un délai pour la mise en œuvre de la nouvelle décision qui est postérieur aux délais prévus dans l'arrêté royal, et ce afin de donner à l'opérateur le temps nécessaire pour s'adapter.

Dans tous les cas, le délai pour la mise en œuvre de la décision doit être d'une durée d'au moins de 5 ans à compter de sa notification. Ce délai minimum de cinq ans est prévu afin de garantir au marché une certaine stabilité. Les critères à prendre en compte pour fixer ce délai sont notamment les critères suivants: le cycle de vie normal d'un équipement, le temps normal pour migrer d'un fournisseur vers un autre et la durée des contrats.

Paragraphe 5

Une décision des ministres concernés par laquelle ces derniers revoient une décision antérieure, assortissent de conditions l'autorisation ou refusent cette autorisation

zullen evalueren op basis van een advies van de inlichtingen- en veiligheidsdiensten en van een advies van het Instituut. Volgens artikel 2, § 1, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, zijn de twee inlichtingen- en veiligheidsdiensten van het Koninkrijk de Veiligheid van de Staat, burgerlijke inlichting- en veiligheidsdienst en de Algemene Dienst inlichting en veiligheid van de Krijgsmacht, militaire inlichting- en veiligheidsdienst.

De adviezen van de inlichtingen- en veiligheidsdiensten kunnen geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Het is belangrijk om te onderstrepen dat het advies van de inlichtingen- en veiligheidsdiensten en het advies van het Instituut niet bindend zijn voor de ministers. Aangezien het advies van het BIPT wordt verstrekt in het kader van een individueel dossier, heeft het in principe geen openbaar nut.

Een gevoelige zone is een gebied dat wordt bepaald door de Koning, op basis van een advies van de Nationale Veiligheidsraad. De zone wordt aangeduid rekening houdend met de gevoeligheid van de sites die er zich bevinden. Een site kan als gevoelig worden beschouwd wanneer deze verband houdt met één van de belangen opgesomd in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Wanneer de betrokken ministers op eigen initiatief hun beslissing herzien, leggen ze een termijn vast voor de uitvoering van de nieuwe beslissing die later komt dan de termijnen waarin het koninklijk besluit voorziet, en dit om de operator de nodige tijd te geven om zich aan te passen.

In elk geval moet de termijn voor de tenuitvoerbrenging van het besluit ten minste 5 jaar bedragen, te rekenen vanaf de kennisgeving ervan. Deze minimumtermijn van vijf jaar is zo bepaald om aan de markt een zekere stabiliteit te garanderen. De in acht te nemen criteria om deze termijn vast te leggen, zijn met name: de normale levenscyclus van een toestel, de normale tijd om van de ene leverancier naar de andere over te stappen en de duur van de contracten.

Paragraaf 5

Een beslissing van de betrokken ministers waarmee ze een vroegere beslissing herzien, voorwaarden aan de machtiging koppelen of deze machtiging weigeren,

peut avoir des conséquences négatives importantes pour le demandeur. Par conséquent, le paragraphe 5 prévoit une procédure de consultation de ce dernier, avant que la décision finale ne soit prise.

Dans son avis, le Conseil d'État se demande quel est le point de départ du délai de 28 jours laissé au demandeur pour formuler des observations écrites lorsque les ministres entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision d'initiative. Ce point de départ est le jour où il est informé du projet de décision des ministres concernés. La loi ne désigne pas l'administration (par exemple l'Institut) ou le ministre (par exemple le ministre des télécoms) qui informera le demandeur de ce projet de décision, afin de permettre une flexibilité en pratique et une amélioration des procédures à l'aide de la pratique.

Paragraphe 6

L'alinéa 1er du paragraphe 6 reflète les nouvelles tâches de l'Institut en matière de gestion des demandes d'autorisation préalable ou de régularisation et de préparation de la décision des ministres. Cela ne signifie pas que ces tâches doivent exclusivement être effectuées par l'Institut. Par exemple, les services de renseignement et de sécurité pourraient également jouer un rôle important pour la préparation de la décision des ministres. Ces nouvelles tâches s'ajoutent aux tâches déjà prévues dans la présente loi, à savoir rendre un avis dans ces dossiers, contrôler le respect de la réglementation et de la décision des ministres et sanctionner le non-respect de ces règles.

Le délai dans lequel le projet de décision ou la décision d'approbation du dossier est communiqué au demandeur après l'introduction du dossier et le délai dans lequel la décision doit être prise après l'audition ou la réception des observations écrites seront fixés par arrêté royal, afin de permettre une adaptation de ces délais s'il apparait de la pratique que ces délais sont trop longs ou trop courts.

Il est à noter que lorsque les ministres revoient une décision antérieure (exemple retire une autorisation octroyée précédemment), il n'y a pas de délai pour envoyer au demandeur le projet de décision. Par contre, le délai fixé par le Roi est bien applicable pour prendre la décision après l'audition ou la réception des observations écrites.

kan voor de verzoeker aanzienlijke negatieve gevolgen hebben. Bijgevolg schrijft paragraaf 5 een raadplegingsprocedure van deze laatste voor, voordat de definitieve beslissing wordt genomen.

In zijn advies vraagt de Raad van State zich af wanneer de termijn van 28 dagen ingaat waarover de verzoeker beschikt om schriftelijke opmerkingen te formuleren wanneer de ministers van plan zijn de machtiging te weigeren, daaraan voorwaarden te koppelen of hun beslissing op eigen initiatief te herzien. Die termijn gaat in op de dag dat de verzoeker wordt ingelicht over de ontwerpbeslissing van de betrokken ministers. De wet wijst niet het bestuur (bijvoorbeeld het Instituut) noch de minister (bijvoorbeeld de minister voor Telecommunicatie) aan die de verzoeker zal inlichten over deze ontwerpbeslissing, met als doel enige flexibiliteit in de praktijk te bieden en de procedures te kunnen verbeteren op basis van de praktijk.

Paragraaf 6

Het eerste lid van paragraaf 6 geeft de nieuwe taken van het Instituut weer op vlak van het beheer van de verzoeken om voorafgaande machtiging of om regularisatie en van de voorbereiding van de beslissing van de ministers. Dit betekent niet dat deze taken uitsluitend door het Instituut moeten worden uitgevoerd. De inlichtingen- en veiligheidsdiensten zouden bijvoorbeeld eveneens een belangrijke rol kunnen spelen bij de voorbereiding van de beslissing van de ministers. Deze nieuwe taken komen bij de taken waarin de onderhavige wet reeds voorziet, namelijk in deze dossiers een advies verstrekken, de naleving van de reglementering en van de beslissing van de ministers controleren en de niet-naleving van deze regels bestraffen.

De termijn waarbinnen de ontwerpbeslissing of de beslissing tot goedkeuring van het dossier wordt meegedeeld aan de verzoeker na de indiening van het dossier en de termijn waarbinnen de beslissing moet worden genomen na de hoorzitting of de ontvangst van de schriftelijke opmerkingen zullen bij koninklijk besluit worden vastgesteld, om een aanpassing van die termijnen mogelijk te maken indien uit de praktijk blijkt dat ze te lang of te kort zijn.

Er moet worden opgemerkt dat wanneer de ministers een vroegere beslissing herzien (bijvoorbeeld een voordien verleende machtiging intrekken), er geen termijn geldt om de ontwerpbeslissing aan de verzoeker toe te sturen. De door de Koning vastgestelde termijn is daarentegen wel van toepassing om de beslissing te nemen na de hoorzitting of de ontvangst van de schriftelijke opmerkingen.

Le nouvel alinéa 4 du paragraphe 6 prévoit une suspension des délais dans lesquels le projet de décision ou la décision d'approbation du dossier est communiqué au demandeur, en cas de demande d'informations ou de documents visée au paragraphe 3, alinéa 2. En effet, plusieurs demandes d'informations peuvent être envisagées dans le cadre du traitement d'un dossier. S'il apparaît que le dossier introduit par le demandeur ne reprend pas les informations requises par l'arrêté royal d'exécution de l'article 105, les informations nécessaires lui seront demandées pour compléter son dossier. Même si le dossier introduit est conforme à cet arrêté royal, il est possible que l'Institut ou les services de renseignement et de sécurité doivent demander des informations complémentaires au demandeur ou à un tiers pour rendre leur avis. Ces différentes demandes d'information auront pour conséquence que plus de temps sera nécessaire pour traiter le dossier.

Le paragraphe 6 prévoit également que "Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus". Une telle disposition peut par exemple être utile si le demandeur, après avoir reçu une décision de refus, introduit un dossier identique.

La décision des ministres concernés ne peut pas comporter de motifs liés à la sûreté intérieure et extérieure de l'État. Cela vise à protéger les avis des services de renseignement. Les avis des services de renseignement comportent des informations qui peuvent, en cas de divulgation, porter atteinte aux intérêts énumérés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Cet alinéa ne prévoit en aucun cas l'exclusion d'une motivation de la décision. Il vise uniquement à écarter une série d'éléments de cette motivation.

Paragraphe 7

Un premier principe inscrit dans la loi pour protéger la liste des zones sensibles est que la personne qui a obtenu une copie de cette liste doit limiter la diffusion de cette copie aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation (entendu au sens large du terme) du réseau 5G. Pour s'assurer que ces principes soient respectés, des sanctions pénales sont prévues. Ces sanctions pénales couvrent les hypothèses dans lesquelles, par exemple, un employé de la personne morale, avec le consentement

Het nieuwe vierde lid van paragraaf 6 voorziet in een schorsing van de termijnen waarbinnen de ontwerpbeslissing of de beslissing tot goedkeuring van het dossier wordt meegedeeld aan de verzoeker, in geval van een verzoek om informatie of om documenten waarvan sprake in paragraaf 3, tweede lid. Er zijn immers verschillende verzoeken om informatie denkbaar in het kader van de behandeling van een dossier. Indien blijkt dat het dossier dat door de verzoeker is ingediend niet de informatie bevat die vereist wordt door het koninklijk besluit ter uitvoering van artikel 105, zullen de nodige inlichtingen aan hem worden gevraagd om zijn dossier te vervolledigen. Zelfs wanneer het ingediende dossier aan dat koninklijk besluit voldoet, is het mogelijk dat het Instituut of de inlichtingen- en veiligheidsdiensten, om hun advies te verstrekken, aanvullende informatie moeten vragen aan de verzoeker of aan een derde. Deze verschillende verzoeken om informatie zullen tot gevolg hebben dat er meer tijd nodig zal zijn om het dossier te behandelen.

Paragraaf 6 bepaalt ook: "Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering." Zo'n bepaling kan bijvoorbeeld nuttig zijn indien de verzoeker na een afwijzende beslissing te hebben ontvangen, een identiek dossier indient.

De beslissing van de betrokken ministers mag geen redenen bevatten die betrekking hebben op de inwendige en uitwendige veiligheid van de Staat. Dit dient ter bescherming van de adviezen van de inlichtingendiensten. De adviezen van de inlichtingendiensten bevatten informatie die in het geval van openbaarmaking afbreuk kan doen aan de belangen opgesomd in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Dit lid voorziet in geen geval in de uitsluiting van een motivering van de beslissing. Het heeft enkel tot doel een aantal elementen uit deze motivering te weren.

Paragraaf 7

Een eerste principe dat in de wet is ingeschreven om de lijst van de gevoelige zones te beschermen is dat de persoon die een kopie van die lijst ontvangen heeft, de verspreiding van die kopie moet beperken tot de personen die daar kennis van moeten hebben en daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie (opgevat in de ruime betekenis van het woord) van het 5G-netwerk uit te voeren. Om ervoor te zorgen dat die principes worden nageleefd, is in strafsancties voorzien. Deze strafsancties hebben betrekking op de gevallen waarin

de cette dernière (poursuite de la personne morale) ou sans son accord (poursuite de la personne physique), transmettrait cette liste à un tiers.

Pour répondre à une remarque du Conseil d'État, le projet de loi ne prévoit plus qu'un opérateur peut consulter la liste des zones sensibles auprès de l'Institut, s'il peut justifier qu'il a besoin d'en connaître.

Par conséquent, l'accès à la liste des zones sensibles se fera conformément à la loi du 11 avril 1994 relative à la publicité de l'administration, en tenant compte notamment de l'article 6, § 1er, de cette loi qui dispose que l'autorité administrative rejette la demande de consultation, d'explication ou de communication sous la forme de copie d'un document administratif si elle a constaté que l'intérêt de la publicité ne l'emporte pas notamment sur la protection de la sécurité de la population ou de l'ordre public, ou encore, de la sûreté ou de la défense nationales.

Ensuite, compte tenu du fait que la liste des zones sensibles contient des informations sensibles qui pourraient être utilisées par des acteurs afin de porter atteinte aux intérêts énumérés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, la présente disposition en projet interdit à la personne qui a obtenu une copie de la liste des zones sensibles de la divulguer à des tiers. Ainsi, cette personne ne peut transmettre la liste des zones sensibles qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.

Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent faire appel à des administrations publiques dans le cadre de la mise en œuvre de l'article 105 de la loi du 13 juin 2005 relative aux communications électroniques. Ces personnes peuvent communiquer aux administrations publiques des informations confidentielles mais uniquement dans la mesure où c'est nécessaire pour ce que ces administrations publiques puissent effectuer la tâche qui leur est confiée.

Pour répondre à une remarque du Conseil d'État, la loi précise les informations confidentielles que les personnes qui traitent le dossier ne peuvent pas communiquer à des tiers. Il s'agit d'abord d'informations confidentielles du demandeur ou d'une entreprise à laquelle une autorité

bijvoorbeeld een werknemer van de rechtspersoon, met de instemming van deze laatste (vervolging van de rechtspersoon) of zonder zijn akkoord (vervolging van de natuurlijke persoon) deze lijst zou versturen aan een derde.

Om te beantwoorden aan een opmerking van de Raad van State schrijft het wetsontwerp niet langer voor dat een operator de lijst met de gevoelige zones kan raadplegen bij het Instituut indien hij kan aantonen dat het voor hem noodzakelijk is om er kennis van te nemen.

Bijgevolg zal de toegang tot de lijst van de gevoelige zones geschieden overeenkomstig de wet van 11 april 1994 betreffende de openbaarheid van bestuur, met name rekening houdende met artikel 6, § 1, van deze wet, dat bepaalt dat de administratieve overheid de vraag om inzage, uitleg of mededeling in afschrift van een bestuursdocument afwijst wanneer zij heeft vastgesteld dat het belang van de openbaarheid niet opweegt tegen de bescherming van de veiligheid van de bevolking of van de openbare orde, de veiligheid of de verdediging van het land.

Vervolgens, rekening houdende met het feit dat de lijst van de gevoelige zones gevoelige informatie bevat die gebruikt zou kunnen worden door actoren om de belangen opgesomd in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen te schaden, is het door de onderhavige ontworpen bepaling voor de persoon die een kopie van de lijst van de gevoelige zones heeft gekregen, verboden om deze aan derden te onthullen. Aldus mag deze persoon de lijst van de gevoelige zones slechts verzenden aan de personen die daar kennis van moeten hebben en toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.

De personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen een beroep doen op openbare besturen in het kader van de uitvoering van artikel 105 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Deze personen mogen aan de openbare besturen vertrouwelijke informatie meedelen, maar enkel in de mate dat dit noodzakelijk is opdat deze openbare besturen de hun toevertrouwde taak kunnen uitvoeren.

Om te beantwoorden aan een opmerking van de Raad van State verduidelijkt de wet de vertrouwelijke informatie die de personen die het dossier behandelen niet mogen meedelen aan derden. Het gaat allereerst om vertrouwelijke informatie van de verzoeker of van

(IBPT ou services de renseignement et de sécurité) aurait demandé des informations. Ces informations confidentielles sont celles que le demandeur ou cette entreprise qualifie comme telles. Cependant, en vertu de l'article 23, § 3, de la loi IBPT-statut (loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges), l'IBPT peut remettre en cause le caractère confidentiel d'informations considérées comme telles par une entreprise. Il va de soi que ce sont les juridictions qui auront le dernier mot sur le caractère confidentiel ou non d'informations d'entreprise. Il s'agit également des informations confidentielles considérées comme telles par une autorité publique. On vise ici les informations confidentielles de l'État, soit des informations qui, en cas de diffusion, porteraient atteinte aux intérêts de l'État.

L'alinéa 6 du paragraphe 7 énonce que les peines prévues en cas de violation du secret professionnel (article 458 du Code pénal) sont applicables en cas de violation de l'obligation de confidentialité qui repose sur les personnes qui traitent le dossier et sur les administrations publiques auxquelles elles feraient appel.

Enfin, il est à noter que suite à la remarque du Conseil d'État, la disposition qui prévoyait que "l'Institut dispose notamment des pouvoirs prévus à l'article 114/2 pour le contrôle du présent article, de son arrêté d'exécution et de la décision des ministres concernés" a été supprimée. En effet, il n'est pas nécessaire de prévoir une telle disposition dans la mesure où l'article 105 fera partie de la loi du 13 juin 2005 relative aux communications électroniques et par conséquent l'Institut dispose déjà des pouvoirs que cette loi lui octroie.

Paragraphe 8

D'abord, le fait que les infrastructures d'un réseau 5G d'un MNO se trouvent sur le territoire de l'Union européenne signifie que les données traitées par ce réseau seront, du moins en partie, également situées sur ce territoire et pourront donc bénéficier de la protection du RGPD (règlement général sur la protection des données, règlement (UE) 2016/679). Par ailleurs, dans son arrêt Télé 2 (21/12/2016, C-203/15), la CJUE a indiqué que la réglementation nationale doit prévoir que les métadonnées que les opérateurs conservent pour les autorités le soient sur le territoire de l'Union européenne.

een onderneming waaraan een bestuur (het BIPT of inlichtingen- en veiligheidsdiensten) informatie zou hebben gevraagd. Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de verzoeker of deze onderneming. Krachtens artikel 23, § 3, van de BIPT-statuutwet (wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector) mag het BIPT evenwel de vertrouwelijke aard van informatie die als zodanig is bestempeld door een onderneming, ter discussie stellen. Het spreekt vanzelf dat de rechtbanken het laatste woord zullen hebben in verband met de al dan niet vertrouwelijke aard van ondernemingsgegevens. Het gaat ook om de vertrouwelijke informatie die zo door een openbaar bestuur wordt beschouwd. Hierbij wordt verwezen naar de vertrouwelijke informatie van de Staat, namelijk informatie die de belangen van de Staat zou schaden, indien ze verspreid zou worden.

Het zesde lid van paragraaf 7 vermeldt dat de straffen die zijn vastgesteld in geval van schending van het beroepsgeheim (artikel 458 van het Strafwetboek) van toepassing zijn in geval van schending van de geheimhoudingsplicht die rust op de personen die het dossier behandelen en op de openbare besturen waarop zij een beroep zouden doen.

Tot slot moet worden opgemerkt dat naar aanleiding van de opmerking van de Raad van State de bepaling die als volgt luidde: "Het Instituut beschikt met name over de bevoegdheden waarvan sprake in artikel 114/2 voor de controle op dit artikel, het uitvoeringsbesluit ervan en de beslissing van de minister" opgeheven is. Het is immers niet nodig om in een dergelijke bepaling te voorzien omdat artikel 105 deel zal uitmaken van de wet van 13 juni 2005 betreffende de elektronische communicatie en bijgevolg beschikt het Instituut reeds over de bevoegdheden die deze wet eraan verleent.

Paragraaf 8

Ten eerste houdt het feit dat de infrastructuren van een 5G-netwerk van een MNO zich op het grondgebied van de Europese Unie bevinden in dat de gegevens die door dat netwerk worden behandeld zich, althans gedeeltelijk, ook op dat grondgebied zullen bevinden en dus zullen kunnen profiteren van de bescherming van de GDPR (algemene verordening gegevensbescherming, Verordening (EU) 2016/679). Bovendien heeft het HvJ-EU in zijn arrest Télé 2 (21/12/2016, C-203/15) aangegeven dat de nationale reglementering moet voorschrijven dat de metadata die de operatoren voor de overheid bewaren, op het grondgebied van de Europese Unie moeten worden bewaard.

L'exigence de localisation du réseau 5G sur le territoire de l'Union européenne inclut les dispositifs matériels et les logiciels hébergés auprès de ces infrastructures. Par ailleurs, lorsqu'un fournisseur de services accède au réseau de l'opérateur par le biais d'une infrastructure informatique de l'opérateur, cette infrastructure fait partie du réseau et doit donc se trouver sur le territoire de l'Union européenne.

