DOC 55 **2572/003**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

10 juin 2022

PROJET DE LOI

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

RAPPORT DE LA PREMIÈRE LECTURE

FAIT AU NOM DE LA COMMISSION
DE L'ÉCONOMIE,
DE LA PROTECTION DES CONSOMMATEURS
ET DE L'AGENDA NUMÉRIQUE
PAR
MM. **Dieter VANBESIEN** ET **Albert VICAIRE**

SOMMAIRE Pages

Voir:

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

Voir aussi:
004: Articles adoptés en première lecture.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

10 juni 2022

WETSONTWERP

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

VERSLAG VAN DE EERSTE LEZING

NAMENS DE COMMISSIE
VOOR ECONOMIE,
CONSUMENTENBESCHERMING
EN DIGITALE AGENDA
UITGEBRACHT DOOR
DE HEREN **Dieter VANBESIEN** EN **Albert VICAIRE**

INHOUD Blz.

Zie:

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

Zie ook:
004: Artikelen aangenomen in eerste lezing.

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Stefaan Van Hecke

A. — Titulaires / Vaste leden:		**B. — Suppléants / Plaatsvervangers:**
N-VA	Michael Freilich, Katrien Houtmeyers, Anneleen Van Bossuyt	Peter De Roover, Joy Donné, Frieda Gijbels, Wouter Raskin
Ecolo-Groen	Barbara Creemers, Stefaan Van Hecke, Albert Vicaire	Laurence Hennuy, Olivier Vajda, Dieter Vanbesien, Gilles Vanden Burre
PS	Christophe Lacroix, Leslie Leoni, Patrick Prévot	Malik Ben Achour, Chanelle Bonaventure, Ahmed Laaouej, Philippe Tison
VB	Erik Gilissen, Reccino Van Lommel	Katleen Bury, Wouter Vermeersch, Hans Verreyt
MR	Denis Ducarme, Florence Reuter	Nathalie Gilson, Kattrin Jadin, Benoît Piedboeuf
CD&V	Leen Dierick	Koen Geens, Jef Van den Bergh
PVDA-PTB	Roberto D'Amico	Maria Vindevoghel, Thierry Warmoes
Open Vld	Kathleen Verhelst	Robby De Caluwé, Christian Leysen
Vooruit	Melissa Depraetere	Anja Vanrobaeys, Kris Verduyckt

C. — Membre sans voix délibérative / Niet-stemgerechtigd lid:

Les Engagés	Maxime Prévot

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

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering 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 definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*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)*

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de ses réunions des 30 mars, 26 avril, 18 mai et 1er juin 2022.

I. — **PROCÉDURE**

Au cours de sa réunion du 30 mars 2022, la commission a décidé, en application de l'article 28.1 du Règlement de la Chambre, de recueillir à propos de ce projet de loi l'avis écrit des personnes et instances suivantes: la *Liga voor Mensenrechten*, la Ligue des droits humains, l'*Orde van Vlaamse Balies*, AVOCATS.BE, le Collège des procureurs généraux, l'Association des juges d'instruction, la Sûreté de l'État, le Service général du renseignement et de la sécurité, le Commissariat général de la Police fédérale, le Comité de vigilance en matière de lutte contre le terrorisme (Comité T), Agoria, ISPA, La Quadrature du Net, Mme Catherine Forget (Université Saint-Louis Bruxelles), Charta21 et l'Organe de contrôle de l'information policière. Les avis reçus ont été mis à la disposition des membres.

La commission a par ailleurs reçu des avis d'initiative de BCPA Belgium et de M. Patrick Breyer, député européen..

II. — **EXPOSÉS INTRODUCTIFS**

A. **Exposé introductif de la ministre en charge des Télécommunications**

Mme Petra De Sutter, vice-première ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste, introduit le projet de loi qui vise principalement à répondre à deux arrêts de la Cour constitutionnelle.

Le premier arrêt est l'arrêt du 22 avril 2021 de la Cour constitutionnelle en matière de conservation de données.

À la suite de l'arrêt *La Quadrature du Net* rendu par la Cour de Justice de l'Union européenne (CJEU) le 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18), la Cour constitutionnelle belge a, par arrêt du 22 avril 2021, annulé les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques. Cette loi est connue sous le nom de "loi *data retention*". Le présent projet vise essentiellement à

DAMES EN HEREN,

Uw commissie heeft dit wetsontwerp besproken tijdens haar vergaderingen van 30 maart, 26 april, 18 mei en 1 juni 2022.

I. — **PROCEDURE**

Tijdens de vergadering van 30 maart 2022 heeft de commissie beslist, met toepassing van artikel 28.1 van het Kamerreglement, schriftelijk advies over dit wetsontwerp in te winnen van de volgende personen en instanties: de Liga voor Mensenrechten, de *Ligue des droits humains,* de Orde van Vlaamse Balies, *AVOCATS. BE*, het College van procureurs-generaal, de Vereniging van Onderzoeksrechters, de Veiligheid van de Staat, de Algemene Dienst Inlichtingen en Veiligheid, het Commissariaat-generaal van de federale politie, het *Comité de vigilance en matière de lutte contre le terrorisme* (Comité T), Agoria, ISPA, *La Quadrature du Net*, mevrouw Catherine Forget (*Université Saint-Louis Bruxelles*), Charta21 en het Controleorgaan op de politionele informatie. De ontvangen adviezen werden de leden ter beschikking gesteld.

De commissie heeft voorts initiatiefadviezen ontvangen van BCPA Belgium en van de heer Patrick Breyer, Europees Parlementslid.

II. — **INLEIDENDE UITEENZETTINGEN**

A. **Inleidende uiteenzetting van de minister bevoegd voor Telecommunicatie**

Mevrouw Petra De Sutter, vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post, licht het wetsontwerp toe. Dit wetsontwerp beoogt in wezen tegemoet te komen aan twee arresten van het Grondwettelijk Hof.

Het eerste arrest, van 22 april 2021, van het Grondwettelijk Hof betreft de gegevensbewaring.