Afin de renforcer la résilience des réseaux en cas d'incidents techniques et/ou diplomatiques internationaux, le Roi devra imposer aux MNO les règles nécessaires afin que les activités indispensables au fonctionnement, à la sécurité et à la continuité du réseau s'effectuent au sein du territoire des États membres de l'Union européenne. Cela se justifie étant donné qu'il n'y a pas de garanties pour les pays tiers que ces tâches peuvent bénéficier des moyens de prévention, de contrôle et de réaction tels que présentés par la Commission et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité dans la stratégie de cybersécurité de la Commission en date du 16/12/2020 (JOIN(2020) 18, "*joint communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*").

Il convient de noter que les règles concernant l'opération du réseau ont été assouplies à la suite de l'avis du Conseil d'État. Dans cet avis, le Conseil d'État fait comprendre que la situation des fournisseurs de services devrait être clarifiée et émet de sérieuses réserves au regard du principe d'égalité et de non-discrimination et du principe de proportionnalité par rapport à une restriction pour un MNO d'avoir recours aux services d'un fournisseur qui ne serait pas à haut risque, du seul fait de sa localisation. Lors des discussions menées pour répondre aux remarques du Conseil d'État, il est apparu que les restrictions géographiques qui doivent être imposées pour la gestion, la configuration, la maintenance ou la supervision du réseau sont trop complexes et trop techniques que pour pouvoir être inscrites dans la loi. L'option a dès lors été choisie d'habiliter le Roi à fixer les exigences concrètes en la matière, en inscrivant le principe dans la loi (c'est également le Roi qui fixe les restrictions concrètes dans le cadre de l'autorisation préalable). Une telle délégation au Roi permettra au Conseil d'État de se prononcer sur les exigences concrètes qui seront fixées dans l'arrêté royal.

Afin d'assurer la proportionnalité des règles fixées par le Roi, la loi prévoit que ces règles ne peuvent être fixées que pour les activités indispensables au fonctionnement,

De eis dat het 5G-netwerk zich op het grondgebied van de Europese Unie moet bevinden, omvat de hardware en de software die in deze infrastructuren wordt gehost. Bovendien, wanneer een dienstenaanbieder toegang krijgt tot het netwerk van de operator via een computerinfrastructuur van de operator, maakt die infrastructuur deel uit van het netwerk en moet die zich dus op het grondgebied van de Europese Unie bevinden.

Om de weerbaarheid van de netwerken in geval van internationale technische en/of diplomatieke incidenten te versterken, zal de Koning de MNO's de nodige regels moeten opleggen opdat de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van het netwerk plaatsvinden binnen het grondgebied van de lidstaten van de Europese Unie. Dat is gerechtvaardigd, aangezien er voor derde landen geen garanties zijn dat deze taken het voordeel kunnen hebben van de preventie-, controle- en reactiemiddelen zoals die op 16/12/2020 door de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid zijn voorgesteld in de cyberveiligheidstrategie van de Commissie (JOIN(2020) 18, "*joint communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*").

Er dient te worden opgemerkt dat de regels betreffende de exploitatie van het netwerk versoepeld zijn naar aanleiding van het advies van de Raad van State. In dat advies laat de Raad van State verstaan dat de situatie van de dienstenaanbieders opgehelderd zou moeten worden en hij maakt wat betreft het gelijkheids- en non-discriminatiebeginsel, alsook het evenredigheidsbeginsel ernstig voorbehoud bij een beperking voor een MNO om een beroep te kunnen doen op de diensten van een aanbieder die geen hoog risico zou vormen, enkel wegens diens lokalisatie. Tijdens de besprekingen die hebben plaatsgevonden om te antwoorden op de opmerkingen van de Raad van State, is gebleken dat de geografische beperkingen die opgelegd moeten worden voor het beheer, de configuratie, het onderhoud van of het toezicht op het netwerk te complex en te technisch zijn om die in de wet te kunnen inschrijven. Daarom is ervoor geopteerd om de Koning bevoegd te verklaren om de concrete eisen ter zake vast te stellen, door het principe in te schrijven in de wet (het is ook de Koning die de concrete beperkingen vaststelt in het kader van de voorafgaande machtiging). Zo'n delegatie aan de Koning zal de Raad van State de mogelijkheid bieden om zich uit te spreken over de concrete eisen die in het koninklijk besluit zullen worden vastgesteld.

Om ervoor te zorgen dat de door de Koning vastgestelde regels evenredig zijn, bepaalt de wet dat deze regels enkel mogen worden vastgesteld voor de

à la sécurité et à la continuité du réseau 5G. Une activité indispensable est par exemple l'exigence suivante inscrite dans la boîte à outils du groupe de coopération NIS ("*Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, 01/2020, p 25): "Veiller à ce que les MNO gèrent leurs centres d'opérations du réseau (NOC) et/ou centres d'opérations de sécurité (SOC) sur place, sur le territoire national et/ou dans l'UE." (traduction libre). Finalement, les règles que le Roi fixe doivent s'appliquer indépendamment du fait que c'est le MNO ou un fournisseur de services qui effectue ces activités, de manière à éviter toute discrimination ou entorse au principe d'égalité.

Le Roi peut étendre les obligations et exigences visées au paragraphe 8, alinéa 1er et 2, aux MVNO qui sont soumis aux trois autorisations visées au paragraphe 1er et aux fournisseurs de réseaux privés de communications électroniques qui y sont également soumis.

CHAPITRE 3

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 4

Cette modification est nécessaire pour permettre à l'IBPT de contrôler le respect de la décision des ministres concernés (en ce compris des conditions qui seraient imposées). Il est à noter que l'article a été revu afin de prendre en compte l'avis du Conseil d'État.

Art. 5

Cette modification est nécessaire dans la mesure où l'IBPT pourrait être amené à transmettre des informations confidentielles d'entreprises aux ministres concernés (voir la liste de ces ministres à l'article 105, § 1, alinéa 3, de la loi du 13 juin 2005 relative aux communications électroniques), afin que ces derniers puissent prendre, de manière éclairée, leur décision visée à l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005.

Art. 6

Cette modification est nécessaire pour permettre à l'IBPT de sanctionner le non-respect de la décision des

activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van het 5G-netwerk. Een absoluut noodzakelijke activiteit is bijvoorbeeld de volgende eis die ingeschreven is in de toolbox van de NIS-samenwerkingsgroep ("*Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, 01/2020, blz. 25): "Waarborgen dat de MNO's hun operationele netwerkcentra (NOC's) en/of operationele beveiligingscentra (SOC's) ter plaatse beheren, op het nationale grondgebied en/of in de EU." (vrij vertaald). Ten laatste moeten de regels die de Koning vaststelt van toepassing zijn los van het feit of die activiteiten worden uitgevoerd door de MNO of een dienstenaanbieder, zodat elke vorm van discriminatie of schending van het gelijkheidsbeginsel vermeden wordt.

De Koning kan de verplichtingen en eisen van paragraaf 8, eerste en tweede lid, uitbreiden naar de MVNO's die onderworpen zijn aan de drie in paragraaf 1 bedoelde machtigingen en naar de aanbieders van private elektronische-communicatienetwerken die eveneens daaraan onderworpen zijn.

HOOFDSTUK 3

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 4

Deze wijziging is noodzakelijk opdat het BIPT de naleving van de beslissing van de betrokken ministers (inclusief van de eventueel opgelegde voorwaarden) kan controleren. Er moet worden opgemerkt dat het artikel herzien is om rekening te houden met het advies van de Raad van State.

Art. 5

Die wijziging is nodig omdat het kan gebeuren dat het BIPT vertrouwelijke informatie van ondernemingen moet doorsturen naar de betrokken ministers (zie de lijst van deze ministers in artikel 105, § 1, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie), opdat zij hun beslissing bedoeld in artikel 105, § 6, eerste lid, van de wet van 13 juni 2005, weloverwogen kunnen nemen.

Art. 6

Deze wijziging is noodzakelijk opdat het BIPT de niet-naleving van de beslissing van de betrokken ministers

ministres concernés qui est visée à l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques.

L'article 21, § 5, de la loi IBPT-statut permet au Conseil de l'IBPT, lorsqu'il conclut à l'existence d'une infraction de donner à un opérateur "l'ordre de remédier à l'infraction, soit immédiatement, soit dans le délai raisonnable qu'il impartit, pour autant que cette infraction n'ait pas cessé" et de préciser "la manière dont il faut remédier à l'infraction".

Un tel pouvoir pourrait par exemple mener l'IBPT à obliger un opérateur à introduire une demande d'autorisation auprès des ministres concernés lorsqu'il a omis de le faire.

Un tel pouvoir pourrait également amener l'IBPT à ordonner à un opérateur de faire rétablir à ses frais la situation antérieure dans un certain délai (en pratique retirer de son réseau certains éléments), si l'opérateur ne respecte pas la décision des ministres concernés de ne pas octroyer l'autorisation ou les conditions attachées à cette dernière.

CHAPITRE 4

Disposition finale et entrée en vigueur

Art. 8

La version de cet article soumise à l'avis du Conseil d'État prévoyait l'entrée en vigueur des obligations de localisation du réseau et de son opération à partir de l'Union européenne pour le 1er janvier 2026. Dorénavant, ce sera le Roi qui fixera les dates d'entrée en vigueur des différentes obligations, et ce pour les raisons suivantes. D'abord, afin de tenir compte des remarques du Conseil d'État concernant la localisation des fournisseurs (voir *supra* les commentaires à l'article 105, § 8), les exigences concrètes en la matière seront dorénavant fixées dans un arrêté royal, délibéré en Conseil des ministres. Dès lors, il est pertinent de prévoir que l'entrée en vigueur de ces exigences soit également fixée par l'arrêté royal délibéré en Conseil des ministres. Par ailleurs, cet arrêté royal pourra le cas échéant prévoir des dates d'entrée en vigueur des obligations différentes selon les couches de réseau et tenir compte le cas échéant des dates d'application des restrictions relatives à l'utilisation des éléments actifs à haut risque sur les diverses parties du réseaux 5G. Pour rappel, ces restrictions et leur

waarvan sprake in artikel 105, § 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie, kan bestraffen.

Artikel 21, § 5, van de BIPT-statuutwet stelt de Raad van het BIPT, wanneer deze besluit tot het bestaan van een overtreding, in staat om een operator "het bevel [te geven] om een eind te maken aan de overtreding, hetzij onmiddellijk, hetzij binnen de redelijke termijn die hij bepaalt, voor zover deze overtreding niet is stopgezet" en "de manier waarop de overtreding ongedaan moet worden gemaakt" te verduidelijken.

Een dergelijke bevoegdheid zou het BIPT er bijvoorbeeld toe kunnen aanzetten om een operator te verplichten om een machtiging te vragen aan de betrokken ministers wanneer hij dat heeft nagelaten te doen.

Een dergelijke bevoegdheid kan het BIPT er ook toe aanzetten om een operator te gelasten om op zijn kosten binnen een bepaalde termijn de vorige situatie te laten herstellen (in de praktijk bepaalde elementen uit zijn netwerk verwijderen), indien de operator het besluit van de betrokken ministers om geen machtiging te verlenen of de daarbij horende voorwaarden, niet naleeft.

HOOFDSTUK 4

Slotbepaling en inwerkingtreding

Art. 8

De versie van dit artikel die voor advies is voorgelegd aan de Raad van State voorzag in de inwerkingtreding van de verplichtingen omtrent de lokalisatie van het netwerk en de exploitatie ervan vanuit de Europese Unie op 1 januari 2026. Voortaan zal het de Koning zijn die de datums van inwerkingtreding van de verschillende verplichtingen zal vaststellen en wel om de volgende redenen. Ten eerste zullen, om rekening te houden met de opmerkingen van de Raad van State betreffende de lokalisatie van de aanbieders (zie hierboven de opmerkingen op artikel 105, § 8), de concrete eisen ter zake voortaan vastgesteld worden in een koninklijk besluit vastgesteld na overleg in de Ministerraad. Het houdt dan ook steek om te bepalen dat de inwerkingtreding van deze eisen eveneens wordt vastgesteld via een koninklijk besluit vastgesteld na overleg in de Ministerraad. Bovendien zal dit koninklijk besluit, in voorkomend geval, de datums van inwerkingtreding van de verschillende verplichtingen kunnen vaststellen naargelang de netwerklagen en, in voorkomend geval, rekening

date d'application seront définies dans un arrêté royal conformément à l'article 105, § 4.

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

Petra DE SUTTER

kunnen houden met de datums van toepassing van de beperkingen op het gebruik van de actieve elementen die een hoog risico vormen in de diverse delen van de 5G-netwerken. Ter herinnering, deze beperkingen en de datum van toepassing ervan zullen worden bepaald in een koninklijk besluit overeenkomstig artikel 105, § 4.

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

Petra DE SUTTER

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G

CHAPITRE 1ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2

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

Art. 2

Dans l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, modifiée en dernier lieu par la loi du 26 mars 2018, les modifications suivantes sont apportées:

1° il est inséré un X° rédigé comme suit:

"X° "MNO": un opérateur qui offre des services de communications électroniques mobiles et qui dispose d'un réseau d'accès radioélectrique propre, ainsi que de tous les éléments utiles à l'exploitation du réseau;";

2° il est inséré un Y° rédigé comme suit:

"Y° "MVNO": un opérateur qui offre des services de communications électroniques mobiles sans être MNO.".

Art. 3

L'article 105, de la même loi, est remplacé par ce qui suit:

"Art. 105. § 1er. Dans le but de préserver les intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, les MNO obtiennent une autorisation des ministres concernés visés à l'alinéa 2 avant d'utiliser un élément de leur réseau.

Pour l'application du présent article, il faut entendre par ministres concernés: le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères.

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2

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

Art. 2

In artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van 26 maart 2018, worden de volgende wijzigingen aangebracht:

1° een bepaling onder X° wordt ingevoegd, luidende:

"X° "MNO": een operator die mobiele elektronische-communicatiediensten aanbiedt en die beschikt over een eigen radiotoegangsnetwerk, alsook over alle nuttige elementen voor de exploitatie van het netwerk; ";

2° een bepaling onder Y° wordt ingevoegd, luidende:

"Y° "MVNO": een operator die mobiele elektronische-communicatiediensten aanbiedt zonder MNO te zijn.".

Art. 3

Artikel 105 van dezelfde wet wordt vervangen als volgt:

"Art. 105. § 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO's een machtiging krijgen van de betrokken ministers beoogd in het tweede lid alvorens een element van hun netwerk te gebruiken.

Voor de toepassing van dit artikel wordt verstaan onder betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken.

L'alinéa 1er n'est pas d'application:

1° pour l'utilisation d'éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d'énergie;

2° pour les points de terminaison tels que définis à l'article 2, 16°, qui n'émettent pas de signaux radioélectriques de service mobile 5G;

3° pour les réseaux mobiles de quatrième génération et des générations antérieures, pour autant qu'ils ne sont pas nécessaires à la transmission des signaux radioélectriques des générations ultérieures à la quatrième génération.

Si l'utilisation dudit élément de réseau est déjà effective à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, 1°, la demande de régularisation est introduite dans les deux mois qui suivent cette date.

Le réseau mobile d'un MNO d'une génération ultérieure à la quatrième génération se trouve sur le territoire de l'Union européenne et est géré, exploité, configuré et supervisé à partir de ce territoire.

§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres:

1° étendre l'obligation d'obtenir une autorisation visée au paragraphe 1er à une ou plusieurs catégories de MVNO;

2° étendre l'obligation d'obtenir une autorisation visée au paragraphe 1er aux fournisseurs de réseaux privés mobiles de communications électroniques ou à une ou plusieurs catégories de fournisseurs, ou charger une ou plusieurs autorités de désigner les fournisseurs soumis à cette obligation;

3° étendre l'obligation d'obtenir une autorisation visée au paragraphe 1er pour bénéficier de services de fournisseurs qui interviennent ponctuellement dans la gestion du réseau, notamment en cas d'incident ou de modification majeure du réseau ou qui gèrent ou supervise quotidiennement des éléments du réseau, pour autant qu'Il fixe les restrictions applicables pour l'utilisation de leurs services;

4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er , alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel relatif à un élément de réseau;

5° préciser les obligations visées au paragraphe 1er, alinéa 5, et les étendre à une ou plusieurs catégories de MVNOs et de fournisseurs visés à l'alinéa 1er, 2°.

§ 3. Le demandeur introduit son dossier auprès des ministres concernés.

Het eerste lid is niet van toepassing:

1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;

2° voor de netwerkaansluitpunten zoals gedefinieerd in artikel 2, 16°, die geen mobiele-dienstradiosignalen uitzenden 5G;

3° voor de mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor de transmissie van radiosignalen van latere generaties dan de vierde.

Indien het voormelde netwerkelement reeds wordt gebruikt op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, 1°, wordt het verzoek om regularisatie ingediend in de twee maanden die volgen op die datum.

Het mobiele netwerk van een MNO van een latere generatie dan de vierde, bevindt zich op het grondgebied van de Europese Unie en wordt vanaf dat grondgebied beheerd, geëxploiteerd, geconfigureerd en gemonitord.

§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:

1° de verplichting om een machtiging bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;

2° de verplichting om een machtiging bedoeld in paragraaf 1 te krijgen, uitbreiden naar de aanbieders van private mobiele elektronische-communicatienetwerken of naar een of meer categorieën van aanbieders, ofwel een of meer autoriteiten opdragen de aan die verplichting onderworpen aanbieders aan te wijzen;

3° de verplichting uitbreiden om een in paragraaf 1 bedoelde machtiging te krijgen om gebruik te maken van diensten van aanbieders die gericht tussenbeide komen in het beheer van het netwerk, met name in geval van incidenten of grote wijzigingen van het netwerk of die dagelijks netwerkelementen beheren of erop toezien, voor zover Hij de restricties vaststelt die voor het gebruik van hun diensten van toepassing zijn;

4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware met betrekking tot een netwerkelement;

5° de verplichtingen bedoeld in paragraaf 1, vijfde lid, preciseren en ze uitbreiden met een of meer categorieën van MVNO's en aanbieders bedoeld in het eerste lid, 2°.

§ 3. De verzoeker dient zijn dossier in bij de betrokken ministers.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, la composition du dossier.

Les ministres concernés transmettent immédiatement le dossier aux entités consultatives afin qu'elles formulent un avis conformément au paragraphe 4, alinéa 4.

Les ministres concernés et l'Institut peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.

§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au § 1er, ou la revoient d'initiative en raison d'un nouvel élément, les ministres concernés mettent en œuvre les restrictions fixées par le Roi, par arrêté délibéré en Conseil des ministres, concernant:

1° l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque;

2° la localisation des éléments de réseaux ou du fournisseur.

Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en œuvre de la nouvelle décision qui est postérieure par rapport aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.

Le profil de risque d'un fournisseur est évalué sur base des critères suivants:

1° La probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un État membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants:

— un lien fort avec le gouvernement du pays en question;

— la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des données ou de sécurité entre l'Union européenne et le pays en question;

— les caractéristiques de la propriété d'entreprise du fournisseur;

— la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements;

— le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive.

De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de samenstelling van het dossier vast.

De betrokken ministers versturen het dossier onverwijld naar de adviserende entiteiten opdat zij een advies formuleren overeenkomstig paragraaf 4, vierde lid.

De betrokken ministers en het Instituut kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.

§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in § 1 bedoelde verzoek of deze op eigen initiatief herzien wegens een nieuw element, leggen de betrokken ministers de beperkingen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende:

1° het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen;

2° de lokalisatie van de netwerkelementen of van de leverancier.

Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.

Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:

1° De kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:

— een sterke link met de regering van het land in kwestie;

— de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;

— de karakteristieken van de eigendom van de onderneming van de leverancier;

— het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;

— het land waaruit de leverancier afkomstig is, voert of is betrokken bij een offensief cyberbeleid.

2° La capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité;

3° La qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation adéquate des priorités est donnée aux pratiques en matière de sécurité.

Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 3.

Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 3, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 3, 2° et 3°.

Les zones sensibles sont identifiées par le Conseil national de sécurité, et ce, en tenant compte de la présence dans ces zones de sites liés aux intérêts énumérés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Un opérateur peut consulter la liste des zones sensibles auprès de l'Institut, s'il peut justifier qu'il a besoin d'en connaître.

§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision d'initiative, le demandeur dispose de vingt-huit jours calendriers après avoir été informé du point de vue des ministres concernés pour présenter ses observations écrites.

Le demandeur peut demander à être entendu. Les ministres concernés peuvent se faire représenter par l'administration de leur choix. L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.

§ 6. Les ministres concernés prennent une décision dans les trois mois à partir de l'introduction de la demande.

S'ils ne sont pas en mesure de prendre une décision dans ce délai, le délai dans lequel la décision sera rendue est communiqué au demandeur.

Sauf en cas d'application de l'alinéa 2, le défaut de décision dans le délai de trois mois fixé à l'alinéa 1er équivaut à un refus.

§ 7. Les personnes qui traitent le dossier introduit en vertu du paragraphe 3 sont tenues au secret professionnel. Elles ne peuvent communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'exercice de leurs fonctions, hormis les exceptions prévues par la loi.