Ten gevolge van het arrest-*La Quadrature du Net*, gewezen door het Hof van Justitie van de Europese Unie (HvJ-EU) op 6 oktober 2020 (samengevoegde zaken C-511/18, C-512/18 en C-520/18), heeft het Belgisch Grondwettelijk Hof, bij arrest van 22 april 2021, de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (de zogeheten "dataretentiewet") vernietigd. Het

réparer cette loi et à rétablir un cadre juridique conforme à la jurisprudence en matière de conservation des “données de trafic et de localisation” au sens de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive “vie privée et communications électroniques”, aussi appelée “directive *e-privacy*”). Cette directive sera remplacée par un règlement, qui utilise une nouvelle terminologie, à savoir “métadonnées” au lieu de “données de trafic et de localisation”.

Cette loi prévoyait l’obligation pour les fournisseurs au public de services de téléphonie, en ce compris par internet, d’accès à l’internet et de courrier électronique par internet (qu’ils soient opérateurs notifiés à l’IBPT ou non) de conserver certaines données de localisation et de trafic, précisées par arrêté royal, pendant une durée de 12 mois, afin que ces données soient disponibles pour des finalités répressives (enquêtes pénales) ou pour l’accomplissement des missions des services de renseignement.

La vice-première ministre fait remarquer que ces données ne concernent pas le contenu des communications. C’est pour cela qu’on parle de “métadonnées” (par exemple “qui appelle qui”). Il ne s’agit donc pas du contenu des appels téléphoniques.

La loi du 29 mai 2016 prévoyait une obligation de conservation généralisée et indifférenciée de certaines métadonnées.

Or, par son arrêt *La Quadrature du Net*, la CJUE a jugé que la conservation généralisée et indifférenciée telle que prévue par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques violait certains principes de droit européen et notamment le droit à la vie privée. Sur la base de la directive e-privacy et de la Charte européenne des droits fondamentaux, l’arrêt de la CJUE a suggéré certaines pistes alternatives à la conservation généralisée et indifférenciée en tout temps:

1) la conservation généralisée et indifférenciée de métadonnées en cas de menace, réelle et actuelle ou prévisible pour la sécurité nationale;

voorliggende wetsontwerp is er voornamelijk op gericht die wet te herstellen en een juridisch kader te scheppen dat strookt met de rechtspraak inzake de bewaring van de “verkeers- en locatiegegevens” in de zin van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie, ook bekend als de “e-privacyrichtlijn”). Deze richtlijn zal worden vervangen door een verordening die een nieuwe terminologie hanteert, met name “metagegevens” in plaats van “verkeers- en locatiegegevens”.

De dataretentiewet voorzag in de verplichting voor aanbieders van openbare telefoniediensten, waaronder ook via het internet, van internettoegang, van e-mail via het internet (ongeacht of ze bij het BIPT al dan niet een kennisgeving hadden gedaan) om bepaalde categorieën locatie- en verkeersgegevens, bepaald bij koninklijk besluit, gedurende een periode van twaalf maanden te bewaren, opdat deze gegevens beschikbaar zouden zijn voor rechtshandhavingsdoeleinden (strafrechtelijk onderzoek) dan wel voor de vervulling van de opdrachten van de inlichtingendiensten.

De vice-eersteminister merkt op dat deze gegevens geen betrekking hebben op de inhoud van de communicatie. Daarom betreft het “metagegevens” (bijvoorbeeld “wie belt wie”). Het gaat dus niet om de inhoud van de telefoongesprekken.

De wet van 29 mei 2016 voorzag in een verplichting tot algemene en ongedifferentieerde bewaring van bepaalde metagegevens.

Het HvJ-EU heeft in zijn arrest-*La Quadrature du Net* echter geoordeeld dat de algemene en ongedifferentieerde bewaring zoals bepaald bij de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, een schending inhield van bepaalde principes van Europees recht, meer bepaald het recht op privacy. Op basis van de e-privacyrichtlijn en van het Handvest van de grondrechten van de Europese Unie heeft het arrest van het HvJ-EU bepaalde alternatieve pistes voor de algemene en ongedifferentieerde databewaring te allen tijde voorgesteld:

1) de algemene en ongedifferentieerde bewaring van metagegevens in geval van een reële en actuele dan wel voorzienbare bedreiging van de nationale veiligheid;

2) la conservation généralisée et indifférenciée des données d'identité civile pour la recherche des infractions ne relevant pas de la criminalité grave;

3) la conservation généralisée et indifférenciée des adresses IP à la source d'une connexion à des fins de lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale;

4) à des fins de lutte contre la criminalité grave et de sauvegarde de la sécurité publique, la conservation ciblée de métadonnées sur une base géographique ou sur la base des personnes dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers, et la conservation rapide de métadonnées ("*quick-freeze*"), à savoir une demande de gel de métadonnées relatives à une personne sur une courte période.

Dans son arrêt d'annulation du 22 avril 2021, la Cour constitutionnelle a repris l'argumentaire de la CJUE.

Dans le projet de loi, certaines pistes évoquées par la CJUE ont été suivies et développées, d'autres pas comme la conservation ciblée sur la base des personnes dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers.

Par ailleurs, la vice-première ministre souligne que des garanties complémentaires ont également été ajoutées au niveau du traitement de ces données par les opérateurs (les mesures de sécurité imposées aux opérateurs sont plus détaillées), ainsi qu'au niveau de la fourniture de ces données aux autorités (encadrement plus strict des conditions entourant cette fourniture et contrôle préalable de la demande de l'autorité envers l'opérateur). Les exigences de la jurisprudence ont ainsi été mises en œuvre.

Enfin, le projet de loi vise également à répondre aux attentes sociétales d'un monde de plus en plus digitalisé: les transactions électroniques (e-commerce) deviennent la norme dans beaucoup de secteurs. Afin de lutter contre certaines formes d'infractions se commettant exclusivement en ligne, il est donc nécessaire que les autorités chargées de la prévention, de la détection et de la poursuite de ces infractions puissent obtenir des opérateurs les données dont ils disposent, dans la mesure nécessaire à l'accomplissement de leurs missions respectives. C'est dans cette optique qu'il est prévu, au chapitre 8 du projet de loi, d'accorder au Service d'inspection des produits de consommation du SPF Santé publique, Sécurité de

2) de algemene en ongedifferentieerde bewaring van burgerlijke-identiteitsgegevens voor het onderzoek naar strafbare feiten die niet onder zware criminaliteit ressorteren;

3) de algemene en ongedifferentieerde bewaring van bron-IP-adressen, ter bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid;

4) met het oog op de bestrijding van zware criminaliteit en ter bescherming van de openbare veiligheid, de gerichte bewaring van metagegevens, op een geografische basis of op basis van personen in bepaalde gebieden of voor bepaalde categorieën van personen van wie vooraf is vastgesteld dat zij een specifiek risico vormen, en snelle bewaring van metagegevens ("*quick freeze*"), waarbij wordt verzocht de metagegevens van een persoon gedurende een korte periode te bevriezen.

In zijn vernietigingsarrest van 22 april 2021 heeft het Grondwettelijk Hof de analyse van het HvJ-EU overgenomen.

In het wetsontwerp zijn sommige van de door het HvJ-EU aangegeven pistes gevolgd en uitgewerkt, andere dan weer niet, zoals de gerichte bewaring op basis van personen in bepaalde gebieden of voor bepaalde categorieën van personen van wie vooraf is vastgesteld dat zij een specifiek risico vormen.

De vice-eersteminister benadrukt voorts dat ook extra waarborgen zijn toegevoegd met betrekking tot de verwerking van deze gegevens door de operatoren (de aan de operatoren opgelegde veiligheidsmaatregelen werden uitgediept), alsook met betrekking tot de verstrekking van deze gegevens aan de autoriteiten (een strikter toezicht op de voorwaarden voor deze verstrekking en een voorafgaande controle van het verzoek van de autoriteit aan de operator). Aldus is uitvoering gegeven aan de vereisten van de rechtspraak.

Ten slotte beoogt dit wetsontwerp tevens in te spelen op de maatschappelijke verwachtingen van een almaar digitaler wordende wereld. Het is duidelijk dat de elektronische transacties (e-commerce) in heel wat sectoren de norm worden. Ter bestrijding van bepaalde vormen van strafbare feiten die uitsluitend online worden gepleegd, is het derhalve noodzakelijk dat de autoriteiten die zijn belast met de preventie, de opsporing en de vervolging van deze feiten, de gegevens kunnen opvragen bij de operatoren die deze in hun bezit hebben, voorzover zulks nodig is om hun respectieve opdrachten te vervullen. Daartoe wordt in hoofdstuk 10 van het wetsontwerp beoogd de inspectiedienst consumptieproducten van de

la Chaîne alimentaire et Environnement, la possibilité d'identifier des personnes morales ou physiques sur la base d'un numéro de téléphone ou d'une adresse IP. Il ne s'agit en d'autres termes que de données qui ne donnent pas d'information précise sur la vie privée des personnes concernées puisqu'elles concernent des données d'identification. Sans la fourniture de ces données, il y aurait une impossibilité matérielle pour ce service de remplir sa mission légale et les enquêtes resteraient immuablement à charge de "X".

L'arrêt d'annulation de la Cour constitutionnelle du 22 avril 2021 a également rendu nécessaire une modification de l'arrêté royal 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après "arrêté royal data"). En outre, l'arrêt d'annulation a également rendu nécessaire la modification de certaines lois organiques, notamment le Code d'instruction criminelle, ou la loi sur la fonction de police. Ce sont ces lois organiques qui fixent les conditions de fourniture des données conservées par les opérateurs aux différentes autorités concernées.

S'agissant de l'historique du dossier, ce dernier a déjà accompli un long chemin.

Le gouvernement a demandé et reçu l'avis:

— du Conseil d'État (hormis sur le projet d'arrêté royal);

— de l'Autorité de protection des données;

— de l'Organe de contrôle de l'information policière (autorité de contrôle spécifique des services de police);

— du Comité permanent R (autorité de contrôle spécifique des services de renseignement);

— de la magistrature (dans le cadre du Conseil national de sécurité);

— des opérateurs, dans le cadre d'une consultation publique de quatre semaines organisée par l'IBPT, conformément à l'article 18 du Code des communications électroniques européen.

Des modifications ont été apportées sur la base de la consultation publique, de l'avis du Conseil d'État et de l'avis des différentes autorités de protection des données.

Le 23 décembre 2021, l'avant-projet de loi et le projet d'"arrêté royal data" ont été soumis au Comité interministériel des Télécommunications et de la Radiodiffusion

FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, in de mogelijkheid te stellen rechtspersonen of natuurlijke personen te identificeren op basis van een telefoonnummer of een IP-adres. Het gaat met andere woorden alleen om gegevens die geen precieze informatie geven over het privéleven van de betrokken personen, aangezien het identificatiegegevens betreft. Zonder deze toegang zou het deze dienst materieel niet mogelijk zijn diens wettelijke taak te vervullen en zouden de onderzoeken altijd ten laste van "X" blijven vallen.

Het vernietigingsarrest van het Grondwettelijk Hof van 22 april 2021 heeft tevens tot gevolg dat het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie moet worden gewijzigd. Bovendien noopte het vernietigingsarrest tot de wijziging van bepaalde organieke wetten, met name het Wetboek van Strafvordering en de wet op het politieambt. Deze organieke wetten bepalen de voorwaarden voor de verstrekking van de door de operatoren bewaarde gegevens aan de diverse betrokken autoriteiten.

Het dossier heeft al een heel traject doorlopen.

De regering heeft het advies gevraagd en ontvangen van:

— de Raad van State (behalve over het ontwerp van koninklijk besluit);

— de Gegevensbeschermingsautoriteit;

— het Controleorgaan op de politionele informatie (specifieke controleoverheid voor de politiediensten);

— het Vast Comité I (specifieke controleoverheid voor de inlichtingendiensten);

— de magistratuur (binnen het kader van de Nationale Veiligheidsraad);

— de operatoren, in het kader van een openbare raadpleging van vier weken die door het BIPT georganiseerd werd, conform artikel 18 van het Europees Wetboek voor elektronische communicatie.

Er werden wijzigingen doorgevoerd op basis van de openbare raadpleging, het advies van de Raad van State en het advies van de diverse gegevensbeschermingsautoriteiten.

Op 23 december 2021 werden het voorontwerp van wet en het ontwerp van "koninklijk besluit data" voorgelegd aan het Interministerieel Comité voor Telecommunicatie en

et la Télévision (conformément à l'article 9, alinéa 2, de l'accord de coopération du 17 novembre 2006). Le Comité interministériel n'a pas fait de remarques. Les textes ont été soumis au Comité de concertation le 2 février 2022. Le Comité de concertation n'a pas non plus formulé d'observations.