2° Het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;

3° De algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het derde lid beoogde criteria aanvullen.

Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het derde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het derde lid, 2° en 3°.

De gevoelige zones worden geïdentificeerd door de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen opgesomd in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Een operator kan de lijst met de gevoelige zones raadplegen bij het Instituut indien hij kan aantonen dat het voor hem noodzakelijk is om er kennis van te nemen.

§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing op eigen initiatief te herzien, beschikt de verzoeker, na ingelicht te zijn over het standpunt van de betrokken ministers, over achtentwintig kalenderdagen tijd om zijn schriftelijke opmerkingen voor te leggen.

De verzoeker kan vragen om te worden gehoord. De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.

§ 6. De betrokken ministers nemen één beslissing binnen drie maanden na de indiening van het verzoek.

Indien ze niet in staat zijn om binnen deze termijn een beslissing te nemen, wordt de termijn waarbinnen de beslissing zal worden genomen, meegedeeld aan de verzoeker.

Behalve in geval van toepassing van het tweede lid, staat het uitblijven van een beslissing binnen de in het eerste lid vastgestelde termijn van drie maanden gelijk aan een weigering.

§ 7. De personen die het krachtens paragraaf 3 ingediende dossier behandelen, zijn onderworpen aan het beroepsgeheim. Zij mogen geen vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functies meedelen aan derden, behalve in de wettelijk vastgelegde uitzonderingen.

L'Institut dispose notamment des pouvoirs prévus à l'article 114/2 pour le contrôle du présent article, de son arrêté d'exécution et de la décision des ministres concernés."

CHAPITRE 3

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 4

Dans l'article 14, § 1er, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, modifiée en dernier lieu par la loi du 7 avril 2019, il est inséré le point j) rédigé comme suit:

"j) toute décision contraignante adoptée par la Commission européenne, par l'Institut, ou par les ministres visés à l'article 105, § 1er, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques.".

Art. 5

A l'article 21, § 1er, de la même loi, les modifications suivantes sont apportées:

1° les mots "ou aux décisions prises" sont remplacés par les mots "à une décision prise".

2° les mots ", ou à une décision prise par les ministres visés à l'article 105, § 1er, alinéa 2, de la loi du 13 juin 2005 relative aux communications électroniques" sont insérés entre les mots "en exécution de cette législation ou réglementation" et ", il fait part le cas échéant de ses griefs à l'intéressé".

CHAPITRE 4

Disposition finale et entrée en vigueur

Art. 6

Le Roi peut codifier les dispositions pertinentes de la loi de 13 juin 2005 relative aux communications électroniques ou d'autres lois relatives aux communications électroniques, en ce compris celles modifiées et insérées par la présente loi, ainsi que les dispositions qui y auraient, jusqu'au moment de la coordination, expressément ou implicitement apporté des modifications.

A cette fin, Il peut:

1° modifier l'ordre, la numérotation et, en général, la présentation des dispositions à codifier;

Het Instituut beschikt met name over de bevoegdheden waarvan sprake in artikel 114/2 voor de controle op dit artikel, het uitvoeringsbesluit ervan en de beslissing van de betrokken ministers."

HOOFDSTUK 3

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische posten telecommunicatiesector

Art. 4

Aan artikel 14, § 1, eerste lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische posten telecommunicatiesector, laatstelijk gewijzigd bij de wet van 7 april 2019, wordt een punt j) ingevoegd, luidende:

"j) elk bindend besluit aangenomen door de Europese Commissie door het Instituut, of door de ministers beoogd in artikel 105, § 1, tweede lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.".

Art. 5

In artikel 21, § 1, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° de woorden "of van de besluiten" worden vervangen door de woorden "op een besluit".

2° de woorden"of op een beslissing genomen door de ministers beoogd in artikel 105, § 1, tweede lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie" worden ingevoegd tussen de woorden "ter uitvoering van die wetgeving of reglementering" en "deelt hij in voorkomend geval zijn grieven mee aan de betrokkene".

HOOFDSTUK 4

Slotbepaling en inwerkingtreding

Art. 6

De Koning kan de relevante bepalingen van de wet van 13 juni 2005 betreffende de elektronische communicatie of van andere wetten inzake elektronische communicatie, met inbegrip van diegene gewijzigd en ingevoegd door deze wet, codificeren, evenals de bepalingen die hieraan uitdrukkelijk of stilzwijgend wijzigingen aanbrengen tot aan het tijdstip van de codificatie.

Daartoe kan Hij:

1° de volgorde en de nummering van de te codificeren bepalingen veranderen en in het algemeen de teksten naar de vorm wijzigen;

2° modifier les références qui seraient contenues dans les dispositions à codifier en vue de les mettre en concordance avec la nouvelle numérotation;

3° modifier la rédaction des dispositions à codifier en vue d'assurer leur concordance et d'en unifier la terminologie sans qu'il puisse être porté atteinte aux principes inscrits dans ces dispositions.

La codification remplacera les dispositions visées à l'alinéa 1er et entrera en vigueur à la date de sa confirmation par la loi.

Art. 7

L'article 105, paragraphe 1er, alinéa 4, entre en vigueur le 1er janvier 2026.

2° de verwijzingen die voorkomen in de te codificeren bepalingen, met de nieuwe nummering overeenbrengen;

3° zonder afbreuk te doen aan de beginselen die in de te codificeren bepalingen vervat zijn, de redactie ervan wijzigen om ze onderling te doen overeenstemmen en eenheid in de terminologie te brengen.

De codificatie vervangt de bepalingen bedoeld in het eerste lid en treedt in werking op de dag van de bekrachtiging ervan bij de wet.

Art. 7

Het artikel 105, paragraaf 1, vierde lid, wordt van kracht op 1 januari 2026.

Analyse d'impact intégrée

Fiche signalétique

A. Auteur

Membre du Gouvernement compétent

Madame Petra De Sutter

Contact cellule stratégique

Nom : Marijke De Rooms

E-mail : marijke.derooms@bosa.fgov.be

Téléphone : +32475730217

Administration

IBPT

Contact administration

Nom : Evy Bawin

E-mail : evy.bawin@BIPT.be

Téléphone : +32476614148

B. Projet

Titre de la règlementation

Avant-projet de loi introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G

Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.

Divers travaux ont été menés au niveau de l'Union européenne concernant la sécurité de la 5G qui ont abouti à des recommandations invitant les Etats membres à prendre des mesures spécifiques. Cet avant-projet doit être lu dans ce contexte.

En conséquence de cet avant-projet, les réseaux 5G devront être situés sur le territoire de l'UE et les opérateurs d'un réseau mobile 5G seront tenus d'obtenir une autorisation préalable ou de régularisation pour l'utilisation de tous les éléments de réseau dans leur réseau mobile 5G. Ces exigences sont introduites pour renforcer notre sécurité nationale.

Analyses d'impact déjà réalisées :

☐ Oui ■ Non

C. Consultations sur le projet de réglementation

Consultation obligatoire, facultative ou informelle

Consultation publique facultative :
https://www.ibpt.be/operateurs/publication/consultation-concernant-les-projets-de-loi-et-darrete-royal-introduisant-des-mesures-de-securite-supplementaires-pour-la-fourniture-de-services-mobiles-5g

D. Sources utilisées pour effectuer l'analyse d'impact

Statistiques, documents, institutions et personnes de référence

/

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

1. Lutte contre la pauvreté

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

2. Égalité des chances et cohésion sociale

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

3. Égalité des femmes et des hommes

1. Quelles personnes sont (directement et indirectement) concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

☐ Des personnes sont concernées. | ■ Aucune personne n'est concernée.

Expliquez pourquoi :

Cet avant-projet s'adressent aux entreprises et pas aux particuliers.

4. Santé

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

5. Emploi

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

6. Modes de consommation et production

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

7. Développement économique

■ Impact positif ☐ Impact négatif | ☐ Pas d'impact

Expliquez

Positif: cet avant-projet visent à sécuriser l'économie belge en diminuant les risques d'ingérence et techniques dans les infrastructures de télécommunication belges. Il est à noter que le système d'autorisation préalable introduit par l'avant-projet vise à préserver les intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Négatif: comme certains éléments de réseau seront considérés comme "à haut risque" à la suite de cet avant-projet et ne pourront donc être utilisés que dans une mesure limitée dans le réseau mobile 5G d'un opérateur de réseau mobile 5G, les MNOs belges auront moins de choix de fournisseurs pour les éléments de réseau 5G. En outre, les opérateurs de réseau mobile 5G devront (éventuellement) changer d'équipementier, bien que le projet d'arrêté royal portant exécution de cet avant-projet prévoit des périodes de transition qui devraient en limiter l'impact.

8. Investissements

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

9. Recherche et développement

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

10. PME

1. Quelles entreprises sont directement et indirectement concernées ?

☒ Des entreprises (dont des PME) sont concernées. | ☐ Aucune entreprise n'est concernée.

Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (

Tous les équipementiers et fournisseurs d'éléments de réseaux mobiles 5G et tous les MNOs (mobile network operators) d'un réseau mobile 5G sont concernés par cet avant-projet. Cela n'inclut pas les PME, donc a fortiori pas les micro-entreprises.

Toutefois, le régime d'autorisation préalable peut être étendu, par arrêté royal délibéré en Conseil des ministres, à d'autres catégories définies par cet avant-projet pour les MVNO (mobile virtual network operator) et les fournisseurs de réseaux privés de communications électroniques mobiles, et ces derniers pouvant être des PME.

2. Identifiez les impacts positifs et négatifs du projet sur les PME.

N.B. les impacts sur les charges administratives doivent être détaillés au thème 11

Pas concernés

☐ Il y a des impacts négatifs.

11. Charges administratives

| ☒ Des entreprises/citoyens sont concernés. ☐ Les entreprises/citoyens ne sont pas concernés.

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation.

Réglementation actuelle	Réglementation en projet
/	Les opérateurs d'un réseau mobile 5G sont tenus d'obtenir une autorisation préalable ou de régularisation pour l'utilisation de tous les éléments de réseau dans leur réseau mobile 5G.

☐ S'il y a des formalités et/ou des obligations dans la réglementation actuelle, cochez cette case.

☒ S'il y a des formalités et/ou des obligations pour la réglementation en projet, cochez cette case.

2. Quels documents et informations chaque groupe concerné doit-il fournir ?

Réglementation en projet

L'opérateur d'un réseau mobile 5G doit constituer un dossier pour chaque demande d'autorisation préalable ou de régularisation. L'article 6 du projet d'arrêté royal portant exécution de cet avant-projet énumère les informations qui doivent être présentes dans ce dossier.

Pour tous les éléments actifs qui sont utiles à la fourniture de services mobiles 5G, il faut au moins inclure les éléments suivants : l'identité des différentes personnes morales qui gèrent, exploitent, configurent et supervisent ces différents éléments + une description des éléments actifs qu'il souhaite utiliser ou utilise + l'identité des équipementiers d'éléments de réseau qui produisent ces éléments actifs.

Lorsque l'opérateur est informé qu'un équipementier auquel il entend faire appel ou auquel il fait appel est considéré comme un équipementier à haut risque, il ajoute également les informations suivantes : la localisation des sites du réseau d'agrégation du réseau de transport et des sites du réseau d'accès radioélectrique dans lesquels il envisage d'utiliser des éléments actifs à haut risque de ces équipementiers ou dans lesquels il les utilise et, pour les sites du réseau d'accès radioélectrique, les zones couvertes par ces sites + des explications détaillées concernant le respect du pourcentage de 35% visé à l'article 5 du projet d'arrêté royal portant exécution de cet avant-projet.

3. Comment s'effectue la récolte des informations et des documents, par groupe concerné ?

Réglementation en projet

L'opérateur d'un réseau 5G soumet lui-même ce dossier au ministre compétent.

4. Quelles est la périodicité des formalités et des obligations, par groupe concerné ?

Réglementation en projet

Ce dossier doit être soumis par nouvel élément de réseau que l'opérateur d'un réseau 5G entend utiliser et en cas de mise à jour modifiant les informations contenues dans la demande préalable.

5. Quelles mesures sont prises pour alléger / compenser les éventuels impacts négatifs ?

Le même dossier peut couvrir plusieurs nouveaux éléments de réseau que l'opérateur d'un réseau 5G a l'intention d'utiliser.

Selon l'arrêté royal portant exécution de cet avant-projet de loi, lorsqu'une mise à jour nécessite une nouvelle demande d'autorisation, le dossier initial peut être soumis à nouveau à condition qu'il indique clairement les modifications apportées à ce dossier initial.

12. Énergie

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

13. Mobilité

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

14. Alimentation

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

15. Changements climatiques

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

16. Ressources naturelles

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

17. Air intérieur et extérieur

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

18. Biodiversité

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

19. Nuisances

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

20. Autorités publiques

☐ Impact positif ☐ Impact négatif | ■ Pas d'impact

21. Cohérence des politiques en faveur du développement

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants : sécurité alimentaire, santé et accès aux médicaments, travail décent, commerce local et international, revenus et mobilisations de ressources domestiques (taxation), mobilité des personnes, environnement et changements climatiques (mécanismes de développement propre), paix et sécurité.

☐ Impact sur les pays en développement. | ■ Pas d'imapct sur les pays en développement.

Expliquez pourquoi :

Aucun des acteurs concernés n'est situé dans un pays en développement ou ne s'adresse à un tel pays.

Geïntegreerde impactanalyse

Beschrijvende fiche

A. Auteur

Bevoegd regeringslid

Mevrouw Petra De Sutter

Contactpersoon beleidscel

Naam : Marijke De Rooms

E-mail : marijke.derooms@bosa.fgov.be

Tel. Nr. : +32475730217

Overheidsdienst

BIPT

Contactpersoon overheidsdienst

Naam : Evy Bawin

E-mail : evy.bawin@BIPT.be

Tel. Nr. : +32476614148

B. Ontwerp

Titel van de regelgeving

Voorontwerp van wet tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten

Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.

Op het niveau van de Europese Unie werden diverse werkzaamheden uitgevoerd met betrekking tot de 5G-beveiliging die zijn uitgemond in aanbevelingen die de lidstaten uitnodigen om specifieke maatregelen te nemen. Het voorontwerp van wet moet in die context worden gelezen.

Ten gevolge van dit voorontwerp, zullen de 5G-netwerken zich op het grondgebied van de EU moeten bevinden en zullen de operatoren van een mobiel 5G-netwerk verplicht zijn een voorafgaande machtiging of regularisatie aan te vragen voor het gebruik van alle netwerkelementen in hun mobiel 5G-netwerk. Deze eisen worden ingevoerd teneinde onze nationale veiligheid te versterken.

Impactanalyses reeds uitgevoerd:

☐ Ja ■ Nee

C. Raadpleging over het ontwerp van regelgeving

Verplichte, facultatieve of informele raadplegingen

Facultatieve openbare raadpleging:
https://www.bipt.be/operatoren/publication/raadpleging-betreffende-de-ontwerpen-van-wet-en-van-koninklijk-besluit-tot-invoering-van-bijkomende-beveiligingsmaatregelen-voor-de-verstrekking-van-mobiele-5g-dienste

D. Bronnen gebruikt om de impactanalyse uit te voeren

Statistieken, referentiedocumenten, organisaties en referentiepersonen

/

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

1. Kansarmoedebestrijding

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

2. Gelijke kansen en sociale cohesie

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

3. Gelijkheid van vrouwen en mannen

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

☐ Er zijn personen betrokken. | ■ Personen zijn niet betrokken.

Leg uit waarom:

Dit voorontwerp richt zich tot bedrijven en niet tot individuen.

4. Gezondheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

5. Werkgelegenheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

6. Consumptie- en productiepatronen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

7. Economische ontwikkeling

■ Positieve impact ☐ Negatieve impact | ☐ Geen impact

Leg uit

Positief: dit voorontwerp heeft tot doel de Belgische economie veilig te stellen door zowel de risico's van inmenging als de technische risico's in de Belgische telecommunicatie-infrastructuur te verminderen. Er zij op gewezen dat het door het voorontwerp ingevoerde stelsel van voorafgaande machtiging ertoe strekt de belangen als bedoeld in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en veiligheidsmachtigingen, -attesten en -kennisgevingen te vrijwaren.

Negatief: doordat sommige netwerkelementen ten gevolge van dit voorontwerp als "een hoog risico vormend" zullen worden beschouwd en deze aldus in slechts beperkte mate mogen worden gebruikt in het mobiel 5G-netwerk van een operator van een mobiel 5G-netwerk, zullen de Belgische MNOs minder keuze hebben qua leveranciers van 5G-netwerkelementen. Bovendien zullen de operatoren van een mobiel 5G-netwerk (mogelijks) van leverancier van diens netwerkelementen moeten veranderen, al voorziet het ontwerp van koninklijk besluit ter uitvoering van dit voorontwerp wel in overgangsperiodes die de impact hiervan moeten beperken.

8. Investeringen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

9. Onderzoek en ontwikkeling

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

10. Kmo's

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?

☒ Er zijn ondernemingen (inclusief kmo's) betrokken. | ☐ Ondernemingen zijn niet betrokken.

Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (

Alle producenten en leveranciers van elementen van mobiele 5G-netwerken en alle MNOs (mobile network operators) van een mobiel 5G-netwerk zijn bij dit voorontwerp betrokken. Hiertoe behoren geen kmo's, dus a fortiori ook geen micro-ondernemingen.

Het is echter wel zo dat het systeem van voorafgaande machtiging, bij een na overleg in de Ministerraad vastgesteld koninklijk besluit, kan worden uitgebreid tot andere in dit voorontwerp omschreven categorieën voor MVNOs (mobile virtual network operators) en aanbieders van private mobiele elektronische communicatienetwerken, en deze laatsten zouden mogelijks een kmo kunnen zijn.

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.

N.B. de impact op de administratieve lasten moet bij het punt 11 gedetailleerd worden

Niet betrokken

☐ Er is een negatieve impact.

11. Administratieve lasten

| ☒ Ondernemingen of burgers zijn betrokken. ☐ Ondernemingen of burgers zijn niet betrokken.

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving.

Huidige regelgeving	Ontwerp van regelgeving
/	Operatoren van een mobiel 5G-netwerk zijn verplicht een voorafgaande machtiging of regularisatie aan te vragen voor het gebruik van alle netwerkelementen in hun mobiel 5G-netwerk.

☐ Vink dit aan indien er formaliteiten en/of verplichtingen zijn in de huidige regelgeving.

☒ Vink dit aan indien er formaliteiten en/of verplichtingen zijn in het ontwerp van regelgeving.

2. Welke documenten en informatie moet elke betrokken doelgroep verschaffen?

Ontwerp van regelgeving

De operator van een mobiel 5G-netwerk dient per verzoek om voorafgaande machtiging of regularisatie een dossier op te stellen. Artikel 6 van het ontwerp van koninklijk besluit ter uitvoering van dit voorontwerp somt de informatie op die in dit dossier aanwezig moet zijn.

Voor alle actieve elementen die nuttig zijn voor de verstrekking van mobiele 5G-diensten moeten minstens de volgende zaken worden vermeld: de identiteit van de verschillende rechtspersonen die deze verschillende elementen beheren, exploiteren, configureren en monitoren + een beschrijving van de actieve elementen die hij wenst te gebruiken of gebruikt + de identiteit van de producenten van netwerkelementen die deze actieve elementen vervaardigen.

Indien de operator ervan op de hoogte is dat de producent op wie hij van plan is een beroep te doen of op wie hij een beroep doet, wordt beschouwd als een producent van netwerkelementen die een hoog risico vormen, voegt hij ook de volgende informatie toe: de locatie van de sites van het aggregatienetwerk van het transportnetwerk, alsook van de sites van het radiotoegangsnetwerk waarin hij van plan is actieve elementen die een hoog risico vormen, te gebruiken of waarin hij ze gebruikt en, voor de sites van het radiotoegangsnetwerk, de zones gedekt door deze sites + een gedetailleerde uitleg over de inachtneming van het percentage van 35% waarvan sprake in artikel 5 van het ontwerp van koninklijk besluit ter uitvoering van dit voorontwerp.

3. Hoe worden deze documenten en informatie, per betrokken doelgroep, ingezameld?

Ontwerp van regelgeving

De operator van een 5G-netwerk dient dit dossier zelf in bij de bevoegde minister.

4. Welke is de periodiciteit van de formaliteiten en verplichtingen, per betrokken doelgroep?

Ontwerp van regelgeving

Dit dossier dient te worden ingediend per nieuw netwerkelement dat de operator van een 5G-netwerk beoogt te gebruiken, en in geval van een update die de in het vorige verzoek vervatte informatie wijzigt.