Bref, à la fin de l'année dernière, le gouvernement avait élaboré un projet de réparation de la "loi *data retention*". Ce projet a été approuvé par le Conseil des ministres du 17 décembre 2021. Pour ce projet, tous les avis nécessaires ont été reçus, et le gouvernement a donc prévu de le soumettre au Parlement dès que possible.

Comme mentionné ci-dessus, le projet de loi à l'examen vise à se conformer à deux arrêts de la Cour constitutionnelle. Le second est l'arrêt du 18 novembre 2021 sur l'identification des utilisateurs.

Le 18 novembre 2021, la Cour constitutionnelle a en effet rendu un arrêt au sujet de la loi du 1er septembre 2016. Cette loi a été adoptée après les attentats de Paris, afin de mettre fin à l'anonymat des utilisateurs de cartes prépayées permettant l'utilisation de services mobiles (appel, accès à Internet, envoi de SMS, etc.) en obligeant les opérateurs à les identifier.

Dans cet arrêt, la Cour ne remet pas en cause le principe de l'identification des utilisateurs de cartes prépayées, mais elle annule la modification apportée par la loi du 1er septembre 2016 à l'article 127 de la loi du 13 juin 2005, "uniquement en ce qu'(elle) ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération". La Cour considère que l'article 22 de la Constitution exige que ces données et documents soient énumérés dans la loi. Elle maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus.

L'arrêt du 18 novembre 2021 de la Cour constitutionnelle porte uniquement sur l'article 127 de la loi du 13 juin 2005. Lorsqu'on analyse cette décision, on constate toutefois que ses enseignements – à savoir le fait que les données à conserver par les opérateurs doivent être mentionnées dans la loi – s'appliquent également aux articles 126 et 126/1 de cette loi tels qu'ils figurent dans le projet de loi relatif à la "conservation des données". Il s'ensuit que ces articles 126 et 126/1 doivent également être modifiés.

Radio-omroep en Televisie (conform artikel 9, tweede lid, van het samenwerkingsakkoord van 17 november 2006). Het Interministerieel Comité heeft geen opmerkingen geformuleerd. De teksten werden aan het Overlegcomité voorgelegd op 2 februari 2022. Het Overlegcomité had evenmin opmerkingen.

Eind vorig jaar had de regering dus een ontwerp van remediëring van de "dataretentiewet" klaar. Dat ontwerp werd goedgekeurd door de Ministerraad van 17 december 2021. Voor dat ontwerp werden alle noodzakelijke adviezen ontvangen, en de regering was dus van plan om naar het Parlement te gaan zodra dat mogelijk was.

Zoals gezegd streeft het wetsontwerp ernaar tegemoet te komen aan twee arresten van het Grondwettelijk Hof. Het tweede arrest is het arrest van 18 november 2021 inzake identificatie van de gebruikers.

Het Grondwettelijk Hof heeft op 18 november 2021 inderdaad een arrest gewezen met betrekking tot de wet van 1 september 2016. Deze wet werd aangenomen na de aanslagen van Parijs, om een einde te maken aan de anonimiteit van de gebruikers van voorafbetaalde kaarten aan de hand waarvan mobiele diensten kunnen worden gebruikt (bellen, internettoegang, sms'en versturen enzovoort), door de operatoren te verplichten deze laatsten te identificeren.

In dat arrest stelt het Hof het principe van identificatie van de gebruikers van voorafbetaalde kaarten niet ter discussie, maar vernietigt het de wijziging aangebracht bij de wet van 1 september 2016 in artikel 127 van de wet van 13 juni 2005 "zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen". Volgens het Hof bepaalt artikel 22 van de Grondwet dat deze gegevens en documenten moeten worden opgesomd in de wet. Het Hof behoudt de gevolgen van de vernietigde bepaling tot de inwerkingtreding van een wetskrachtige norm waarin die identificatiegegevens en identificatiedocumenten worden opgesomd en uiterlijk tot en met 31 december 2022.

Het arrest van het Grondwettelijk Hof van 18 november 2021 heeft enkel betrekking op artikel 127 van de wet van 13 juni 2005. Na analyse van het arrest is echter gebleken dat de lessen van het arrest – namelijk dat de door de operatoren te bewaren gegevens in de wet moeten worden opgenomen – ook van toepassing zijn op de artikelen 126 en 126/1 van die wet zoals deze in het wetsontwerp "dataretentie" zijn voorzien. Daaruit volgt dat die artikelen 126 en 126/1 eveneens gewijzigd moeten worden.

À cet effet, le gouvernement présentera dans les semaines à venir des amendements au projet de loi à l'examen. Il s'agit donc d'un deuxième volet de ce dossier. Compte tenu de l'importance et de l'urgence de la matière, le gouvernement a toutefois jugé opportun de soumettre dès à présent le premier volet au Parlement.

La vice-première ministre rappelle enfin que ce projet de loi réparatrice est le résultat du travail considérable fourni par de nombreux services et experts et en particulier par l'IBPT, qu'elle tient à remercier chaleureusement. La tâche n'a pas été facile puisque le projet de loi relève de la responsabilité de plusieurs ministres, à savoir:

— elle-même en tant que ministre des Télécommunications;

— le ministre de la Justice, car les données sont principalement conservées à des fins judiciaires;

— la ministre de la Défense, car les services de renseignement utilisent également les données conservées par les opérateurs;

— mais aussi les ministres responsables des différentes lois organiques qui ont été modifiées, c'est-à-dire:

• la ministre Verlinden pour les modifications apportées à la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;

• le secrétaire d'État Michel pour les modifications apportées à la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;

• le ministre Van Quickenborne pour les modifications apportées au Code d'instruction criminelle;

• la ministre Verlinden pour les modifications apportées à la loi du 5 août 1992 sur la fonction de police;

• la ministre Dedonder pour les modifications apportées à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

• le ministre Van Peteghem pour les modifications apportées à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers;

• le premier ministre De Croo pour les modifications apportées à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS");

De regering zal daartoe in de komende weken amendementen indienen op het voorliggende wetsontwerp. Er komt dus een tweede deel bij dit dossier. Gelet op het belang van het dossier en de hoogdringendheid achtte de regering het niettemin aangewezen het eerste deel reeds in te dienen bij het Parlement.