5. Welke maatregelen worden genomen om de eventuele negatieve impact te verlichten / te compenseren?

Eenzelfde dossier mag betrekking hebben op meerdere nieuwe netwerkelementen die de operator van een 5G-netwerk beoogt te gebruiken.

Wanneer een update een nieuw verzoek om machtiging vergt, mag het initiële dossier opnieuw worden ingediend, mits duidelijk wordt aangegeven welke wijzigingen werden aangebracht ten opzichte van dat initiële dossier.

12. Energie

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

13. Mobiliteit

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

14. Voeding

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

15. Klimaatverandering

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

16. Natuurlijke hulpbronnen

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

17. Buiten- en binnenlucht

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

18. Biodiversiteit

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

19. Hinder

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

20. Overheid

☐ Positieve impact ☐ Negatieve impact | ■ Geen impact

21. Beleidscoherentie ten gunste van ontwikkeling

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van: voedselveiligheid, gezondheid en toegang tot geneesmiddelen, waardig werk, lokale en internationale handel, inkomens en mobilisering van lokale middelen (taxatie), mobiliteit van personen, leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling), vrede en veiligheid.

☐ Impact op ontwikkelingslanden. | ■ Geen impact op ontwikkelingslanden.

Leg uit waarom:

Geen van de betrokken actoren bevindt zich in, noch richt zich tot een ontwikkelingsland.

AVIS DU CONSEIL D'ÉTAT N° 69.160/4 DU 6 MAI 2021

Le 1er avril 2021, le Conseil d'État, section de législation, a été invité par la Vice-Première Ministre et Ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G'.

L'avant-projet a été examiné par la quatrième chambre le 6 mai 2021. La chambre était composée de Martine Baguet, président de chambre, Luc Cambier et Bernard Blero, conseillers d'État, Marianne Dony, assesseur, et Charles-Henri Van Hove, greffier assumé.

Le rapport a été présenté par Anne Vagman, premier auditeur, et Julien Gaul, auditeur adjoint.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine Baguet.

L'avis, dont le texte suit, a été donné le 6 mai 2021.

*

ADVIES VAN DE RAAD VAN STATE NR. 69.160/4 VAN 6 MEI 2021

Op 1 april 2021 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en Minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten'.

Het voorontwerp is door de vierde kamer onderzocht op 6 mei 2021. De kamer was samengesteld uit Martine Baguet, kamervoorzitter, Luc Cambier en Bernard Blero, staatsraden, Marianne Dony, assessor, en Charles-Henri Van Hove, toegevoegd griffier.

Het verslag is uitgebracht door Anne Vagman, eerste auditeur, en Julien Gaul, adjunct-auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine Baguet.

Het advies, waarvan de tekst hierna volgt, is gegeven op 6 mei 2021.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet‡ , à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

Observations générales

1.1. L'avant-projet à l'examen instaure plusieurs restrictions dans le cadre du déploiement des réseaux et de l'exploitation des technologies mobiles de cinquième génération, à savoir:

– l'obligation pour les "Mobile Network Operator" de disposer d'une autorisation préalable pour pouvoir utiliser certains éléments de leur réseau (article 105, § 1er, alinéa 1er, en projet); l'avant-projet prévoit la possibilité d'étendre l'obligation à d'autres catégories d'entreprises (article 105, § 2, 1° et 2°, en projet);

– l'obligation d'introduire une demande de régularisation dans le cas où l'utilisation de certains éléments des réseaux des "Mobile Network Operator" est effective au moment de l'entrée en vigueur de l'arrêté royal visé à l'article 105, § 4, alinéa 1er, 1°, en projet (article 105, § 1er, alinéa 4, en projet);

– l'obligation selon laquelle le réseau mobile d'un "Mobile Network Operator" d'une génération ultérieure à la quatrième génération doit se trouver sur le territoire de l'Union européenne et être géré, exploité, configuré et supervisé à partir de ce territoire (article 105, § 1er, alinéa 5, en projet); l'avant-projet prévoit la possibilité d'étendre la même obligation à d'autres catégories d'entreprises (article 105, § 2, 5°, en projet);

– la possibilité d'imposer l'obtention d'une autorisation préalable pour pouvoir bénéficier de services de "fournisseurs" – qui ne sont donc pas nécessairement des fournisseurs à "haut risque" – intervenant ponctuellement dans la gestion du réseau (article 105, § 2, 3°, en projet);

– l'obligation de disposer d'une autorisation préalable en cas de mise à jour d'un logiciel ou d'un dispositif matériel relatif à un élément du réseau (article 105, § 2, 4°, en projet);

‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp‡, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

Algemene opmerkingen

1.1. Bij voorliggend voorontwerp worden verschillende beperkingen opgelegd in het kader van de uitrol van de netwerken en de exploitatie van de mobiele technologieën van de vijfde generatie, namelijk:

– de verplichting voor de "Mobile Network Operators" om over een voorafgaande machtiging te beschikken om bepaalde elementen van hun netwerk te mogen gebruiken (ontworpen artikel 105, § 1, eerste lid); het voorontwerp voorziet in de mogelijkheid om die verplichting uit te breiden naar andere categorieën van ondernemingen (ontworpen artikel 105, § 2, 1° en 2°);

– de verplichting om een verzoek om regularisatie in te dienen ingeval bepaalde netwerkelementen van de "Mobile Network Operators" reeds daadwerkelijk gebruikt worden op het ogenblik dat het koninklijk besluit bedoeld in het ontworpen artikel 105, § 4, eerste lid, 1°, in werking treedt (ontworpen artikel 105, § 1, vierde lid);

– de verplichting dat het mobiele netwerk van een "Mobile Network Operator" van een latere generatie dan de vierde zich op het grondgebied van de Europese Unie moet bevinden en vanaf dat grondgebied beheerd, geëxploiteerd, geconfigureerd en gemonitord moet worden (ontworpen artikel 105, § 1, vijfde lid); het voorontwerp voorziet in de mogelijkheid om dezelfde verplichting uit te breiden tot andere categorieën van ondernemingen (ontworpen artikel 105, § 2, 5°);

– de mogelijkheid om voor te schrijven dat een voorafgaande machtiging verkregen moet worden om gebruik te kunnen maken van diensten van "aanbieders" – die dus niet noodzakelijk aanbieders zijn die een "hoog risico" vormen – die gericht tussenbeide komen in het beheer van het netwerk (ontworpen artikel 105, § 2, 3°);

– de verplichting om over een voorafgaande machtiging te beschikken in geval van een update van software of hardware met betrekking tot een netwerkelement (ontworpen artikel 105, § 2, 4°);

‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

– la mise en place de restrictions concernant l'utilisation d'éléments de réseau ou de services de "fournisseurs à haut risque" sur l'ensemble du territoire national ou dans des "zones sensibles" de ce territoire encore à déterminer (article 105, § 4, alinéa 1er, 1°, en projet);

– la mise en place de restrictions concernant la "localisation des éléments de réseaux ou du fournisseur" (article 105, § 4, alinéa 1er, 2°, en projet).

Ces mesures limitent principalement la liberté d'entreprise, la liberté de circulation des marchandises, la liberté de circulation des services et l'usage libre des biens, garantis, selon le cas, par la Constitution, le droit européen et le droit international.

De telles restrictions ne sont admissibles que dans la mesure où elles poursuivent des motifs d'intérêt général, reposent sur des critères objectifs, non discriminatoires et connus à l'avance, sont appropriées à la réalisation de l'objectif invoqué et sont nécessaires à la poursuite de cet objectif.

1.2. Ceci appelle les observations suivantes.

1.3. S'il peut être admis que les intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 'relative à la classification et aux habilitations, attestations et avis de sécurité', évoqués notamment à l'article 105, § 1er, alinéa 1er, en projet, peuvent, selon les circonstances de l'espèce, constituer de tels motifs d'intérêt général, l'avant-projet à l'examen est en défaut, dans certaines de ses dispositions, de circonscrire suffisamment le régime qu'il instaure à la poursuite de ces objectifs et de garantir la proportionnalité des mesures envisagées.

De même, à certains égards, la prévisibilité[1] du régime mis en place n'est pas garantie à suffisance. Cette prévisibilité, qui contribue, au demeurant à s'assurer de la proportionnalité des restrictions envisagées permet, plus fondamentalement, de garantir le respect du principe de légalité des incriminations, qui résulte notamment de l'article 7 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. En effet, dès lors que les manquements aux obligations imposées par le texte en projet ou aux décisions prises en vertu de celui-ci sont susceptibles de faire l'objet de sanctions, notamment d'amendes administratives susceptibles d'être qualifiées de pénales au sens de cette Convention, le principe de légalité des incriminations rappelé ci-avant trouve à s'appliquer.

[1] Sur ce dernier point, il est rappelé que pour des raisons de sécurité juridique, de prévisibilité de la norme et d'égalité de traitement, il convient en outre que les termes utilisés dans l'avant-projet, en particulier ceux en rapport avec son champ d'application et les restrictions qu'il prévoit, soient les plus compréhensibles possibles.

– het opleggen van beperkingen met betrekking tot het gebruik van netwerkelementen of diensten van "leveranciers die een hoog risico vormen" op heel het nationaal grondgebied of in nog te bepalen "gevoelige zones" van dat grondgebied (ontworpen artikel 105, § 4, eerste lid, 1°);

– het opleggen van beperkingen met betrekking tot de "lokalisatie van de netwerkelementen of van de leverancier" (ontworpen artikel 105, § 4, eerste lid, 2°).

Bij die maatregelen worden vooral beperkingen opgelegd aan de vrijheid van ondernemerschap, het vrije verkeer van goederen, het vrij verrichten van diensten en het vrije gebruik van goederen, die naargelang het geval door de Grondwet, het Europees recht en het internationaal recht gewaarborgd worden.

Dergelijke beperkingen kunnen slechts aanvaard worden voor zover daaraan redenen van algemeen belang ten grondslag liggen, ze op objectieve, niet-discriminerende en vooraf gekende criteria berusten, ze geschikt zijn om het aangevoerde doel te bereiken en nodig zijn om dat doel na te streven.

1.2. Dat alles geeft aanleiding tot de volgende opmerkingen.

1.3. Hoewel aanvaard kan worden dat de belangen vermeld in artikel 3, § 1, van de wet van 11 december 1998 'betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen', waarnaar inzonderheid in het ontworpen artikel 105, § 1, eerste lid, verwezen wordt, naargelang van de omstandigheden van het concrete geval dergelijke redenen van algemeen belang kunnen zijn, wordt in een aantal bepalingen van voorliggend voorontwerp niet duidelijk genoeg omschreven welke regeling daarbij ingevoerd wordt met het oog op het nastreven van die doelen en het garanderen van de proportionaliteit van de voorgenomen maatregelen.

Zo ook wordt de voorzienbaarheid[1] van de ingevoerde regeling in bepaalde opzichten niet voldoende gewaarborgd. Die voorzienbaarheid, die er overigens toe bijdraagt dat men zich kan vergewissen van de proportionaliteit van de voorgenomen beperkingen, maakt het, wat nog belangrijker is, mogelijk de naleving te garanderen van het beginsel van de wettelijkheid van de strafbaarstellingen, welk beginsel voortvloeit uit inzonderheid artikel 7 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Het hierboven in herinnering gebrachte beginsel van de wettelijkheid van de strafbaarstellingen is immers van toepassing, aangezien op de niet-naleving van de verplichtingen die bij de ontworpen tekst opgelegd worden of van de beslissingen die krachtens die tekst genomen worden, sancties staan, meer bepaald administratieve geldboetes die bestempeld kunnen worden als strafrechtelijk in de zin van dat verdrag.

[1] Wat dat punt betreft, wordt erop gewezen dat het, ter wille van de rechtszekerheid, de voorzienbaarheid van de norm en de gelijkheid van behandeling, bovendien wenselijk is dat de termen die in het voorontwerp gebruikt worden, in het bijzonder die met betrekking tot het toepassingsgebied ervan en de beperkingen waarin het voorziet, zo bevattelijk mogelijk zijn.

À cet égard, il y a lieu de mentionner spécialement les difficultés suivantes:

1° L'article 105, § 4, alinéa 1er, 1° et 2°, en projet habilite le Roi, par arrêté délibéré en Conseil des ministres, à fixer des "restrictions" concernant "l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque" et "la localisation des éléments de réseaux ou du fournisseur". Cette disposition peut se comprendre comme habilitant le Roi à apporter différentes sortes de restrictions pour tout motif qu'il estimerait raisonnable, ce qui n'est pas de nature à assurer la proportionnalité des restrictions envisagées et ne parait pas, en outre, être conforme à l'intention de l'auteur de l'avant-projet. La difficulté pointée pourrait être levée en complétant la disposition à l'examen de sorte qu'il apparaisse que les "restrictions" que le Roi est habilité à fixer ne peuvent l'être qu'en vue de garantir les intérêts visés au paragraphe 1er, alinéa 1er, de l'article 105 en projet.

2° Le régime mis en place n'est pas d'application, notamment, pour les points de terminaison du réseau qui n'émettent pas de "signaux radioélectriques de service mobile 5G" et exclut les "réseaux mobiles de quatrième génération et des générations antérieures" (article 105, § 1er, alinéa 3, 2° et 3°, en projet). S'agissant de concepts clés dans la définition du champ d'application de l'avant- projet, il convient d'en délimiter les contours avec précision. Certes, l'exposé des motifs mentionne que "[l]a présente loi vise les réseaux mobiles de cinquième génération (5G). Plutôt que de définir ces termes, ce qui pourrait créer certaines discussions, il a été choisi de faire référence à la 5G en excluant les réseaux mobiles de quatrième génération et des générations antérieures". Toutefois, l'absence même de définition parait, en soi, plus de nature à entrainer une insécurité juridique qu'une définition dont les termes pourraient créer des discussions. La définition du champ d'application du texte en projet sera en conséquence revue.

3° La notion de "réseaux privés mobiles" employée à l'article 105, § 2, 2°, en projet n'est pas définie.

4° Dans la version française, la notion de "dispositif matériel relatif à un élément de réseau", employée à l'article 105, § 2, 4°, en projet manque de clarté; mieux vaut préciser qu'il s'agit d'un "dispositif matériel d'un système informatique constituant un élément de réseau"[2].

5° L'article 105, § 4, alinéa 1er, en projet permet aux ministres compétents de revoir d'initiative l'autorisation qui a été octroyée, "en raison d'un nouvel élément". Cette formulation manque de précision. L'avant-projet sera revu aux fins de préciser la nature de ce nouvel élément ou le contexte dans lequel il

[2] La version néerlandaise utilise en effet la notion de "hardware".

In dat verband moet inzonderheid melding gemaakt worden van de volgende moeilijkheden:

1° Bij het ontworpen artikel 105, § 4, eerste lid, 1° en 2°, wordt de Koning gemachtigd om bij een besluit vastgesteld na overleg in de Ministerraad beperkingen vast te stellen met betrekking tot "het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen" en "de lokalisatie van de netwerkelementen of van de leverancier". Die bepaling kan aldus opgevat worden dat daarbij de Koning gemachtigd wordt om verscheidene soorten beperkingen op te leggen om elke reden die hij redelijk zou achten, waarmee niet gegarandeerd kan worden dat de voorgenomen beperkingen proportioneel zijn, en die bepaling is bovendien blijkbaar niet in overeenstemming met de bedoeling van de steller van het voorontwerp. De moeilijkheid waarop zopas gewezen is, zou verholpen kunnen worden door de voorliggende bepaling aldus aan te vullen dat daaruit blijkt dat de "beperkingen" tot het opleggen waarvan de Koning gemachtigd wordt, alleen opgelegd mogen worden om de belangen te waarborgen waarnaar in paragraaf 1, eerste lid, van het ontworpen artikel 105 verwezen wordt.

2° De regeling die ingevoerd wordt, is onder meer niet van toepassing voor de netwerkaansluitpunten die geen "mobiele-dienstradiosignalen 5G" uitzenden, terwijl de "mobiele netwerken van de vierde generatie en [van] vroegere generaties" daar niet onder vallen (ontworpen artikel 105, § 1, derde lid, 2° en 3°). Aangezien dat sleutelbegrippen zijn voor het afbakenen van het toepassingsgebied van het voorontwerp, dient nauwkeurig bepaald te worden wat daaronder valt. In de memorie van toelichting wordt weliswaar vermeld dat "[d]e onderhavige wet (…) op de mobiele netwerken van de vijfde generatie (5G) [doelt]. In plaats van deze termen te definiëren, wat bepaalde discussies zou kunnen doen ontstaan, is ervoor geopteerd om naar 5G te verwijzen door de mobiele netwerken van de vierde generatie en vroegere generaties uit te sluiten." Het ontbreken zelf van een definitie lijkt evenwel op zich veeleer van dien aard dat ze tot rechtsonzekerheid leidt dan een definitie waarvan de bewoordingen discussies zouden kunnen doen ontstaan. De bepaling van het toepassingsgebied van de ontworpen tekst moet bijgevolg herzien worden.

3° Er wordt geen definitie gegeven van het begrip "private mobiele netwerken" dat in het ontworpen artikel 105, § 2, 2°, gebruikt wordt.

4° Het begrip "dispositif matériel relatif à un élément de réseau" dat in de Franse tekst van het ontworpen artikel 105, § 2, 4°, gebruikt wordt, is onduidelijk; het zou beter zijn te preciseren dat het gaat om een "dispositif matériel d'un système informatique constituant un élément de réseau".[2]

5° Het ontworpen artikel 105, § 4, eerste lid, biedt de bevoegde ministers de mogelijkheid om de verleende machtiging op eigen initiatief te herzien "wegens een nieuw element". Die formulering laat qua duidelijkheid te wensen over. Het voorontwerp moet aldus herzien worden dat daarin de aard van

[2] In de Nederlandse tekst wordt immers het begrip "hardware" gebruikt.

s'insère, par exemple en se référant aux conditions qui ont été examinées dans le cadre de l'octroi de l'autorisation.

6° L'article 105, § 4, alinéa 1er, 2°, en projet habilite le Roi à arrêter des restrictions concernant "la localisation des éléments de réseaux ou du fournisseur". La section de législation n'aperçoit pas la portée exacte de la notion de "localisation du fournisseur", dont le texte ne mentionne pas qu'il est ou serait "à haut risque". L'exposé des motifs ne comporte aucune explication à ce propos. S'il y a lieu de considérer que l'habilitation ainsi envisagée permet au Roi de restreindre la possibilité de faire usage des éléments de réseau ou des services d'un fournisseur qui ne serait pas à haut risque, en fonction de son unique "localisation", des réserves sérieuses doivent être émises quant à l'admissibilité de cette restriction au regard du principe d'égalité et de non-discrimination et du principe de proportionnalité.

7° Les critères qui permettent d'évaluer le "profil de risque" des fournisseurs (article 105, § 4, alinéa 3, en projet) gagneraient à être davantage précisés. Il en va ainsi pour les critères en projet ayant vocation à démontrer la "probabilité d'ingérence" comme pour les termes de "lien fort", de "gouvernement"[3], de "situation", de "contrôle démocratique ou législatif", de "caractéristiques de la propriété d'entreprise du fournisseur", d'"exercer toute forme de pression", le "pays originaire" du fournisseur, et de "mène ou est associé à une politique cyber offensive".

1.4. L'avant-projet sera revu, complété et précisé à la lumière des observations qui précèdent.

2. Suivant l'article 105, § 1er, alinéa 1er, en projet, l'autorisation que les "Mobile Network Operator" doivent obtenir avant "d'utiliser un élément de leur réseau" est délivrée par les "ministres concernés", à savoir le premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères.

Cependant, à la lecture de l'avant-projet, la nature de cette autorisation et le degré d'intervention des ministres concernés dans sa conception sont incertains: faut-il considérer que cette autorisation est constituée de six actes juridiques distincts devant chacun être adopté par les ministres à titre individuel selon une procédure distincte ou bien s'agit-il d'un seul et unique acte juridique auquel les ministres concernés doivent formellement consentir dans le cadre d'une seule et même procédure?

[3] Ne faut-il pas viser les "autorités publiques" plutôt que le seul "gouvernement"?

dat nieuw element of de context waarvan het deel uitmaakt, verduidelijkt wordt, bijvoorbeeld door te verwijzen naar de voorwaarden die onderzocht zijn in het kader van het verlenen van de machtiging.

6° Bij het ontworpen artikel 105, § 4, eerste lid, 2°, wordt de Koning gemachtigd om beperkingen vast te stellen met betrekking tot "de lokalisatie van de netwerkelementen of van de leverancier". Het is de afdeling Wetgeving niet duidelijk wat de precieze draagwijdte is van het begrip "lokalisatie van de leverancier", aangezien de tekst niet vermeldt of de leverancier "een hoog risico" vormt of zou kunnen vormen. In de memorie van toelichting wordt daaromtrent geen enkele uitleg gegeven. Indien ervan uitgegaan moet worden dat de aldus in het vooruitzicht gestelde machtiging de Koning in staat stelt de mogelijkheid te beperken om gebruik te maken van de netwerkelementen of van de diensten van een leverancier die op basis van zijn unieke "lokalisatie" geen hoog risico zou vormen, moet ernstig voorbehoud gemaakt worden bij de aanvaardbaarheid van die beperking in het licht van het gelijkheids- en non-discriminatiebeginsel en het proportionaliteitsbeginsel.