Tot slot herinnert de vice-eersteminister eraan dat dit ontwerp van remediëringswet het resultaat is van het harde werk van vele diensten en deskundigen, en in het bijzonder van het BIPT, die zij van harte wenst te bedanken. Het was geen gemakkelijke opdracht omdat het wetsontwerp onder de verantwoordelijkheid van verschillende ministers valt, met name:

— zijzelf, als minister van Telecommunicatie;

— de minister van Justitie, omdat de gegevens hoofdzakelijk voor gerechtelijke doeleinden worden bewaard;

— de minister van Defensie, omdat de inlichtingendiensten ook gebruikers zijn van de door de operatoren bewaarde gegevens;

— maar ook de ministers die verantwoordelijk zijn voor de verschillende organieke wetten die zijn gewijzigd, zijnde:

• minister Verlinden voor de wijziging van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;

• staatssecretaris Michel voor de wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

• minister Van Quickenborne voor de wijzigingen van het Wetboek van strafvordering;

• minister Verlinden voor de wijzigingen van de wet van 5 augustus 1992 op het politieambt;

• minister Dedonder voor de wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

• minister Van Peteghem voor de wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten;

• premier De Croo voor de wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet");

• le ministre Vandenbroucke pour les modifications apportées à la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits.

Le projet à l'examen est également le résultat d'une mise en balance difficile de différents éléments:

— le droit individuel à une protection correcte des données à caractère personnel;

— le droit collectif à la sécurité et les besoins opérationnels des services de police et de renseignement;

— les possibilités techniques des opérateurs et la nécessité de pouvoir disposer d'un cadre juridique stable.

B. **Exposé introductif du ministre en charge de la Justice**

M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice et de la Mer du Nord, indique que le texte à l'examen présente un intérêt capital pour la justice et la police, pour l'élucidation d'infractions et pour l'identification et la poursuite des auteurs.

Le vice-premier ministre tient tout d'abord à préciser la notion de "métadonnées". Une certaine presse assimile le texte à l'examen à une loi sur les écoutes, mais il ne s'agit pas de cela. En effet, le projet de loi porte non sur l'interception du contenu de communications, mais sur les données d'identification, de localisation et de trafic.

Les données d'identification sont des données qui permettent de répondre aux questions suivantes: à qui appartient par exemple un numéro de téléphone ou une adresse IP déterminés? Quels sont les numéros de téléphone d'une personne?

Les données de trafic permettent de répondre aux questions suivantes: qui a communiqué avec qui? (Qui a appelé un numéro déterminé? Qui a surfé sur un site internet déterminé?)

Il y a enfin les données de localisation, qui permettent d'associer un appareil ou un point de raccordement à un lieu concret et inversement. À partir de quel pylône un appel a-t-il été envoyé? Quels étaient les appareils reliés à un pylône déterminé à un moment donné?

Les utilisateurs des services de communication électronique et les opérateurs génèrent donc beaucoup de signaux lorsqu'ils communiquent ou tentent de communiquer entre eux, et laissent de nombreuses traces

• minister Vandenbroucke voor de wijziging van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten.

Het voorliggende ontwerp is voorts de vrucht van een moeilijke evenwichtsoefening tussen:

— het individuele recht op het correct beschermen van persoonsgegevens;

— het collectieve recht op veiligheid en de operationele behoeften van de politie- en inlichtingendiensten;

— en de technische mogelijkheden van de operatoren en de nood aan een stabiel juridisch kader.

B. **Inleidende uiteenzetting van de minister bevoegd voor Justitie**

De heer Vincent Van Quickenborne, vice-eersteminister en minister van Justitie en Noordzee, geeft aan dat de voorliggende tekst van groot belang is voor justitie en politie, voor de opheldering van misdrijven en voor de opsporing en de vervolging van de daders.

Bij wijze van inleiding verduidelijkt de vice-eersteminister de term "metadata". In bepaalde pers wordt dit wetsontwerp de afluisterwet genoemd, maar die vlag dekt de lading niet. Deze tekst heeft het immers niet over het onderscheppen van de inhoud van communicatie, maar wel over de identificatiegegevens, de locatiegegevens en de verkeersgegevens.

De identificatiegegevens zijn gegevens die het mogelijk maken na te gaan wie bijvoorbeeld achter een bepaald telefoonnummer of een bepaald IP-adres zit, of welke de telefoonnummers van een persoon zijn.

De verkeersgegevens zijn gegevens die het mogelijk maken na te gaan wie heeft gecommuniceerd met wie (Wie heeft een bepaald nummer gebeld? Wie heeft een bepaalde website bezocht?).

Tot slot zijn er de locatiegegevens. Die maken het mogelijk een toestel of verbindingspunt aan een concrete plaats te koppelen, en omgekeerd. Van welke zendmast kwam een oproep? Welke toestellen waren verbonden met een bepaalde zendmast op een bepaald moment?

De gebruikers van elektronische communicatiediensten en de operatoren genereren dus veel signalen wanneer ze met elkaar (proberen te) communiceren; ze laten veel sporen achter. Die sporen kunnen vervolgens door de

derrière eux. Ces traces peuvent ensuite être utilisées par les autorités judiciaires ou les services de renseignement à différents moments de l'enquête.

Les données d'identification et les données de localisation et de trafic sont souvent combinées et sont utilisées à la fois à charge et à décharge.

Ces métadonnées constituent dès lors un élément central de l'enquête: elles sont objectives et fiables et sont mises à profit dans près de 95 % des enquêtes pénales. Leur intérêt est inestimable. Le vice-premier ministre cite quelques exemples:

— Lorsqu'on trouve un corps et qu'il n'y a pas de témoins, ni de traces exploitables, le tribunal réclame les données de tous les appareils qui se trouvaient à proximité des lieux au moment présumé du décès. C'est ainsi que l'on recherche des suspects potentiels.

— En cas de disparations inquiétantes, on examine toujours les derniers endroits où un appareil s'est connecté à une antenne. Il est également possible d'examiner si cet appareil se connecte quelque part à une antenne au même moment.

— En ce qui concerne les victimes de la traite ou du trafic des êtres humains, du crime organisé ou du terrorisme, l'enquête doit se concentrer sur les personnes de contact et sur les lieux pour démasquer les réseaux et rechercher les auteurs.

Dans chacun de ces dossiers, le tribunal a recours aux métadonnées pour faire progresser l'enquête.

Le vice-premier ministre indique qu'il va poursuivre son intervention en commençant par commenter la nouvelle approche proposée. Il expliquera ensuite comment il entend régler l'accès aux données dans le prolongement de ce qui existe déjà aujourd'hui, puis il évoquera les solutions de l'Union européenne et d'autres États membres. Enfin, avant de conclure, il commentera les avis reçus et la manière dont leurs principaux points ont été pris en compte.