7° De criteria op basis waarvan het "risicoprofiel" van de leveranciers (ontworpen artikel 105, § 4, derde lid) beoordeeld kan worden, zouden nader gepreciseerd moeten worden. Dat geldt voor de ontworpen criteria waarvan het de bedoeling is dat daarmee aangetoond wordt hoe groot de kans op inmenging is, zoals voor de woorden "sterke link", "regering",[3] "situatie", "democratische of wetgevende controle", "karakteristieken van de eigendom van de onderneming van de leverancier", "enige vorm van pressie uit te oefenen", "het land waaruit de leverancier afkomstig is" en "voert of is betrokken bij een offensief cyberbeleid".

1.4. Het voorontwerp moet in het licht van de voorgaande opmerkingen herzien, aangevuld en verduidelijkt worden.

2. De machtiging die de "Mobile Network Operators" moeten verkrijgen alvorens "een element van hun netwerk te gebruiken", wordt volgens het ontworpen artikel 105, § 1, eerste lid, verleend door de "betrokken ministers", namelijk de eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken.

Het lezen van het voorontwerp verschaft evenwel geen duidelijkheid omtrent de aard van die machtiging en omtrent de mate waarin de betrokken ministers meewerken aan de totstandkoming ervan: moet ervan uitgegaan worden dat die machtiging bestaat uit zes afzonderlijke rechtshandelingen die elk volgens een afzonderlijke procedure op individuele basis door de ministers vastgesteld moeten worden of gaat het om één enkele rechtshandeling waarmee de betrokken ministers in het kader van één en dezelfde procedure formeel moeten instemmen?

[3] Moet niet naar de "overheid" verwezen worden in plaats van louter naar de "regering"?

Cette incertitude est de nature à entrainer de nombreuses difficultés de compréhension de l'avant-projet et, partant, une insécurité juridique. Ainsi, à titre d'illustration, les questions suivantes se posent:

– au stade du dépôt de la demande: une seule demande doit-elle être introduite, et dans ce cas, auprès de quel ministre?

– au stade du traitement du dossier de demande: en cas de pluralité de demandes à introduire, à partir du dépôt de quelle demande le délai de trois mois dans lequel la décision doit être prise, prend-il cours? De même, quel est le point de départ du délai de 28 jours laissé au demandeur pour formuler des observations écrites lorsque les ministres entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision d'initiative? Chacun des ministres doit-il traiter de manière individuelle le dossier et demander l'avis de l'IBPT et des services de renseignement?

L'avant-projet sera revu de manière à lever cette incertitude en clarifiant la nature de l'autorisation requise et les modalités d'adoption de la décision concernée.

Observations particulières

Dispositif

Article 2

À l'article 2 de l'avant-projet, il convient de remplacer les lettres et signes "X°" et "Y°" par, respectivement, les nombres "87°" et "88°"[4].

Articles 3 et 7

Article 105, § 1er, en projet

L'alinéa 4 en projet prévoit que les demandes de régularisation pour l'utilisation d'éléments de réseau doivent être introduites dans les deux mois qui suivent "la date d'entrée en vigueur de l'arrêté royal" devant déterminer, conformément à l'article 105, § 4, alinéa 1er, 1°, en projet, les restrictions concernant l'utilisation "d'éléments de réseau ou de services de fournisseurs à haut risque".

Or, l'article 7 de l'avant-projet prévoit que l'article 105, § 1er, alinéa 4, entre en vigueur le 1er janvier 2026.

[4] La numérotation des termes définis à l'article 2 de la loi du 13 juin 2005 'relative aux communications électroniques' s'arrête au 86°, en l'état des textes publiés au Moniteur belge à ce jour.

Door die onduidelijkheid zijn veel bepalingen van het voorontwerp moeilijk te begrijpen en ontstaat er bijgevolg rechtsonzekerheid. Zo rijzen bijvoorbeeld de volgende vragen:

– in het stadium van de indiening van het verzoek: moet één enkel verzoek ingediend worden en, zo ja, bij welke minister?

– in het stadium van de behandeling van het aanvraagdossier: ingeval verscheidene verzoeken ingediend moeten worden, vanaf de indiening van welk verzoek gaat dan de termijn van drie maanden in waarbinnen de beslissing genomen moet worden? Zo ook rijst de vraag wanneer de termijn van 28 dagen ingaat waarover de verzoeker beschikt om schriftelijke opmerkingen te formuleren, wanneer de ministers van plan zijn de machtiging te weigeren, daaraan voorwaarden te koppelen of hun beslissing op eigen initiatief te herzien? Moet elk van de betrokken ministers afzonderlijk het dossier behandelen en het advies van het BIPT en de inlichtingendiensten aanvragen?

Het voorontwerp moet aldus herzien worden dat die onduidelijkheid weggenomen wordt door de aard van de vereiste machtiging en de nadere regels inzake het nemen van de betrokken beslissing te verduidelijken.

Bijzondere opmerkingen

Dispositief

Artikel 2

In artikel 2 van het voorontwerp dienen de letters en tekens "X°" en "Y°" respectievelijk vervangen te worden door de getallen "87°" en "88°".[4]

Artikelen 3 en 7

Ontworpen artikel 105, § 1

Volgens het ontworpen vierde lid dienen de verzoeken om regularisatie voor het gebruik van netwerkelementen ingediend te worden in de twee maanden die volgen op "de datum van inwerkingtreding van het koninklijk besluit" waarbij overeenkomstig het ontworpen artikel 105, § 4, eerste lid, 1°, vastgesteld moet worden welke beperkingen gelden voor het gebruik "van netwerkelementen of van diensten van leveranciers die een hoog risico vormen".

Luidens artikel 7 van het voorontwerp wordt artikel 105, § 1, vierde lid, evenwel pas van kracht op 1 januari 2026.

[4] Bij de huidige stand van de teksten die tot op heden in het Belgisch Staatsblad bekendgemaakt zijn, houdt de nummering van de termen die in artikel 2 van de wet van 13 juni 2005 'betreffende de elektronische communicatie' gedefinieerd worden op bij de bepaling onder 86°.

Il résulte d'une lecture combinée de ces dispositions que cet arrêté royal doit nécessairement entrer en vigueur après que soit entré en vigueur l'article 105, § 1er, alinéa 4, en projet à défaut de quoi les opérateurs visés ne pourront pas valablement introduire de demande de régularisation.

Il appartient à l'auteur de l'avant-projet de vérifier si telle est son intention et, le cas échéant, de revoir l'articulation de ces dispositions.

Article 3

Article 105, § 2, en projet

Le 2° en projet habilite le Roi à charger une ou plusieurs autorités, non autrement identifiées, de désigner "les fournisseurs" soumis à l'obligation d'obtenir l'autorisation des différents ministres concernés dont il est question à l'article 105, § 1er, en projet.

Le texte en projet ne permet pas de comprendre clairement si le pouvoir de déterminer ces "fournisseurs" comprend la fixation de règles générales, auquel cas il s'agirait d'une compétence réglementaire, ou s'il s'agit plutôt de désigner, de manière individuelle, les fournisseurs en question, en tenant compte des intérêts repris à l'article 3, § 1er, de la loi du 11 décembre 1998.

Dans ce cadre, il y a lieu de rappeler que l'attribution d'un pouvoir réglementaire à une autorité, non autrement désignée, qui n'est pas politiquement responsable devant une assemblée démocratiquement élue n'est en principe pas admissible, dès lors qu'elle porte atteinte au principe de l'unité du pouvoir réglementaire et à celui de la responsabilité politique des ministres. Une telle délégation ne pourrait être acceptée que s'il s'agissait de mesures ayant une portée limitée et technique, ce qui ne serait pas le cas s'il y a lieu d'interpréter la délégation en cause comme permettant à ces autorités de désigner des catégories de fournisseurs devant être soumises à l'obligation de recueillir l'autorisation des ministres concernés. La délégation d'un tel pouvoir réglementaire n'est dès lors pas admissible à l'égard de ces autorités non autrement identifiées.

Si telle n'est pas l'intention de l'auteur de l'avant-projet, il convient d'exprimer plus clairement que la délégation portera uniquement sur un pouvoir de décision individuelle selon des critères précis qui seront fixés préalablement dans le texte en projet ou par voie d'habilitation au Roi, à portée réglementaire.

La disposition en projet sera revue en conséquence.

Uit het in onderling verband lezen van die bepalingen blijkt dat het koninklijk besluit in kwestie uit de aard der zaak pas in werking mag treden na de inwerkingtreding van het ontworpen artikel 105, § 1, vierde lid, aangezien de betrokken operatoren anders niet op geldige wijze een verzoek om regularisatie zullen kunnen indienen.

De steller van het voorontwerp dient na te gaan of dat wel zijn bedoeling is en in voorkomend geval de onderlinge afstemming tussen die bepalingen te herzien.

Artikel 3

Ontworpen artikel 105, § 2

Luidens de ontworpen bepaling onder 2° kan de Koning een of meer, niet nader genoemde, autoriteiten ermee belasten "de aanbieders" aan te wijzen die onderworpen zijn aan de verplichting om van alle betrokken ministers de machtiging te verkrijgen waarvan in het ontworpen artikel 105, § 1, sprake is.

Uit de ontworpen tekst blijkt niet duidelijk of de bevoegdheid om te bepalen wie die "aanbieders" zijn de bevoegdheid omvat om ter zake algemene regels vast te stellen, in welk geval het om een verordenende bevoegdheid zou gaan, dan wel of het veeleer de bedoeling is de aanbieders in kwestie op individuele basis aan te wijzen, rekening houdend met de belangen vermeld in artikel 3, § 1, van de wet van 11 december 1998.

In dit verband dient eraan herinnerd te worden dat in principe niet aanvaard kan worden dat een regelgevende bevoegdheid toegekend wordt aan een niet nader genoemde autoriteit die geen politieke verantwoordelijkheid draagt ten aanzien van een democratisch verkozen vergadering, omdat aldus afbreuk gedaan wordt aan het beginsel van de eenheid van de verordenende macht en aan het beginsel van de politieke verantwoordelijkheid van de ministers. Een dergelijke delegatie zou alleen aanvaard kunnen worden wanneer het gaat om maatregelen met een beperkte en technische draagwijdte, wat niet het geval zou zijn indien de delegatie in kwestie aldus uitgelegd dient te worden dat die autoriteiten op grond daarvan categorieën aanbieders mogen aanwijzen voor wie de verplichting moet gelden om van de betrokken ministers de machtiging te verkrijgen. Dat een dergelijke regelgevende bevoegdheid aan die niet nader genoemde autoriteiten toegekend wordt, kan derhalve niet aanvaard worden.

Als zulks niet de bedoeling van de steller van het voorontwerp is, dient duidelijker tot uiting gebracht te worden dat de toe te kennen bevoegdheid beperkt blijft tot de bevoegdheid om individuele beslissingen te nemen volgens duidelijke criteria die vooraf vastgesteld zijn in de thans ontworpen tekst of door middel van een aan de Koning verleende machtiging van regelgevende aard.

De ontworpen bepaling moet dienovereenkomstig herzien worden.

Article 105, § 3, en projet

1. À l'alinéa 3 en projet, il y a lieu de faire référence au paragraphe 4, "alinéa 5", et non "alinéa 4".

2. Les modalités d'introduction et du traitement de la demande n'étant pas précisées dans le texte en projet, il se recommande, à l'instar de ce qui a été fait pour la composition du dossier, d'habiliter le Roi à les fixer.

3. Suivant l'alinéa 4 en projet, il apparait que les services de renseignement, qui interviennent au même titre que l'IBPT dans le cadre de l'instruction de la demande en formulant un avis, ne disposent pas, contrairement à l'IBPT, de la possibilité de demander des renseignements complémentaires.

L'auteur de l'avant-projet vérifiera si cela est conforme à son intention et, le cas échéant, adaptera l'alinéa 4 en projet en conséquence.

Article 105, § 4, en projet

1. L'alinéa 2 en projet prévoit que, lorsqu'ils "revoient leur décision d'initiative", les ministres peuvent fixer une date de mise en œuvre de la nouvelle décision "qui est postérieure par rapport aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification".

Il ressort de cette disposition que le Roi serait dès lors habilité à fixer des délais dans lesquels les restrictions envisagées devront être mises en œuvre lorsqu'ils attribuent les autorisations initiales, ce qui ne ressort ni de l'alinéa 1er, ni de l'exposé des motifs.

L'alinéa 1er sera revu afin de mieux faire ressortir cette habilitation et les critères au moyen desquels les délais seront fixés.

2. Afin de se concilier avec l'intention exprimée dans l'exposé des motifs, l'alinéa 3 sera complété en indiquant qu'il n'est pas requis que plusieurs critères parmi les trois critères énumérés soient rencontrés pour qu'un fournisseur puisse être qualifié comme étant "à haut risque".

3. L'alinéa 6 confie au Conseil national de sécurité un pouvoir réglementaire consistant en l'identification des "zones sensibles" au sein desquelles les fournisseurs qualifiés comme étant "à haut risque" ne pourront ni fournir des éléments de réseaux ni prester des services.

Dès lors que la Constitution a attribué exclusivement au Roi le pouvoir réglementaire revenant au pouvoir exécutif fédéral et que les pouvoirs doivent être exercés de la manière déterminée par la Constitution, le principe de l'unité du pouvoir réglementaire s'applique et il est par conséquent exclu

Ontworpen artikel 105, § 3

1. In het ontworpen derde lid dient naar het "vijfde lid" van paragraaf 4 verwezen te worden, en niet naar het "vierde lid" ervan.

2. Aangezien in de ontworpen tekst niet vermeld wordt volgens welke nadere regels het verzoek ingediend en behandeld moet worden, verdient het aanbeveling om, zoals dat voor de samenstelling van het dossier gedaan is, de Koning te machtigen dat te bepalen.

3. Uit het ontworpen vierde lid blijkt dat de inlichtingendiensten, die net zoals het BIPT betrokken zijn bij het onderzoek van het verzoek, aangezien zij in dat kader een advies uitbrengen, in tegenstelling tot het BIPT niet over de mogelijkheid beschikken om aanvullende inlichtingen te vragen.

De steller van het voorontwerp moet nagaan of dat overeenstemt met zijn bedoeling en moet in voorkomend geval het ontworpen vierde lid dienovereenkomstig herzien.

Ontworpen artikel 105, § 4

1. Luidens het ontworpen tweede lid kunnen de ministers, wanneer zij "op eigen initiatief hun beslissing herzien", een datum van uitvoering van de nieuwe beslissing vastleggen "die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt".

Uit die bepaling blijkt dat de Koning bijgevolg gemachtigd zou zijn om, wanneer zij de oorspronkelijke machtigingen toekennen, de termijnen vast te stellen waarbinnen de in het vooruitzicht gestelde beperkingen ten uitvoer gelegd moeten worden, wat niet blijkt uit het eerste lid, noch uit de memorie van toelichting.

Het eerste lid moet aldus herzien worden dat die machtiging duidelijker tot uiting komt en er moet bepaald worden op basis van welke criteria die termijnen vastgesteld dienen te worden.

2. Met het oog op de overeenstemming met de bedoeling die in de memorie van toelichting geuit wordt, moet het derde lid aangevuld worden met de vermelding dat niet vereist is dat voldaan is aan meer dan één van de drie daarin vermelde criteria opdat een leverancier geacht kan worden "een hoog risico te vormen".

3. Bij het zesde lid wordt aan de Nationale Veiligheidsraad een verordenende bevoegdheid toegekend, die erin bestaat de "gevoelige zones" aan te wijzen waarbinnen de leveranciers die geacht worden "een hoog risico te vormen" noch netwerkelementen mogen leveren, noch diensten mogen verrichten.

Doordat de Grondwet de aan de federale uitvoerende macht toekomende verordenende bevoegdheid alleen aan de Koning toegekend heeft en de machten uitgeoefend dienen te worden op de wijze bij de Grondwet bepaald, geldt het beginsel van de eenheid van de verordenende macht, zodat uitgesloten is

que le pouvoir réglementaire soit exercé d'une autre manière que celle prescrite par la Constitution. Dès lors, le législateur fédéral ne peut en principe déléguer des compétences normatives qu'au Roi.

Cette règle vaut d'autant plus en l'espèce que le Conseil national de sécurité est un organe stratégique et de coordination, ne disposant pas de pouvoir de décision propre, qui a été créé par Roi sur la base de l'article 37 de la Constitution[5].

L'avant-projet sera revu en confiant au Roi le soin de déterminer les "zones sensibles".

4. S'agissant de la publicité à donner aux arrêtés fixant le périmètre des "zones sensibles", l'alinéa 7 en projet est rédigé comme suit:

"Un opérateur peut consulter la liste des zones sensibles auprès de l'Institut, s'il peut justifier qu'il a besoin d'en connaitre".

Cette disposition soulève deux difficultés.

4.1.1. Selon l'article 190 de la Constitution, "[a]ucune loi, aucun arrêté ou règlement d'administration générale, provinciale ou communale, n'est obligatoire qu'après avoir été publié dans la forme déterminée par la loi".

La détermination des périmètres des zones sensibles, qui, comme en l'espèce, conditionnent la mise en œuvre d'un régime juridique précis à l'égard des tiers, ne constitue pas en soi un acte réglementaire au sens de l'article 3 des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973. Elle n'en est pas moins un arrêté ou un règlement d'administration générale au sens de l'article 190 de la Constitution, par opposition aux actes à portée individuelle[6].

La liste de ces zones et de leurs périmètres doit dès lors faire l'objet d'une publicité suffisante à l'égard des tiers, à défaut de quoi celles-ci ne pourront sortir d'effets à leur égard, spécialement, en l'occurrence, à l'égard des opérateurs.

4.1.2. Contrairement au prescrit de l'article 6 de la loi du 31 mai 1961 'relative à l'emploi des langues en matière législative, à la présentation, à la publication et à l'entrée en vigueur des textes légaux et réglementaires', il ressort du texte en projet que la liste des zones sensibles et de leurs périmètres ne fera pas l'objet d'une publication au Moniteur belge, ne serait-ce que par extrait ou par mention, à l'instar de ce que prévoit l'article 56, § 1er, alinéa 4, des lois 'sur

dat de verordenende macht op een andere wijze uitgeoefend wordt dan door de Grondwet voorgeschreven is. In beginsel mag de federale wetgever derhalve alleen aan de Koning normatieve bevoegdheden delegeren.

Die regel geldt in casu des te meer daar de Nationale Veiligheidsraad een strategisch en coördinerend orgaan is, dat niet over een eigen beslissingsbevoegdheid beschikt en door de Koning opgericht is op grond van artikel 37 van de Grondwet.[5]

Het voorontwerp moet aldus herzien worden dat aan de Koning de taak opgedragen wordt de "gevoelige zones" te bepalen.

4. In verband met de ruchtbaarheid die gegeven mag worden aan de besluiten waarbij de grenzen van de "gevoelige zones" bepaald worden, wordt in het ontworpen zevende lid het volgende voorgeschreven:

"Een operator kan de lijst met de gevoelige zones raadplegen bij het Instituut indien hij kan aantonen dat het voor hem noodzakelijk is om er kennis van te nemen."

Die bepaling doet twee moeilijkheden rijzen.

4.1.1. Krachtens artikel 190 van de Grondwet is "[g]een wet, geen besluit of verordening van algemeen, provinciaal of gemeentelijk bestuur (…) verbindend dan na te zijn bekendgemaakt in de vorm bij de wet bepaald".

De bepaling van de grenzen van de gevoelige zones, die in casu een voorwaarde zijn om ten aanzien van derden een specifieke juridische regeling toe te passen, vormt op zich geen verordenende handeling in de zin van artikel 3 van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973. Die handeling is niettemin een besluit of verordening van algemeen bestuur in de zin van artikel 190 van de Grondwet en valt dus geenszins onder de handelingen met individuele strekking.[6]

Aan de lijst van die zones en van de grenzen ervan moet ten aanzien van derden dan ook voldoende bekendheid gegeven worden, aangezien ze anders ten aanzien van die derden, en in casu in het bijzonder ten aanzien van de operatoren, geen gevolgen kunnen hebben.