La nouvelle approche à l'égard de la rétention de données

L'arrêt *La Quadrature du Net* de la CJUE du 6 octobre 2020 indique que la conservation générale et indifférenciée des métadonnées de communication est l'exception et non la règle. En d'autres termes, le système prévu dans la loi du 13 juin 2005 qui imposait aux opérateurs de

rechterlijke macht of door de inlichtingendiensten worden gebruikt op uiteenlopende momenten van het onderzoek.

De identificatiegegevens en de locatie- en verkeersgegevens worden vaak gekruist en worden zowel à charge als à decharge gebruikt.

Deze metadata zijn dan ook een centraal onderdeel van het onderzoek: ze zijn objectief en betrouwbaar en worden in zowat 95 % van de strafonderzoeken gebruikt. Het belang ervan valt nauwelijks te onderschatten. De vice-eersteminister geeft enkele voorbeelden:

— Wanneer een lichaam wordt gevonden en er geen getuigen zijn of goede sporen zijn, vraagt het gerecht gegevens op van alle toestellen die zich omstreeks het vermoedelijke tijdstip van overlijden in de buurt van die plaats bevonden. Zo zoekt men mogelijke verdachten.

— Bij onrustwekkende verdwijningen wordt altijd gekeken naar de laatste plaatsen waar een toestel met een zendmast was verbonden. Er is ook een manier om te kijken of dat toestel op dat moment ergens met een zendmast verbinding maakt.

— Bij slachtoffers van mensenhandel of mensensmokkel, bij georganiseerde misdaad of terrorisme moet onderzoek worden gevoerd naar de contactpersonen en locaties om netwerken te ontdekken en daders op te sporen.

Bij elk van die dossiers doet het gerecht een beroep op metadata om het onderzoek vooruit te helpen.

In het vervolg van zijn betoog zal de vice-eersteminister eerst het voorstel van nieuwe aanpak toelichten. Vervolgens zal hij schetsen hoe in de toegang tot de data wordt voorzien, voortbouwend op wat vandaag al bestaat. Daarna zal hij een blik werpen op de oplossingen van de EU en van andere lidstaten. Alvorens te besluiten zal hij nog ingaan op de ontvangen adviezen en de manier waarop met de belangrijkste punten daarvan rekening werd gehouden.

De nieuwe aanpak voor dataretentie

Het arrest-*Quadrature du Net* van het HvJ-EU van 6 oktober 2020 geeft aan dat de algemene en ongedifferentieerde bewaring van de communicatiemetagegevens de uitzondering is, niet de regel. Zulks houdt in dat de verplichting waarin de wet van 13 juni 2005

conserver d'office ces métadonnées pendant 12 mois au profit des *law enforcement authorities* n'est plus autorisé.

Le message de la Cour européenne, réitéré par notre Cour constitutionnelle, est donc clair: la *data retention* n'est permise que si elle est ciblée et strictement nécessaire.

Pour le ministre de la Justice, il est particulièrement important que les droits et libertés individuels soient respectés et que les dérogations ne soient autorisées que dans la mesure où elles sont strictement nécessaires dans une société démocratique. Il est évident que ces métadonnées concernent la vie privée des gens et que l'accès à ces données et leur utilisation sont donc "intrusifs".

Il faut donc se fixer pour règle que les pouvoirs publics n'auront rien à voir avec ces données (ni avec les métadonnées, ni avec le contenu de la communication), lesquelles relèvent de la sphère privée. Les données ne seront pas conservées par les pouvoirs publics, mais bien par les opérateurs télécoms.

Il existe toutefois une exception. Les services de renseignement et de sécurité peuvent obtenir à la fois des métadonnées et le contenu de la communication auprès des opérateurs. Cette procédure est strictement encadrée: l'accès n'est pas systématique. Cette procédure ne s'applique que dans certains cas bien définis, sur réquisition d'un procureur (à des fins d'identification) ou d'un juge (juge d'instruction ou commission BIM) (localisation et échanges). Pour la prise de connaissance du contenu de la communication, le Code d'instruction criminelle prévoit des règles encore plus strictes.

C'est pourquoi il a également été prévu que les données ne seront pas conservées par les pouvoirs publics, mais bien par les opérateurs eux-mêmes. Étant donné qu'il faut toujours éviter que ces données fassent l'objet d'abus (y compris par des acteurs autres que la justice et la police), leur conservation par les opérateurs est soumise à des règles et à des procédures strictes.

Pour permettre l'accès à celles-ci, des règles concernant la conservation des données ont également été fixées. Ces règles sont conformes aux principes de la protection des données. Il faut donc distinguer clairement la conservation, d'une part, de l'accès, d'autre part.

Les arrêts récemment rendus par la Cour constitutionnelle et la CJUE en matière de rétention des données et, plus précisément, de conservation des données, ont

voor de operatoren voorzag om die metagegevens automatisch gedurende een periode van twaalf maanden te bewaren voor de *law enforcement authorities,* niet langer toegestaan is.

De boodschap van het Europees Hof, herhaald door het Belgische Grondwettelijk Hof, is dan ook duidelijk: alleen gerichte en strikt noodzakelijke dataretentie is toegestaan.

Voor de minister van Justitie is het bijzonder belangrijk dat de individuele rechten en vrijheden worden geëerbiedigd en dat daarvan slechts wordt afgeweken in de mate waarin zulks strikt noodzakelijk is in een democratische samenleving. Het moge duidelijk zijn dat deze metadata betrekking hebben op het privéleven van mensen, en dat de toegang tot en het gebruik van die gegevens dus "intrusief" zijn.

De regel moet dus duidelijk luiden dat de overheid geen uitstaans heeft met deze gegevens (noch met de metadata noch met de inhoud van de communicatie). Dit behoort tot de privésfeer. Ze worden niet bij de overheid bewaard maar wel bij de telecomoperatoren.

Er is evenwel een uitzondering. Er bestaat een manier voor inlichtingen- en veiligheidsdiensten om zowel metadata als de inhoud van de communicatie van de operatoren te verkrijgen. Dit is streng geregeld: er is geen systematische toegang. Dit gebeurt alleen in welomschreven gevallen, op vordering van een procureur (voor identificatie) of een rechter (onderzoeksrechter dan wel BIM-commissie) (voor locatie en verkeer). Om kennis te nemen van de inhoud van de communicatie zijn er nog strengere regels bepaald in het Wetboek van Strafvordering.

Daarom is ook bepaald dat de gegevens niet worden bewaard door de overheid, maar wel door de operatoren zelf. Misbruik van deze data (ook door andere actoren dan justitie en politie) moet te allen tijde voorkomen worden, vandaar dat deze bewaring door de operatoren gebeurt volgens strenge regels en procedures.

Om de toegang mogelijk te maken, zijn er ook regels bepaald over de bewaring van de gegevens. Deze regels beantwoorden aan de beginselen van gegevensbescherming. Er moet dus een duidelijk onderscheid gemaakt worden tussen de bewaring enerzijds en de toegang anderzijds.

De recente arresten van het Grondwettelijk Hof en het HvJ-EU op het gebied van dataretentie en meer bepaald over de bewaring van gegevens hebben de regering

obligé le gouvernement à mener une réflexion approfondie sur la conservation d'un équilibre entre le caractère strictement nécessaire de l'ingérence dans la vie privée, soit la conservation des données à caractère personnel par les opérateurs, pour la sûreté de notre société, et le droit au respect de la vie privée. Le gouvernement a élaboré un système qui garantit qu'il n'y aura pas de régression opérationnelle dans la "recherche de la vérité" tout en respectant totalement les limites définies par la jurisprudence de la Cour constitutionnelle et de la CJUE.

Le texte à l'examen propose une approche totalement nouvelle de la conservation des données qui se fonde sur une analyse à la fois objective et dynamique des risques en matière de sûreté dans chaque arrondissement judiciaire, dans chaque zone de police et dans tous les lieux stratégiques de notre pays.

Le vice-premier ministre rappelle que le projet n'est pas une simple réparation en matière de *data retention* mais une façon nouvelle de concevoir la manière et les limites pour réaliser à titre préventif une conservation des données: il n'y a plus d'office de conservation généralisée et indifférenciée sur l'ensemble du territoire belge des métadonnées. Seule une conservation ciblée sur la base de critères objectifs, dynamiques, auditables et audités sera permise.

Ces critères feront également l'objet d'un contrôle annuel effectif.

Quelles sont donc les nouvelles approches proposées par le gouvernement pour cibler cette *data retention*?

(i) Critère statistique

Une conservation des métadonnées des communications, et leur durée, est organisée par arrondissement judiciaire sur la base d'un pourcentage statistique des faits relevant de la criminalité grave fixé dans la loi. Concrètement, il s'agit du nombre moyen d'infractions pénales visées à l'article 90*ter* du Code d'instruction criminelle (C.I.cr.), enregistrées sur une période de trois ans. À partir du moment où une moyenne de trois infractions pénales graves sont commises par 1 000 habitants par an dans un arrondissement judiciaire, les données sont conservées dans cet arrondissement.

Le vice-premier ministre explique la double motivation d'avoir choisi comme critère la liste des infractions reprises à l'article 90*ter*, §§ 2 à 4, C.I.cr.

Cette disposition reprend tout d'abord la liste des formes de criminalité généralement considérées comme les plus graves. Il s'agit notamment des attentats à la

genoopt grondig na te denken over hoe men het evenwicht kan bewaren tussen de strikt noodzakelijke aard van de inmenging in het privéleven, zijnde de bewaring van persoonsgegevens door de operatoren, voor de veiligheid van onze samenleving, en het recht op een privéleven. De regering heeft een systeem uitgewerkt waarbij ervoor wordt gezorgd dat er geen operationele regressie is in de "waarheidsbevinding", terwijl er toch volledig binnen de krijtlijnen van de rechtspraak van het Grondwettelijk Hof en het HvJ-EU wordt gebleven.

De voorliggende tekst is een volledig vernieuwende benadering op het gebied van de bewaring van gegevens, die gebaseerd is op een zowel objectieve als dynamische analyse van de veiligheidsrisico's, op het niveau van elk gerechtelijk arrondissement, elke politiezone en alle strategische plaatsen van ons land.

De vice-eersteminister wijst erop dat het wetsontwerp niet louter een reparatie inzake dataretentie beoogt, maar erop gericht is een nieuwe regeling en nieuwe grenzen te bepalen om preventief gegevens te bewaren: op het volledige Belgische grondgebied worden de metagegevens niet langer automatisch algemeen en ongedifferentieerd bewaard. Alleen de gerichte bewaring op grond van objectieve, dynamische, controleerbare en gecontroleerde criteria zal worden toegestaan.

Deze criteria zullen ook effectief jaarlijks gecontroleerd worden.

Wat behelst de nieuwe door de regering voorgestelde aanpak inzake dataretentie?

(i) Statistisch criterium

Er wordt een bewaring georganiseerd van de metadata van communicatie, en de duur ervan, per gerechtelijk arrondissement, aan de hand van een in de wet vastgesteld statistisch percentage van zware criminele feiten. *In concreto* gaat het over het gemiddelde aantal strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering, die over een periode van drie jaar zijn geregistreerd. Zodra gemiddeld drie zware strafbare feiten per 1 000 inwoners per jaar in een gerechtelijk arrondissement gepleegd worden, worden er in dat arrondissement data bewaard.

De vice-eersteminister geeft aan dat er twee redenen zijn waarom de lijst van strafbare feiten vervat in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering als criterium werd gekozen.

In dat artikel worden eerst en vooral de vormen van criminaliteit opgesomd die doorgaans als de zwaarste worden beschouwd. Men denke aan: aanranding van de

pudeur sur mineur et majeur, des viols, des enlèvements et recels de mineur, des organisations criminelles, de la traite des êtres humains.

Ensuite, la liste des infractions énumérées à l'article 90*ter*, §§ 2 à 4, est également utilisée pour permettre le recours à des mesures plus attentatoires à la vie privée. C'est par exemple le cas de la mesure d'interception et de prise de connaissance de communications non accessibles au public ou de la mesure de recherche secrète dans un système informatique.

L'Organe de contrôle de l'information policière a, dans son avis sur ce projet de loi, validé ce choix en indiquant que "[l]adite "liste des écoutes" de l'art. 90*ter* C.i.cr. est, *de lege lata*, en droit belge, le seul véritable critère utilisable pour pouvoir différencier lesdits "délits graves" de la "criminalité ordinaire"".