4.1.2. Anders dan voorgeschreven wordt in artikel 6 van de wet van 31 mei 1961 'betreffende het gebruik der talen in wetgevingszaken, het opmaken, bekendmaken en inwerkingtreden van wetten en verordeningen', vloeit uit de ontworpen tekst voort dat de lijst van de gevoelige zones en van de grenzen ervan, blijkens de ontworpen tekst, niet bekendgemaakt zal worden in het Belgisch Staatsblad, zelfs niet bij uittreksel of bij vermelding, zoals voorgeschreven in artikel 56, § 1, vierde lid,

---

5 Voir l'arrêté royal du 22 décembre 2020 'portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité'.

6 Voir, en ce sens, notamment, C.E. (13e ch.), 10 aout 2001, n° 98.248, Beckers et csrts.

5 Zie het koninklijk besluit van 22 december 2020 'tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid'.

6 Zie, in die zin, onder andere, RvS (13e k.), 10 augustus 2001, nr. 98.248, Beckers et al.

l'emploi des langues en matière administrative', coordonnées le 18 juillet 1966[7].

Interrogée sur l'intention de l'auteur de l'avant-projet à cet égard, la déléguée de la Ministre a confirmé et expliqué ce qui suit:

"Il n'est pas prévu de publier la liste des zones sensibles au Moniteur belge dès lors qu'elle contient des informations sensibles qui pourraient être utilisées à des fins de malveillance par des acteurs afin de porter atteinte aux intérêts énumérés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Toutefois, pour que les opérateurs qui sont soumis à l'obligation de l'autorisation préalable, en l'occurrence les MNOs, puissent introduire leur dossier auprès des ministres en connaissance de cause, l'article 105, § 4, al. 7, prévoit qu'ils pourront consulter la liste en question dans les locaux de l'IBPT au cas où ils en ont besoin. Ainsi, les opérateurs de téléphonie mobile, qui sont les seuls pour qui la publication est réellement utile, pourront avoir accès à la liste en question".

Cette explication parait pouvoir, à priori, justifier, au regard du principe d'égalité, la non-publication, in extenso, des arrêtés concernés au Moniteur belge. Par contre, une publication de ces arrêtés par voie de mention au Moniteur belge parait compatible avec le but légitime poursuivi par la disposition à l'examen.

La disposition sera revue de manière à assurer une publicité suffisante de ces arrêtés à l'égard des tiers.

4.2. Par ailleurs, il y a lieu d'avoir égard à l'article 32 de la Constitution qui dispose:

"Chacun a le droit de consulter chaque document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134".

En l'occurrence, la disposition à l'examen déroge à trois égards au droit concerné:

– elle entend limiter l'accès à la liste des zones sensibles aux seuls opérateurs;

– ceux-ci ne disposent pas du droit de se faire remettre copie de la liste, mais uniquement de la consulter;

van de wetten 'op het gebruik van de talen in bestuurszaken', gecoördineerd op 18 juli 1966.[7]

Naar aanleiding van een vraag over de bedoeling van de steller van het voorontwerp in dit verband heeft de gemachtigde van de minister de volgende bevestigende uitleg verstrekt:

"Il n'est pas prévu de publier la liste des zones sensibles au Moniteur belge dès lors qu'elle contient des informations sensibles qui pourraient être utilisées à des fins de malveillance par des acteurs afin de porter atteinte aux intérêts énumérés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Toutefois, pour que les opérateurs qui sont soumis à l'obligation de l'autorisation préalable, en l'occurrence les MNOs, puissent introduire leur dossier auprès des ministres en connaissance de cause, l'article 105, § 4, al. 7, prévoit qu'ils pourront consulter la liste en question dans les locaux de l'IBPT au cas où ils en ont besoin. Ainsi, les opérateurs de téléphonie mobile, qui sont les seuls pour qui la publication est réellement utile, pourront avoir accès à la liste en question."

Op het eerste gezicht lijkt met die uitleg in het licht van het gelijkheidsbeginsel verantwoord te kunnen worden waarom de besluiten in kwestie niet in extenso in het Belgisch Staatsblad bekendgemaakt zouden worden. Het lijkt evenwel verenigbaar met het legitiem doel dat met de voorliggende bepaling nagestreefd wordt om die besluiten louter bij vermelding in het Belgisch Staatsblad bekend te maken.

Deze bepaling moet aldus herzien worden dat ervoor gezorgd wordt dat die besluiten genoegzaam aan derden bekendgemaakt worden.

4.2. Daarenboven dient aandacht geschonken te worden aan artikel 32 van de Grondwet, dat als volgt luidt:

"Ieder heeft het recht elk bestuursdocument te raadplegen en er een afschrift van te krijgen, behoudens in de gevallen en onder de voorwaarden bepaald door de wet, het decreet of de regel bedoeld in artikel 134."

In casu wordt met deze ontworpen bepaling in drie opzichten afgeweken van het recht in kwestie:

– deze bepaling strekt ertoe alleen aan de operatoren inzage te verlenen in de lijst met de gevoelige zones;

– de operatoren beschikken niet over het recht om van die lijst een afschrift te krijgen, maar alleen over het recht om ze te mogen raadplegen;

[7] Cette disposition prévoit notamment que "[l]es arrêtés royaux et ministériels bilingues sont publiés intégralement par la voie du *Moniteur belge*, texte français et texte néerlandais en regard l'un de l'autre dans le mois de leur date. Néanmoins, lorsqu'ils n'intéressent pas la généralité des citoyens, ils peuvent n'être publiés que par extrait ou ne faire l'objet que d'une simple mention au *Moniteur belge*".

[7] In die bepaling wordt onder meer voorgeschreven dat "[d]e tweetalige koninklijke en ministeriële besluiten (…) integraal in het *Belgisch Staatsblad* bekendgemaakt [worden], de Nederlandse tekst tegenover de Franse, binnen één maand van hun dagtekening. Nochtans wanneer zij geen belang hebben voor de meerderheid van de burgers, mogen zij bij uittreksel bekendgemaakt worden of het voorwerp zijn van een gewone vermelding in het *Belgisch Staatsblad*".

– les opérateurs doivent justifier du “besoin d’en connaitre”.

Si l’article 32 de la Constitution habilite le législateur concerné à prévoir des cas dans lesquels le droit de consulter chaque document administratif et de s’en faire remettre copie ne s’applique pas, les exceptions ainsi mises en place doivent, dans le respect du principe d’égalité, poursuivre un but légitime et demeurer proportionnées au but légitime poursuivi.

La loi du 11 avril 1994 ‘relative à la publicité de l’administration’, qui organise le régime général d’accès aux documents administratifs, prévoit déjà des exceptions à l’accès à certains documents. Ainsi, l’article 6, § 1er, de cette loi dispose que l’autorité administrative rejette la demande de consultation, d’explication ou de communication sous la forme de copie d’un document administratif si elle a constaté que l’intérêt de la publicité ne l’emporte pas notamment sur la protection de la sécurité de la population ou de l’ordre public, ou encore, la sureté ou la défense nationales.

Cette disposition organise un système de refus au cas par cas de l’accès à un document administratif ou de la communication d’une copie de ce document, sans instituer un régime général d’interdiction à priori d’accès à une catégorie spécifique de documents ou de limitation à priori de l’accès d’un document déterminé à telles catégories de personnes. Un tel système de décision individuelle à posteriori permet de garantir la protection de la sécurité publique, de l’ordre public, et de la sureté et de la défense nationale. Un tel régime d’actes à portée individuelle susceptibles de recours, in fine auprès de la section du contentieux administratif du Conseil d’État, est ainsi de nature à garantir la proportionnalité des restrictions apportées au droit d’accès aux documents administratifs.

Pour sa part, le texte en projet restreint de manière radicale le droit à la transparence administrative en ce qui concerne la liste des zones sensibles, cette liste ne pouvant être consultée que par un opérateur, à la condition qu’il puisse “justifier qu’il a besoin d’en connaitre” et en excluant toute possibilité d’en prendre copie.

Il appartient à l’auteur de l’avant-projet d’être en mesure de démontrer que la différence de traitement qu’institue le dispositif à l’examen entre les personnes qui, parce qu’elles n’ont pas la qualité d’opérateur, se trouvent à priori exclues de toute possibilité de prendre connaissance de la liste des zones sensibles, et les personnes qui souhaitent prendre connaissance d’autres documents administratifs sensibles sur le plan de la sécurité publique, de l’ordre public, et de la sureté et de la défense nationale, auxquelles s’applique le système mis en place par la loi du 11 avril 1994, spécialement son article 6,

– de operatoren moeten aantonen “dat het voor hen noodzakelijk is om er kennis van te nemen”.

Hoewel de betrokken wetgever er bij artikel 32 van de Grondwet toe gemachtigd wordt te bepalen in welke gevallen het recht om elk bestuursdocument te raadplegen en daarvan een afschrift te krijgen niet geldt, moet met de uitzonderingen die aldus gemaakt worden, met inachtneming van het gelijkheidsbeginsel, een legitiem doel nagestreefd worden en moeten ze proportioneel blijven ten opzichte van het legitiem doel dat aldus nagestreefd wordt.

De wet van 11 april 1994 ‘betreffende de openbaarheid van bestuur’, die de algemene regeling inzake de toegang tot bestuursdocumenten bevat, voorziet reeds in uitzonderingen op de toegang tot bepaalde documenten. Zo wordt in artikel 6, § 1, van die wet bepaald dat de administratieve overheid de vraag om inzage in, uitleg over of mededeling van een afschrift van een bestuursdocument afwijst, wanneer zij vastgesteld heeft dat het belang van de openbaarheid niet opweegt tegen de bescherming van onder andere de veiligheid van de bevolking of de openbare orde, of nog de veiligheid of de verdediging van het land.

Bij die bepaling wordt een systeem ingesteld in het kader waarvan de toegang tot een bestuursdocument of de afgifte van een afschrift van dat document geval per geval geweigerd kan worden, maar wordt geen algemene regeling ingevoerd volgens welke het a priori verboden zou zijn toegang te verlenen tot een specifieke categorie documenten of volgens welke de toegang tot een welbepaald document a priori tot deze of gene categorie personen beperkt zou kunnen worden. Met een dergelijk systeem van a posteriori te nemen individuele beslissingen kan ervoor gezorgd worden dat de openbare veiligheid, de openbare orde en de veiligheid en de verdediging van het land beschermd worden. Een degelijke regeling, in het kader waarvan handelingen met individuele strekking gesteld kunnen worden waartegen in laatste instantie bij de afdeling Bestuursrechtspraak van de Raad van State beroep ingesteld kan worden, is aldus van dien aard dat daarmee de proportionaliteit gegarandeerd kan worden van de beperkingen die aan het recht op toegang tot bestuursdocumenten opgelegd worden.

In de ontworpen tekst, daarentegen, wordt het recht op bestuurlijke transparantie betreffende de lijst met de gevoelige zones op radicale wijze beperkt, aangezien, naar luid daarvan, alleen een operator die lijst mag raadplegen en dan nog op voorwaarde dat hij kan aantonen “dat het voor hem noodzakelijk is om er kennis van te nemen” en elke mogelijkheid om daarvan een afschrift te nemen uitgesloten is.

De steller van het voorontwerp moet kunnen aantonen dat de verschillende behandeling die bij voorliggend dispositief ingevoerd wordt tussen degenen voor wie het, omdat ze geen operator zijn, a priori volstrekt niet mogelijk is om van de lijst met de gevoelige zones kennis te nemen en degenen die kennis wensen te nemen van andere gevoelige bestuursdocumenten op het stuk van de openbare veiligheid, de openbare orde en de veiligheid en de verdediging van het land, die vallen onder de regeling die ingevoerd is bij de wet van 11 april 1994, en in het bijzonder bij de artikel 6 van die wet, op een redelijke

repose sur une justification objective et raisonnable rendant cette différence de traitement conforme au principe d'égalité[8].

À défaut, la disposition à l'examen sera revue.

4.3. Eu égard à l'intention ainsi exprimée et sous réserve du point 4.2, l'auteur de l'avant- projet examinera s'il ne convient pas de prévoir des garanties supplémentaires encadrant la consultation des zones sensibles de manière à éviter la divulgation d'informations y afférentes.

Article 105, § 5, en projet

1. Afin de garantir l'efficacité du droit prévu au paragraphe 5 de formuler par écrit et, le cas échéant, oralement, des observations, il se recommande que la disposition en projet précise que le demandeur puisse être accompagné par les conseils, techniques ou juridiques, de son choix.

2. Le mot "calendriers" sera omis à l'alinéa 1er.

Article 105, § 6, en projet

Aux fins de garantir l'égalité de traitement entre les différents opérateurs demandeurs de l'autorisation envisagée et pour des raisons de sécurité juridique, il appartient à l'auteur de l'avant-projet d'imposer un délai maximal de prise de décision lorsqu'il est fait usage de la possibilité prévue à l'alinéa 2 en projet.

Le régime de décision implicite organisé à l'article 105, § 6, alinéa 3, sera revu pour prendre également en considération le dépassement du délai maximal précité.

Article 105, § 7, en projet

1. Le paragraphe 7 en projet limite la portée du secret professionnel aux informations qualifiées de "confidentielles".

À cet égard, de deux choses l'une:

1° soit l'ensemble des informations dont ont connaissance les intéressés revêtent, dans l'intention de l'auteur de l'avant-projet, un caractère confidentiel: dans ce cas, le mot "confidentielles" est inutile et sera omis;

2° soit seules certaines des informations concernées revêtent, dans l'intention de l'auteur de l'avant-projet, un caractère confidentiel: dans ce cas, il convient de préciser lesquelles.

8 Voir C.C., 19 décembre 2013, n° 169/2013.

en objectieve verantwoording berust zodat die verschillende behandeling conform het gelijkheidsbeginsel is.[8]

Zo niet, moet de voorliggende bepaling herzien worden.

4.3. Gelet op de aldus geuite bedoeling en onder voorbehoud van punt 4.2, moet de steller van het voorontwerp nagaan of het niet raadzaam is om in het kader van de raadpleging van de gevoelige zones in aanvullende waarborgen te voorzien teneinde te voorkomen dat ruchtbaarheid gegeven wordt aan inlichtingen die daarmee verband houden.

Ontworpen artikel 105, § 5

1. Teneinde de werkzaamheid te garanderen van het in paragraaf 5 vervatte recht om schriftelijk en, in voorkomend geval, mondeling opmerkingen te maken, is het aan te bevelen om in de ontworpen bepaling op te nemen dat de verzoeker zich kan laten vergezellen door de technische of juridische raadslieden van zijn keuze.

2. In het eerste lid schrijve men "dagen" in plaats van "kalenderdagen".

Ontworpen artikel 105, § 6

Om ervoor te zorgen dat alle operatoren die om de in het vooruitzicht gestelde machtiging verzoeken gelijk behandeld worden en om redenen van rechtszekerheid dient de steller van het voorontwerp een maximumtermijn te bepalen waarbinnen een beslissing genomen moet worden wanneer gebruikgemaakt wordt van de mogelijkheid waarin het ontworpen tweede lid voorziet.

De regeling van stilzwijgende beslissing waarin het ontworpen artikel 105, § 6, derde lid, voorziet, moet aldus herzien worden dat eveneens rekening gehouden wordt met het overschrijden van de voormelde maximumtermijn.

Ontworpen artikel 105, § 7

1. In de ontworpen paragraaf 7 wordt de reikwijdte van het beroepsgeheim beperkt tot de informatie die als "vertrouwelijk" bestempeld wordt.

In dat verband is het van tweeën één:

1° ofwel is alle informatie waarvan de betrokkenen kennis hebben volgens de bedoeling van de steller van het voorontwerp vertrouwelijk van aard, in welk geval het woord "vertrouwelijke" overbodig is en dan ook weggelaten moet worden;

2° ofwel is slechts een gedeelte van de informatie in kwestie volgens de bedoeling van de steller van het voorontwerp vertrouwelijk van aard, in welk geval aangegeven dient te worden weke informatie als vertrouwelijk geldt.

8 Zie GwH 19 december 2013, nr. 169/2013.

La disposition à l'examen sera revue à la lumière de cette observation.

2. En ce qu'elle énonce que l'Institut dispose "notamment" des pouvoirs prévus à l'article 114/2 de la loi du 13 juin 2005 'relative aux communications électroniques', la disposition à l'examen ne permet pas de comprendre quels sont les pouvoirs, autres que ceux prévus par cet article 114/2, dont l'Institut dispose aux fins de contrôler l'application de l'article 105 en projet, son arrêté d'exécution et la décision des ministres concernés.

La disposition en projet sera revue afin de clarifier les pouvoirs de l'Institut en l'espèce.

3. L'attention de l'auteur de l'avant-projet est attirée sur le fait qu'un certain nombre de dispositions de la loi du 13 juin 2005 font l'objet de modifications dans le cadre d'un avant-projet de loi 'portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques', lequel fait l'objet d'une demande d'avis enrôlée sous le n° 69.166/4.

L'article 159 de cet avant-projet a vocation à abroger l'article 114/2 de la loi du 13 juin 2005, auquel l'article 105, § 7, en projet renvoie.

L'auteur de l'avant-projet veillera à la bonne concordance des textes en projet.

Article 4

L'article 14, § 1er, alinéa 1er, 3°, j), en projet est à ce point vague que l'on pourrait le comprendre comme habilitant l'IBPT à contrôler le respect de l'ensemble des "décisions contraignantes" de la Commission européenne ou des six ministres visés à l'article 105, § 1er, alinéa 2, de la loi du 13 juin 2005, sans avoir égard à l'objet réglé par ces décisions.

Il appartient à l'auteur de l'avant-projet de préciser le contexte dans lequel les décisions reprises à l'article 14, § 1er, alinéa 1er, 3°, j), en projet pourraient être prises ainsi que leur objet de manière à circonscrire précisément les pouvoirs de l'IBPT dans ce cadre.

L'article 14, § 1er, alinéa 1er, 3°, j), en projet sera revu en conséquence.

De voorliggende bepaling moet in het licht van deze opmerking herzien worden.

2. Voor zover in de ontworpen bepaling staat dat het Instituut "met name" beschikt over de bevoegdheden waarvan sprake is in artikel 114/2 van de wet van 13 juni 2005 'betreffende de elektronische communicatie', kan daaruit niet opgemaakt worden over welke andere bevoegdheden dan die vermeld in dat artikel 114/2 het Instituut beschikt om controle uit te oefenen op de toepassing van het ontworpen artikel 105, het uitvoeringsbesluit ervan en de beslissing van de betrokken ministers.

De ontworpen bepaling moet aldus herzien worden dat verduidelijkt wordt over welke bevoegdheden het Instituut in dat geval beschikt.

3. De steller van het voorontwerp wordt er opmerkzaam op gemaakt dat een aantal bepalingen van de wet van 13 juni 2005 gewijzigd worden in het kader van een voorontwerp van wet 'houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie', dat aan de Raad van State voorgelegd is in het kader van een adviesaanvraag die op de rol ingeschreven is onder het nummer 69.166/4.

Artikel 159 van dat voorontwerp strekt tot opheffing van artikel 114/2 van de wet van 13 juni 2005, waarnaar verwezen wordt in het ontworpen artikel 105, § 7.

De steller van het voorontwerp moet zorgen voor een goede onderlinge afstemming tussen de ontworpen teksten.

Artikel 4

Het ontworpen artikel 14, § 1, eerste lid, 3°, j), is dermate vaag dat die ontworpen bepaling opgevat zou kunnen worden als een machtiging aan het BIPT om toezicht uit te oefenen op de naleving van alle "bindende besluiten" van de Europese Commissie of van de zes ministers bedoeld in artikel 105, § 1, tweede lid, van de wet van 13 juni 2005, ongeacht de aangelegenheid die bij die besluiten geregeld wordt.

De steller van het voorontwerp dient te verduidelijken in welke context de besluiten vermeld in het ontworpen artikel 14, § 1, eerste lid, 3°, j), vastgesteld zouden kunnen worden en op welke aangelegenheid ze betrekking zouden kunnen hebben, teneinde nauwkeurig af te bakenen over welke bevoegdheden het BIPT in dat kader beschikt.

Het ontworpen artikel 14, § 1, eerste lid, 3°, j), moet dienovereenkomstig herzien worden.

Article 7

Il est renvoyé à l'observation sous l'article 105, § 1er, en projet.

*

Le greffier, *Le président,*

Charles-Henri Van Hove Martine Baguet

Artikel 7

Er wordt verwezen naar de opmerking die bij het ontworpen artikel 105, § 1, gemaakt is.

*

De griffier, *De voorzitter,*

Charles-Henri Van Hove Martine Baguet

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

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

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

La vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste est chargée de présenter, en notre nom, à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

CHAPITRE 2

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

Art. 2

Dans l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques, modifiée en dernier lieu par la loi du 26 mars 2018, les modifications suivantes sont apportées:

1° il est inséré un 87° rédigé comme suit:

"87° "MNO": un opérateur qui offre des services de communications électroniques mobiles et qui dispose d'un réseau d'accès radioélectrique propre, ainsi que de tous les éléments utiles à l'exploitation du réseau;";

2° il est inséré un 88° rédigé comme suit:

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

Op de voordracht van de vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post is ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze naam bij de Kamer van volksvertegenwoordigers in te dienen:

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2

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

Art. 2

In artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van 26 maart 2018, worden de volgende wijzigingen aangebracht:

1° een bepaling onder 87° wordt ingevoegd, luidende:

"87° "MNO": een operator die mobiele elektronischecommunicatiediensten aanbiedt en die beschikt over een eigen radiotoegangsnetwerk, alsook over alle nuttige elementen voor de exploitatie van het netwerk;";

2° een bepaling onder 88° wordt ingevoegd, luidende:

“88° “MVNO”: un opérateur qui offre des services de communications électroniques mobiles sans être MNO.”.

Art. 3

L’article 105, de la même loi, est remplacé par ce qui suit:

“Art. 105. § 1er. Dans le but de préserver les intérêts visés à l’article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, les MNO obtiennent une autorisation établie de façon conjointe par les ministres concernés visés à l’alinéa 3 avant d’utiliser un élément de leur réseau 5G.

En tenant compte des intérêts visés à l’alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut prévoir que cette autorisation est également nécessaire avant que les MNO ne puissent bénéficier de services de fournisseurs qui consistent à intervenir ponctuellement dans la gestion de ce réseau, notamment en cas d’incident ou de modification majeure du réseau, ou à gérer ou superviser quotidiennement des éléments du réseau ou est également nécessaire avant qu’ils ne puissent bénéficier de certains de ces services.

Pour l’application du présent article, il faut entendre par ministres concernés: le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l’Intérieur et le ministre des Affaires étrangères.

Un réseau 5G est un réseau de communications électroniques dont le réseau d’accès radioélectrique est basé sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l’Union internationale des télécommunications.

Les alinéas 1er et 2 ne sont pas d’application:

1° pour l’utilisation d’éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d’énergie;

2° pour les points de terminaison pour autant qu’ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l’Union internationale des télécommunications;

3° pour les éléments de réseaux mobiles de quatrième génération et des générations antérieures, pour autant qu’ils ne soient pas nécessaires à la fourniture d’un réseau 5G.

“88° “MVNO”: een operator die mobiele elektronische-communicatiediensten aanbiedt zonder MNO te zijn.”.

Art. 3

Artikel 105 van dezelfde wet wordt vervangen als volgt:

“Art. 105. § 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO’s een machtiging krijgen die gezamenlijk is opgesteld door de betrokken ministers beoogd in het derde lid alvorens een element van hun 5G-netwerk te gebruiken.

Rekening houdende met de in het eerste lid bedoelde belangen en bij besluit vastgesteld na overleg in de Ministerraad, kan de Koning bepalen dat deze machtiging ook noodzakelijk is voordat de MNO’s diensten van aanbieders kunnen genieten die erin bestaan gericht tussenbeide te komen in het beheer van dat netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks elementen van het netwerk te beheren of te superviseren, of ook noodzakelijk is voordat ze bepaalde van deze diensten kunnen genieten.

Voor de toepassing van dit artikel wordt verstaan onder betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken.

Een 5G-netwerk is een elektronische-communicatienetwerk waarvan het radiotoegangsnetwerk gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie.

Het eerste en het tweede lid zijn niet van toepassing:

1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;

2° voor de netwerkaansluitpunten voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie;

3° voor de elementen van mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor het aanbieden van een 5G-netwerk.

Si l'utilisation de l'élément de réseau ou le recours au fournisseur de services est déjà effectif à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, une autorisation de régularisation est demandée dans les deux mois qui suivent cette date.

§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres:

1° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à une ou plusieurs catégories de MVNO;

2° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à la société anonyme de droit public ASTRID, et aux fournisseurs de réseaux privés de communications électroniques qui ont été désignés comme exploitant d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou comme opérateur de services essentiels au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

3° charger une ou plusieurs autorités de désigner par décision individuelle, lorsque c'est nécessaire pour préserver les intérêts visés au paragraphe 1er, alinéa 1er, les autres fournisseurs de réseaux privés de communications électroniques soumis à l'obligation d'obtenir les autorisations visées au paragraphe 1er;

4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er , alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau;

§ 3. Le demandeur introduit son dossier auprès de l'Institut, selon les modalités qu'il fixe sur son site internet.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, les modalités de traitement de la demande et la composition du dossier.

Les ministres concernés, l'Institut et les services de renseignement et de sécurité peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.

§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au paragraphe 1er, ou la revoient

Indien het gebruik van het netwerkelement of het beroep op de dienstenaanbieder reeds bestaat op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, wordt een machtiging tot regularisatie gevraagd in de twee maanden die volgen op die datum.

§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:

1° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;

2° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar de naamloze vennootschap van publiek recht ASTRID en naar de aanbieders van private elektronische-communicatienetwerken die aangewezen zijn als exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of als aanbieder van essentiële diensten in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

3° een of meer autoriteiten opdragen om via individuele beslissing, wanneer dat noodzakelijk is om de in paragraaf 1, eerste lid bedoelde belangen te vrijwaren, de andere aanbieders van private elektronische-communicatienetwerken aan te wijzen die onderworpen zijn aan de verplichting om de in paragraaf 1 bedoelde machtigingen te krijgen;

4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware van het netwerk;

§ 3. De verzoeker dient zijn dossier in bij het Instituut, volgens de nadere regels die het op zijn website bepaalt.

De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels voor de behandeling van het verzoek en de samenstelling van het dossier vast.

De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.

§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in paragraaf 1 bedoelde verzoek of deze op

d'initiative en raison d'un nouvel élément de nature à remettre en cause leur décision, les ministres concernés mettent en œuvre les restrictions et délais de mise en œuvre fixés par le Roi, par arrêté délibéré en Conseil des ministres, concernant l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque.

Ces restrictions et ces délais de mise en œuvre ne peuvent être fixés qu'en vue de garantir la protection des intérêts visés au paragraphe 1er, alinéa 1er.

Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en œuvre de la nouvelle décision qui est postérieure aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.

Le profil de risque d'un fournisseur est évalué sur base des critères suivants:

1° la probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un État membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants:

a) un lien fort avec les autorités publiques du pays en question;

b) la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des données ou de sécurité entre l'Union européenne et le pays en question;

c) les caractéristiques de la propriété d'entreprise du fournisseur;

d) la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements;

e) le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive.

2° la capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité;

3° la qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation

eigen initiatief herzien wegens een nieuw element dat hun beslissing ter discussie stelt, leggen de betrokken ministers de beperkingen en toepassingstermijnen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen.

Die beperkingen en toepassingstermijnen mogen enkel vastgesteld worden om de bescherming van de belangen bedoeld in paragraaf 1, eerste lid, te garanderen.

Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.

Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:

1° de kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:

a) een sterke link met de overheidsinstanties van het land in kwestie;

b) de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;

c) de karakteristieken van de eigendom van de onderneming van de leverancier;

d) het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;

e) het land waaruit de leverancier afkomstig is, voert of is betrokken bij een offensief cyberbeleid.

2° het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;

3° de algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste

adéquate des priorités est donnée aux pratiques en matière de sécurité.

Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 4.

Un seul de ces critères peut justifier qu'un fournisseur soit qualifié comme étant à haut risque.

Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 4, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 4, 2° et 3°.

Les zones sensibles sont identifiées par le Roi, sur base d'un avis du Conseil national de sécurité, et ce, en tenant compte de la présence dans ces zones de sites liés aux intérêts visés au paragraphe 1er, alinéa 1er.

L'arrêté royal identifiant les zones sensibles est publié par voie de mention au *Moniteur belge*.

§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision, le demandeur dispose de vingt-huit jours après avoir reçu le projet de décision pour présenter ses observations écrites.

La possibilité est offerte au demandeur d'être entendu. Il peut se faire accompagner par les conseils, techniques ou juridiques, de son choix.

Les ministres concernés peuvent se faire représenter par l'administration de leur choix. L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.

§ 6. Les ministres concernés prennent ensemble une seule décision. L'Institut pose tous les actes utiles en vue de sa préparation.

Dans le délai fixé par le Roi, qui commence après l'introduction de la demande, le demandeur reçoit la décision des ministres qui octroie l'autorisation ou le projet de décision dans lequel ils refusent l'autorisation ou l'assortissent de conditions.

hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het vierde lid beoogde criteria aanvullen.

Slechts één van deze criteria kan reeds rechtvaardigen dat een aanbieder wordt aangeduid als een hoog risico vormend.

Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het vierde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het vierde lid, 2° en 3°.

De gevoelige zones worden geïdentificeerd door de Koning, op basis van een advies van de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen bedoeld in paragraaf 1, eerste lid.

Het koninklijk besluit dat de gevoelige zones identificeert, wordt bekendgemaakt via vermelding in het *Belgisch Staatsblad*.

§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing te herzien, beschikt de verzoeker, na de ontwerpbeslissing te hebben ontvangen, over achtentwintig dagen tijd om zijn schriftelijke opmerkingen voor te leggen.

De verzoeker wordt de kans geboden om te worden gehoord. Hij mag zich laten vergezellen door de technische of juridische raadgevers van zijn keuze.

De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.

§ 6. De betrokken ministers nemen samen één beslissing. Het Instituut stelt alle nuttige daden met het oog op de voorbereiding ervan.

Binnen de door de Koning vastgestelde termijn, die ingaat na de indiening van het verzoek, ontvangt de verzoeker ofwel de beslissing van de ministers waarin de machtiging wordt verleend, ofwel de ontwerpbeslissing waarin ze de machtiging weigeren of voorwaarden daaraan koppelen.

En cas d'audition ou d'observations écrites du demandeur, visées au paragraphe 5, les ministres prennent leur décision au plus tard dans le délai fixé par le Roi, qui commence à partir de la réception des observations écrites ou de la date de l'audition, la date la plus tardive étant retenue.

La demande d'informations ou de documents visée au paragraphe 3, alinéa 2, ou adressée au demandeur afin qu'il complète son dossier, suspend les délais fixés aux alinéas 2 et 3, jusqu'au jour où les informations ou documents demandés sont fournis.

Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus.

§ 7. La personne qui obtient une copie de la liste des zones sensibles visée au paragraphe 4, alinéa 8, ne peut la transmettre qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.

Est punie d'une amende pénale de 1000 euros à 100 000 euros: la personne qui divulgue des informations relatives à la liste visée à l'alinéa 1er à une personne qui n'est pas visée à cet alinéa.

Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent communiquer à des administrations publiques qu'elles consultent dans ce cadre des informations confidentielles lorsque c'est nécessaire pour l'accomplissement de la tâche qu'elles leur confient.

Les personnes et les administrations publiques visées à l'alinéa 3 ne peuvent communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'application du présent article, hormis les exceptions prévues par la loi.

Ces informations confidentielles sont celles qui sont qualifiées comme telles par la personne qui les a fournies, sans préjudice de l'article 23, paragraphe 3, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

La violation de l'interdiction visée à l'alinéa 4 sera punie par les peines prévues à l'article 458 du Code pénal ou l'une de ces peines.

In geval van een hoorzitting of van schriftelijke opmerkingen van de verzoeker, waarvan sprake in paragraaf 5, nemen de ministers hun beslissing uiterlijk binnen de termijn die door de Koning is vastgesteld en die ingaat vanaf de ontvangst van de schriftelijke opmerkingen of vanaf de datum van de hoorzitting, waarbij de datum die het laatst komt in aanmerking wordt genomen.

Het verzoek om inlichtingen of om documenten, waarvan sprake in paragraaf 3, tweede lid, of dat gericht is aan de verzoeker om zijn dossier te vervolledigen, schorst de termijnen die vastgesteld zijn in het tweede en het derde lid, tot de dag waarop de gevraagde inlichtingen of documenten worden verstrekt.

Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering.

§ 7. De persoon die een kopie krijgt van de in paragraaf 4, achtste lid, bedoelde lijst van de gevoelige zones, mag die maar verzenden aan de personen die daar kennis van moeten hebben en die daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.

Wordt bestraft met een strafrechtelijke boete van 1000 euro tot 100 000 euro: de persoon die informatie onthult in verband met de in het eerste lid bedoelde lijst aan een persoon die in dat lid niet is beoogd.

Personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen aan openbare besturen die zij in dat kader raadplegen vertrouwelijke informatie meedelen wanneer dat nodig is voor het vervullen van de taak die zij aan hen toevertrouwen.

De in het derde lid bedoelde personen en openbare besturen mogen derden geen vertrouwelijke informatie meedelen waarvan zij kennis hebben in het kader van de toepassing van dit artikel, buiten de in de wet bepaalde uitzonderingen.

Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de persoon die ze heeft verstrekt, onverminderd artikel 23, paragraaf 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.

De schending van het in het vierde lid bedoelde verbod wordt bestraft met de straffen die zijn bepaald in artikel 458 van het Strafwetboek of met één van die straffen.

§ 8. Lorsqu'un MNO offre en Belgique des services de communications électroniques à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des États membres de l'Union européenne. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, et par arrêté délibéré en Conseil des ministres, le Roi peut fixer les exigences qui découlent de cette obligation.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi impose aux MNO visés à l'alinéa 1er les règles nécessaires pour qu'ils effectuent les activités indispensables au fonctionnement, à la sécurité et à la continuité de leur réseau, qu'Il détermine, au sein du territoire des États membres de l'Union européenne.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut étendre les règles et exigences visées aux alinéas 1er et 2 aux MVNO et fournisseurs de réseaux privés de communications électroniques qui sont soumis aux autorisations visées au paragraphe 1er.

§ 8. Wanneer een MNO in België elektronischecommunicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuren van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de eisen vaststellen die uit die verplichting voortvloeien.

Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, legt de Koning de in het eerste lid bedoelde MNO's de noodzakelijke regels op opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk, die Hij bepaalt, uitoefenen binnen het grondgebied van de lidstaten van de Europese Unie.

Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de regels en eisen bedoeld in het eerste en tweede lid uitbreiden naar de MVNO's en aanbieders van private elektronischecommunicatienetwerken die onderworpen zijn aan de machtigingen bedoeld in paragraaf 1.

CHAPITRE 3

HOOFDSTUK 3

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 4

Art. 4

Dans l'article 14, paragraphe 1er, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, modifiée en dernier lieu par la loi du 7 avril 2019, il est inséré un point j) rédigé comme suit:

"j) toute décision contraignante adoptée par:

i) l'Institut;

ii) les ministres sur base de l'article 105, paragraphe 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques;

iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal".

Aan artikel 14, paragraaf 1, eerste lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, laatstelijk gewijzigd bij de wet van 7 april 2019, wordt een punt j) ingevoegd, luidende:

"j) elk bindend besluit aangenomen door:

i) het Instituut;

ii) de ministers op basis van artikel 105, paragraaf 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector".

Art. 5

Dans l'article 14, paragraphe 2, 3°, de la même loi, il est inséré un point j) rédigé comme suit:

j) les ministres visés à l'article 105, paragraphe 1er, alinéa 3, de la loi du 13 juin 2005 relative aux communications électroniques et leur cabinet, pour la mise en œuvre de cet article.

Art. 6

A l'article 21, paragraphe 1er, de la même loi, les modifications suivantes sont apportées:

1° les mots "ou aux décisions prises" sont remplacés par les mots "à une décision prise".

2° les mots ", ou à une décision visée à l'article 105, paragraphe 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques" sont insérés entre les mots "en exécution de cette législation ou réglementation" et ", il fait part le cas échéant de ses griefs à l'intéressé".

CHAPITRE 4

Disposition finale et entrée en vigueur

Art. 7

Le Roi peut codifier les dispositions pertinentes de la loi de 13 juin 2005 relative aux communications électroniques ou d'autres lois relatives aux communications électroniques, en ce compris celles modifiées et insérées par la présente loi, ainsi que les dispositions qui y auraient, jusqu'au moment de la coordination, expressément ou implicitement apporté des modifications.

A cette fin, Il peut:

1° modifier l'ordre, la numérotation et, en général, la présentation des dispositions à codifier;

2° modifier les références qui seraient contenues dans les dispositions à codifier en vue de les mettre en concordance avec la nouvelle numérotation;

3° modifier la rédaction des dispositions à codifier en vue d'assurer leur concordance et d'en unifier la terminologie sans qu'il puisse être porté atteinte aux principes inscrits dans ces dispositions.

Art. 5

In artikel 14, paragraaf 2, 3°, van dezelfde wet wordt een punt j) ingevoegd, luidende:

j) de ministers bedoeld in artikel 105, paragraaf 1, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel.

Art. 6

In artikel 21, paragraaf 1, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° de woorden "of van de besluiten"worden vervangen door de woorden "op een besluit".

2° de woorden" of op een beslissing bedoeld in artikel 105, paragraaf 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie" worden ingevoegd tussen de woorden "ter uitvoering van die wetgeving of reglementering" en "deelt hij in voorkomend geval zijn grieven mee aan de betrokkene".

HOOFDSTUK 4

Slotbepaling en inwerkingtreding

Art. 7

De Koning kan de relevante bepalingen van de wet van 13 juni 2005 betreffende de elektronische communicatie of van andere wetten inzake elektronische communicatie, met inbegrip van diegene gewijzigd en ingevoegd door deze wet, codificeren, evenals de bepalingen die hieraan uitdrukkelijk of stilzwijgend wijzigingen aanbrengen tot aan het tijdstip van de codificatie.

Daartoe kan Hij:

1° de volgorde en de nummering van de te codificeren bepalingen veranderen en in het algemeen de teksten naar de vorm wijzigen;

2° de verwijzingen die voorkomen in de te codificeren bepalingen, met de nieuwe nummering overeenbrengen;

3° zonder afbreuk te doen aan de beginselen die in de te codificeren bepalingen vervat zijn, de redactie ervan wijzigen om ze onderling te doen overeenstemmen en eenheid in de terminologie te brengen.

La codification remplacera les dispositions visées à l'alinéa 1er et entrera en vigueur à la date de sa confirmation par la loi.

Art. 8

Le Roi fixe, par arrêté royal délibéré en Conseil des ministres, l'entrée en vigueur de l'arrêté royal visé à l'article 105, paragraphe 8, alinéas 1er , 2 et 3, de la loi du 13 juin 2005 relative aux communications électroniques, tel qu'inséré par l'article 3 de la présente loi, au plus tôt le 1er janvier 2026.

Donné à Bruxelles, le 19 novembre 2021

PHILIPPE

PAR LE ROI:

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

Petra DE SUTTER

De codificatie vervangt de bepalingen bedoeld in het eerste lid en treedt in werking op de dag van de bekrachtiging ervan bij de wet.

Art. 8

De Koning stelt, bij koninklijk besluit vastgesteld na overleg in de Ministerraad, de inwerkingtreding van het koninklijk besluit bedoeld in artikel 105, paragraaf 8, eerste, tweede en derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie, zoals ingevoegd door artikel 3 van deze wet, op zijn vroegst vast op 1 januari 2026.

Gegeven te Brussel, 19 november 2021

FILIP

VAN KONINGSWEGE:

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

Petra DE SUTTER

COORDINATION DES ARTICLES

TEXTE DE BASE	TEXTE DE BASE ADAPTÉ AU PROJET
Loi du 13 juin 2005 relative aux communications électroniques	**Loi du 13 juin 2005 relative aux communications électroniques**
TITRE Ier. - Définitions et principes généraux.	**TITRE Ier. - Définitions et principes généraux.**
CHAPITRE Ier. - Généralités.	**CHAPITRE Ier. - Généralités.**
Art. 2. Pour l'application de la présente loi, il faut entendre par:	**Art. 2.** Pour l'application de la présente loi, il faut entendre par:
	[…]
	87° "MNO": un opérateur qui offre des services de communications électroniques mobiles et qui dispose d'un réseau d'accès radioélectrique propre, ainsi que de tous les éléments utiles à l'exploitation du réseau ;
	88° "MVNO": un opérateur qui offre des services de communications électroniques mobiles sans être MNO.
CHAPITRE II. - Des services d'intérêt public	**CHAPITRE II. - Des services d'intérêt public**
Art. 105. Dans les conditions et selon les modalités techniques et financières fixées par le Roi après avis de l'Institut, un ou plusieurs opérateurs désignés par le Roi après avis de l'Institut satisfont à toutes les demandes raisonnables:	***Art. 105. § 1er. Dans le but de préserver les intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, les MNO obtiennent une autorisation établie de façon conjointe par les ministres concernés visés à l'alinéa 3 avant d'utiliser un élément de leur réseau 5G.***
1° d'accès aux services de commutation de données;	***En tenant compte des intérêts visés à l'alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut prévoir que cette autorisation est également nécessaire avant que les MNO ne puissent bénéficier de services de fournisseurs qui consistent à intervenir ponctuellement dans la gestion de ce réseau, notamment en cas d'incident ou de modification majeure du réseau, ou à gérer ou superviser quotidiennement des éléments du réseau ou est également nécessaire avant qu'ils ne puissent bénéficier de certains de ces services.***

2° d'accès à des réseaux numériques en position déterminée, y compris au réseau numérique à intégration de services, ainsi qu'à un ensemble de services basés sur ces réseaux;	***Pour l'application du présent article, il faut entendre par ministres concernés : le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères.***
3° d'accès à un service de télex et de télégraphie.	***Un réseau 5G est un réseau de communications électroniques dont le réseau d'accès radioélectrique est basé sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications.***
Ces demandes restent valables jusqu'à une date fixée par le Roi, après avis de l'Institut.	***Les alinéas 1er et 2 ne sont pas d'application:***
	1° pour l'utilisation d'éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d'énergie;
	2° pour les points de terminaison pour autant qu'ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications;
	3° pour les éléments de réseaux mobiles de quatrième génération et des générations antérieures, pour autant qu'ils ne soient pas nécessaires à la fourniture d'un réseau 5G.
	Si l'utilisation dudit élément de réseau ou le recours au fournisseur de services est déjà effectif à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, une autorisation de régularisation est demandée dans les deux mois qui suivent cette date.
	§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres:
	1° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à une ou plusieurs catégories de MVNO;
	2° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à la société anonyme de droit public A.S.T.R.I.D., et

	aux fournisseurs de réseaux privés de communications électroniques qui ont été désignés comme exploitant d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou comme opérateur de services essentiels au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique,;
	3° charger une ou plusieurs autorités de désigner par décision individuelle, lorsque c'est nécessaire pour préserver les intérêts visés au paragraphe 1er, alinéa 1er, les autres fournisseurs de réseaux privés de communications électroniques soumis à l'obligation d'obtenir les autorisations visées au paragraphe 1er;
	4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er , alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau;
	§ 3. Le demandeur introduit son dossier auprès de l'Institut, selon les modalités qu'il fixe sur son site internet.
	Le Roi fixe, par arrêté délibéré en Conseil des Ministres, les modalités de traitement de la demande et la composition du dossier.
	Les ministres concernés, l'Institut et les services de renseignement et de sécurité peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.
	§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au paragraphe 1er, ou la revoient d'initiative en raison d'un nouvel élément de nature à remettre en cause leur décision, les ministres concernés mettent en œuvre les restrictions et délais de mise en œuvre fixés par le Roi, par arrêté délibéré en Conseil des ministres, concernant l'utilisation, sur le territoire national ou dans les zones

	sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque.
	Ces restrictions et ces délais de mise en œuvre ne peuvent être fixés qu'en vue de garantir la protection des intérêts visés au paragraphe 1er, alinéa 1er.
	Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en œuvre de la nouvelle décision qui est postérieure aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.
	Le profil de risque d'un fournisseur est évalué sur base des critères suivants:
	1° la probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un État membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants:
	a) un lien fort avec les autorités publiques du pays en question;
	b) la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des données ou de sécurité entre l'Union européenne et le pays en question;
	c) les caractéristiques de la propriété d'entreprise du fournisseur;
	d) la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements;
	e) le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive.

	2° la capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité;
	3° la qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation adéquate des priorités est donnée aux pratiques en matière de sécurité.
	Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 4.
	Un seul de ces critères peut justifier qu'un fournisseur soit qualifié comme étant à haut risque.
	Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 4, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 4, 2° et 3°.
	Les zones sensibles sont identifiées par le Roi, sur base d'un avis du Conseil national de sécurité, et ce, en tenant compte de la présence dans ces zones de sites liés aux intérêts visés au paragraphe 1er, alinéa 1er.
	L'arrêté royal identifiant les zones sensibles est publié par voie de mention au Moniteur belge.
	§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou revoir leur décision, le demandeur dispose de vingt-huit jours après avoir reçu le projet de décision pour présenter ses observations écrites.
	La possibilité est offerte au demandeur d'être entendu. Il peut se faire accompagner par les conseils, techniques ou juridiques, de son choix.
	Les ministres concernés peuvent se faire représenter par l'administration de leur choix.

	L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.
	§ 6. Les ministres concernés prennent ensemble une seule décision. L'Institut pose tous les actes utiles en vue de sa préparation.
	Dans le délai fixé par le Roi, qui commence après l'introduction de la demande, le demandeur reçoit la décision des ministres qui octroie l'autorisation ou le projet de décision dans lequel ils refusent l'autorisation ou l'assortissent de conditions.
	En cas d'audition ou d'observations écrites du demandeur, visées au paragraphe 5, les ministres prennent leur décision au plus tard dans le délai fixé par le Roi, qui commence à partir de la réception des observations écrites ou de la date de l'audition, la date la plus tardive étant retenue.
	La demande d'informations ou de documents visée au paragraphe 3, alinéa 2, ou adressée au demandeur afin qu'il complète son dossier, suspend les délais fixés aux alinéas 2 et 3, jusqu'au jour où les informations ou documents demandés sont fournis.
	Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus.
	§ 7. La personne qui obtient une copie de la liste des zones sensibles visée au paragraphe 4, alinéa 8, ne peut la transmettre qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.
	Est punie d'une amende pénale de 1000 euros à 100.000 euros : la personne qui divulgue des informations relatives à la liste visée à l'alinéa 1er à une personne qui n'est pas visée à cet alinéa.
	Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent communiquer à des administrations publiques qu'elles consultent

	dans ce cadre des informations confidentielles lorsque c'est nécessaire pour l'accomplissement de la tâche qu'elles leur confient.
	Les personnes et les administrations publiques visées à l'alinéa 3 ne peuvent communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'application du présent article, hormis les exceptions prévues par la loi.
	Ces informations confidentielles sont celles qui sont qualifiées comme telles par la personne qui les a fournies, sans préjudice de l'article 23, paragraphe 3, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.
	La violation de l'interdiction visée à l'alinéa 4 sera punie par les peines prévues à l'article 458 du Code pénal ou l'une de ces peines.
	§ 8. Lorsqu'un MNO offre en Belgique des services de communications électroniques à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des Etats membres de l'Union européenne. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, et par arrêté délibéré en Conseil des ministres, le Roi peut fixer les exigences qui découlent de cette obligation.
	En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi impose aux MNO visés à l'alinéa 1er les règles nécessaires pour qu'ils effectuent les activités indispensables au fonctionnement, à la sécurité et à la continuité de leur réseau, qu'Il détermine, au sein du territoire des États membres de l'Union européenne.
	En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut étendre les règles et exigences visées aux alinéas 1er et 2 aux MVNO et fournisseurs de réseaux privés de communications

	électroniques qui sont soumis aux autorisations visées au paragraphe 1er.
Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	**Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges**
CHAPITRE III. - L'Institut.	**CHAPITRE III. - L'Institut.**
Section 2. - Compétences et Missions.	**Section 2. - Compétences et Missions.**
Art. 14. § 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes :	[…]
1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants ;	
2° la prise de décisions administratives ;	
3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :	
a) la loi du 13 juin 2005 relative aux communications électroniques ;	
b) le Titre Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;	
c) la loi du 26 janvier 2018 relative aux services postaux ;	

d) les articles 14, § 2, 2°, et 21, §§ 5 à 7, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges ;	
e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;	
f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;	
g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;	
h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ;	
i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.	
	j) toute décision contraignante adoptée par:
	i) l'Institut;
	ii) les ministres sur base de l'article 105, paragraphe 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques;
	iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal;
[…]	[…]
§ 2. Dans le cadre de ses compétences, l'Institut :	[…]

1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte;	
2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;	
3° coopère avec et communique de l'information à :	
a) la Commission européenne, l'ENISA, l'Office et à l'ORECE;	
b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;	
c) les autorités de régulation des autres secteurs économiques;	
d) les services publics fédéraux en charge de la protection des consommateurs;	
e) les autorités belges en charge de la concurrence;	
Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les	

modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut;	
f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;	
g) les services publics qui ont une compétence en matière de sécurité publique, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;	
h) la Commission de la protection de la vie privée;	
i) le Service public fédéral chargé des statistiques et de l'information économique;	
	j) les ministres visés à l'article 105, paragraphe 1er, alinéa 3, de la loi du 13 juin 2005 relative aux communications électroniques et leur cabinet, pour la mise en œuvre de cet article.
[...]	[...]
Section 3. - Le Conseil.	**Section 3. - Le Conseil.**
Sous-section 3. - Fonctionnement.	**Sous-section 3. - Fonctionnement.**
Art. 21. § 1er. Si le Conseil dispose d'un faisceau d'indices qui pourraient indiquer une infraction à la législation ou à la réglementation dont l'Institut contrôle le respect, ou aux décisions prises par l'Institut en exécution de cette législation ou réglementation, il fait part le cas échéant de ses griefs à l'intéressé ainsi que des mesures envisagées visées au paragraphe 5 qui seront appliquées en cas de confirmation de l'infraction.	**Art. 21.** § 1er. Si le Conseil dispose d'un faisceau d'indices qui pourraient indiquer une infraction à la législation ou à la réglementation dont l'Institut contrôle le respect, ***à une décision prise*** par l'Institut en exécution de cette législation ou réglementation, ***ou à une décision visée à l'article 105, paragraphe 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques,*** il fait part le cas échéant de ses griefs à l'intéressé ainsi que des mesures envisagées visées au paragraphe 5 qui seront appliquées en cas de confirmation de l'infraction.
[...]	[...]

COÖRDINATIE VAN DE ARTIKELEN

BASIS TEKST	BASISTEKST AANGEPAST AAN HET PROJECT
Wet van 13 juni 2005 betreffende de elektronische communicatie	**Wet van 13 juni 2005 betreffende de elektronische communicatie**
TITEL I. - Definities en algemene principes.	**TITEL I. - Definities en algemene principes.**
HOOFDSTUK I. - Algemeen.	**HOOFDSTUK I. - Algemeen.**
Art. 2. Voor de toepassing van deze wet wordt verstaan onder:	**Art. 2.** Voor de toepassing van deze wet wordt verstaan onder:
	[…]
	"87° "MNO": een operator die mobiele elektronische-communicatiediensten aanbiedt en die beschikt over een eigen radiotoegangsnetwerk, alsook over alle nuttige elementen voor de exploitatie van het netwerk; ";
	"88° "MVNO": een operator die mobiele elektronische-communicatiediensten aanbiedt zonder MNO te zijn.".
HOOFDSTUK II. - Diensten van algemeen belang	**HOOFDSTUK II. - Diensten van algemeen belang**
Art. 105. Onder de voorwaarden en volgens de nadere technische en financiële regels die de Koning na advies van het Instituut vaststelt, voldoen een of meer operatoren die na advies van het Instituut door de Koning worden aangewezen, aan alle redelijke verzoeken:	***Art. 105. § 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO's een machtiging krijgen die gezamenlijk is opgesteld door de betrokken ministers beoogd in het derde lid alvorens een element van hun 5G-netwerk te gebruiken.***
1° om toegang tot diensten voor gegevensschakeling;	***Rekening houdende met de in het eerste lid bedoelde belangen en bij besluit vastgesteld na overleg in de Ministerraad, kan de Koning bepalen dat deze machtiging ook noodzakelijk is voordat de MNO's diensten van aanbieders kunnen genieten die erin bestaan gericht tussenbeide te komen in het beheer van dat netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks elementen van het netwerk te beheren of te superviseren, of ook noodzakelijk is voordat ze bepaalde van deze diensten kunnen genieten.***

2° om toegang tot digitale netwerken op een vaste locatie, waaronder het digitale netwerk voor geïntegreerde diensten, alsook alle diensten die op die netwerken gebaseerd zijn;	***Voor de toepassing van dit artikel wordt verstaan onder betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken.***
3° om toegang tot een telex- en telegrafiedienst;	***Een 5G-netwerk is een elektronische-communicatienetwerk waarvan het radiotoegangsnetwerk gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie.***
Die verzoeken blijven geldig tot op een datum vastgesteld door de Koning, na advies van het Instituut.	***Het eerste en het tweede lid zijn niet van toepassing:***
	1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;
	2° voor de netwerkaansluitpunten voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie;
	3° voor de elementen van mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor het aanbieden van een 5G-netwerk.
	Indien het gebruik van het voormelde netwerkelement of het beroep op de dienstenaanbieder reeds bestaat op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, wordt een machtiging tot regularisatie gevraagd in de twee maanden die volgen op die datum.
	§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:
	1° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;

	2° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar de naamloze vennootschap van publiek recht A.S.T.R.I.D. en naar de aanbieders van private elektronische-communicatienetwerken die aangewezen zijn als exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of als aanbieder van essentiële diensten in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;
	3° een of meer autoriteiten opdragen om via individuele beslissing, wanneer dat noodzakelijk is om de in paragraaf 1, eerste lid bedoelde belangen te vrijwaren, de andere aanbieders van private elektronische-communicatienetwerken aan te wijzen die onderworpen zijn aan de verplichting om de in paragraaf 1 bedoelde machtigingen te krijgen;
	4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware van het netwerk;
	§ 3. De verzoeker dient zijn dossier in bij het Instituut, volgens de nadere regels die het op zijn website bepaalt.
	De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels voor de behandeling van het verzoek en de samenstelling van het dossier vast.
	De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.
	§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in paragraaf 1 bedoelde verzoek of deze op eigen initiatief herzien wegens een nieuw element dat hun beslissing

	ter discussie stelt, leggen de betrokken ministers de beperkingen en toepassingstermijnen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen.
	Die beperkingen en toepassingstermijnen mogen enkel vastgesteld worden om de bescherming van de belangen bedoeld in paragraaf 1, eerste lid, te garanderen.
	Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.
	Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:
	1° de kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:
	a) een sterke link met de overheidsinstanties van het land in kwestie;
	b) de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;

	c) de karakteristieken van de eigendom van de onderneming van de leverancier;
	d) het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;
	e) het land waaruit de leverancier afkomstig is, voert of is betrokken bij een offensief cyberbeleid.
	2° het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;
	3° de algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging.
	De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het vierde lid beoogde criteria aanvullen.
	Slechts één van deze criteria kan reeds rechtvaardigen dat een aanbieder wordt aangeduid als een hoog risico vormend.
	Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het vierde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het vierde lid, 2° en 3°.
	De gevoelige zones worden geïdentificeerd door de Koning, op basis van een advies van de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen bedoeld in paragraaf 1, eerste lid.

	Het koninklijk besluit dat de gevoelige zones identificeert, wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.
	§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing te herzien, beschikt de verzoeker, na de ontwerpbeslissing te hebben ontvangen, over achtentwintig dagen tijd om zijn schriftelijke opmerkingen voor te leggen.
	De verzoeker wordt de kans geboden om te worden gehoord. Hij mag zich laten vergezellen door de technische of juridische raadgevers van zijn keuze.
	De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.
	§ 6. De betrokken ministers nemen samen één beslissing. Het Instituut stelt alle nuttige daden met het oog op de voorbereiding ervan.
	Binnen de door de Koning vastgestelde termijn, die ingaat na de indiening van het verzoek, ontvangt de verzoeker ofwel de beslissing van de ministers waarin de machtiging wordt verleend, ofwel de ontwerpbeslissing waarin ze de machtiging weigeren of voorwaarden daaraan koppelen.
	In geval van een hoorzitting of van schriftelijke opmerkingen van de verzoeker, waarvan sprake in paragraaf 5, nemen de ministers hun beslissing uiterlijk binnen de termijn die door de Koning is vastgesteld en die ingaat vanaf de ontvangst van de schriftelijke opmerkingen of vanaf de datum van de hoorzitting, waarbij de datum die het laatst komt in aanmerking wordt genomen.
	Het verzoek om inlichtingen of om documenten, waarvan sprake in paragraaf 3, tweede lid, of dat gericht is aan de verzoeker om zijn dossier te vervolledigen, schorst de termijnen die vastgesteld zijn in het tweede en het derde lid, tot de dag waarop de gevraagde inlichtingen of documenten worden verstrekt.

	Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering.
	§ 7. De persoon die een kopie krijgt van de in paragraaf 4, achtste lid, bedoelde lijst van de gevoelige zones, mag die maar verzenden aan de personen die daar kennis van moeten hebben en die daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.
	Wordt bestraft met een strafrechtelijke boete van 1000 euro tot 100.000 euro: de persoon die informatie onthult in verband met de in het eerste lid bedoelde lijst aan een persoon die in dat lid niet is beoogd.
	Personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen aan openbare besturen die zij in dat kader raadplegen vertrouwelijke informatie meedelen wanneer dat nodig is voor het vervullen van de taak die zij aan hen toevertrouwen.
	De in het derde lid bedoelde personen en openbare besturen mogen derden geen vertrouwelijke informatie meedelen waarvan zij kennis hebben in het kader van de toepassing van dit artikel, buiten de in de wet bepaalde uitzonderingen.
	Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de persoon die ze heeft verstrekt, onverminderd artikel 23, paragraaf 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.
	De schending van het in het vierde lid bedoelde verbod wordt bestraft met de straffen die zijn bepaald in artikel 458 van het Strafwetboek of met één van die straffen.

	§ 8. Wanneer een MNO in België elektronische-communicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuren van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de eisen vaststellen die uit die verplichting voortvloeien.
	Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, legt de Koning de in het eerste lid bedoelde MNO's de noodzakelijke regels op opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk, die Hij bepaalt, uitoefenen binnen het grondgebied van de lidstaten van de Europese Unie.
	Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de regels en eisen bedoeld in het eerste en tweede lid uitbreiden naar de MVNO's en aanbieders van private elektronische-communicatienetwerken die onderworpen zijn aan de machtigingen bedoeld in paragraaf 1.
Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.	**Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.**
<u>HOOFDSTUK III.</u> - Het Instituut.	**<u>HOOFDSTUK III.</u> - Het Instituut.**
<u>Afdeling 2.</u> - Bevoegdheden en opdrachten.	**<u>Afdeling 2.</u> - Bevoegdheden en opdrachten.**
Art. 14. § 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur, met betrekking tot de sector digitale infrastructuren in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en	[…]

informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:	
1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers;	
2° het nemen van administratieve beslissingen;	
3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:	
a) de wet van 13 juni 2005 betreffende de elektronische communicatie;	
b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;	
c) de wet van 26 januari 2018 betreffende de postdiensten;	
d) de artikelen 14, § 2, 2°, en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	
e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	
f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;	
g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische	

communicatie en digitale infrastructuren betreft;	
h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sector digitale infrastructuren;	
i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.	
	j) elk bindend besluit aangenomen door:
	i) het Instituut;
	ii) de ministers op basis van artikel 105, paragraaf 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
	iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector;".
[…]	[…]
§ 2. In het kader van zijn bevoegdheden :	[…]
1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het	

Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;	
2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;	
3° werkt het Instituut samen met en verstrekt het informatie aan :	
a) de Europese Commissie, ENISA, het Bureau en aan BEREC;	
b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;	
c) de regulerende instanties in de overige economische sectoren;	
d) de federale overheidsdiensten die belast zijn met consumentenbescherming;	
e) de Belgische instanties die belast zijn met mededinging.	
De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;	
f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;	
g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of	

bescherming van het economische en wetenschappelijke potentieel van het land;	
h) de Commissie voor de bescherming van de persoonlijke levenssfeer;	
i) de federale overheidsdienst die belast is met statistiek en economische informatie;	
	j) de ministers bedoeld in artikel 105, paragraaf 1, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel.
[…]	[…]
Afdeling 3. - De Raad.	**Afdeling 3. - De Raad.**
Onderafdeling 3. - Werking.	**Onderafdeling 3. - Werking.**
Art. 21. § 1. Indien de Raad over een reeks aanwijzingen beschikt die zouden kunnen wijzen op een overtreding van de wetgeving of reglementering waarvan de naleving door het Instituut wordt gecontroleerd of van de besluiten van het Instituut genomen ter uitvoering van die wetgeving of reglementering, deelt hij [3 in voorkomend geval]3 zijn grieven mee aan de betrokkene, alsook de beoogde maatregelen bedoeld in paragraaf 5 die toegepast zullen worden, indien de overtreding bevestigd wordt.	**Art. 21.** § 1. Indien de Raad over een reeks aanwijzingen beschikt die zouden kunnen wijzen op een overtreding van de wetgeving of reglementering waarvan de naleving door het Instituut wordt gecontroleerd, ***op een besluit*** van het Instituut genomen ter uitvoering van die wetgeving of reglementering, ***of op een beslissing bedoeld in artikel 105, paragraaf 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie,*** deelt hij in voorkomend geval zijn grieven mee aan de betrokkene, alsook de beoogde maatregelen bedoeld in paragraaf 5 die toegepast zullen worden, indien de overtreding bevestigd wordt.
[…]	[…]