En fonction du nombre moyen de faits, quatre durées de conservation sont alors possibles: aucune conservation des données au niveau de l'arrondissement, une conservation pendant six mois, une conservation pendant neuf mois et une conservation pendant douze mois.

Si le seuil de trois infractions graves par 1 000 habitants n'est pas atteint dans un arrondissement, les données ne seront plus conservées au niveau de l'ensemble de l'arrondissement, mais au niveau d'une entité géographique plus petite, à savoir, la zone de police. Le même système temporel variable en fonction du taux de criminalité (rien, six mois, neuf mois, douze mois) est d'application.

Voici quelques exemples concrets pour clarifier les choses. Anvers est le plus grand arrondissement judiciaire de Belgique en termes de population: 1 869 730 habitants en 2019. À Anvers, ce seuil de trois faits pour 1 000 habitants, qui implique que les métadonnées peuvent être conservées pendant six mois, signifie qu'au cours des trois dernières années, une moyenne de 5 609 infractions graves par an doit avoir eu lieu.

Pour l'arrondissement de Bruxelles (1 218 255 habitants en 2019), ce seuil signifie qu'il doit y avoir eu une moyenne de 3 655 infractions graves par an au cours des trois dernières années.

Pour un arrondissement comme Charleroi (583 928 habitants en 2019), ceci implique qu'il y ait eu 1 752 faits en moyenne sur les trois dernières années ou sur un total de trois ans, 5 256 faits graves.

Par ces illustrations, le vice-premier ministre démontre que le seuil de trois faits de la liste de l'article 90*ter*, §§ 2 à 4, C.i.cr. par 1 000 habitants correspond à un nombre

eerbaarheid van minder- en meerderjarigen, verkrachting, ontvoering en verberging van minderjarigen, criminele organisaties en mensenhandel.

Voorts wordt op basis van de lijst van strafbare feiten opgesomd in artikel 90*ter*, §§ 2 tot 4, tevens overgegaan tot het nemen van meer intrusieve maatregelen op het vlak van de persoonlijke levenssfeer, zoals de onderschepping en kennisname van communicatie die niet toegankelijk is voor het publiek, alsook de geheime zoeking in een informaticasysteem.

In zijn advies inzake dit wetsontwerp stemt het Controleorgaan op de politionele informatie (COC) in met die keuze: "De zgn. "taplijst" van art. 90*ter* Sv. is *de lege lata* naar Belgisch recht het enige echt bruikbare criterium om zgn. "zware misdrijven" te kunnen onderscheiden van "gewone criminaliteit".

Er zijn, afhankelijk van het gemiddelde aantal feiten, vervolgens vier bewaartermijnen mogelijk: geen retentie van gegevens op niveau van het arrondissement, retentie gedurende zes maanden, retentie gedurende negen maanden en retentie gedurende twaalf maanden.

Als de drempel van drie zware feiten per 1 000 inwoners van een arrondissement niet wordt gehaald, zullen de gegevens niet langer worden bewaard voor het gehele arrondissement, maar wel op kleinere schaal, namelijk op het niveau van de politiezone. Naargelang van de criminaliteitscijfers is dezelfde variabele temporele regeling van toepassing (geen retentie, zes maanden, negen maanden, twaalf maanden).

Enkele concrete voorbeelden ter verduidelijking. Antwerpen is het grootste gerechtelijk arrondissement in België qua inwoners: 1 869 730 inwoners in 2019. In Antwerpen impliceert deze drempel van drie incidenten per 1 000 inwoners, waarbij de metadata gedurende zes maanden zouden kunnen worden bewaard, dat er zich in de afgelopen drie jaar gemiddeld 5 609 zware strafbare feiten per jaar moeten hebben voorgedaan.

Voor het arrondissement Brussel (1 218 255 inwoners in 2019) betekent deze drempel dat er in de afgelopen drie jaar gemiddeld 3 655 zware strafbare feiten per jaar moeten zijn geweest.

Voor een arrondissement als Charleroi (583 928 inwoners in 2019) impliceert zulks dat er de afgelopen drie jaar gemiddeld 1 752 zware strafbare feiten zijn geweest, zijnde 5 256 zware feiten op een totaal van drie jaar.

Met die voorbeelden wil de vice-eersteminister aan te tonen dat de drempel van drie feiten van de lijst van artikel 90*ter*, §§ 2 tot 4, van het Wetboek van Strafvordering,

très élevé de faits de criminalité grave. Ce nombre élevé indique également un enracinement de la criminalité grave au sein de l'arrondissement. Ce seuil a aussi évidemment un impact sur la sécurité de la population, et pour certaines infractions sur les attentes légitimes des victimes d'être assistées: qu'elles soient secourues mais également que les auteurs de l'infraction perpétrée qui leur a causé préjudice soient identifiés et poursuivis.

L'avis de *Child Focus* et celui de l'Institut pour l'Égalité des Femmes et des Hommes corroborent tout à fait ce point.

(ii) Critère statistique appliqué

L'approche de cette conservation ciblée des données basée sur ce critère statistique implique également que l'ensemble du territoire national peut être couvert. Si, après un recensement minutieux de chaque arrondissement judiciaire et de chaque zone de police, il apparaît que la criminalité grave est suffisamment élevée dans chacun de ces endroits, il y aura une conservation ciblée des données, mais les conséquences seront générales. En d'autres termes, il est possible d'avoir une conservation des données différenciée mais générale.

(iii) Quid de la jurisprudence européenne?

Cette approche est, selon le vice-premier ministre, entièrement conforme à l'exigence de la CJUE qui, dans son arrêt *La Quadrature du Net*, indique elle-même que la conservation fondée sur un critère géographique objectif est l'une des options possibles et demande aux États membres de tenir compte de la proportionnalité de la mesure par rapport à l'objectif poursuivi. Plus précisément, la Cour indique que la conservation doit être nécessaire et aussi limitée que possible dans le temps.

En outre, le gouvernement met en œuvre ce critère géographique de manière dynamique et transparente: les statistiques sont établies et validées chaque année par l'Organe de contrôle de l'information policière, et seront publiées au *Moniteur belge* par arrêté ministériel.

Il est donc possible de couvrir l'ensemble du territoire. Certains prétendront sans doute que la réglementation est incompatible avec la jurisprudence, ne fût-ce que sur ce point. Le gouvernement n'est pas d'accord avec ce raisonnement, qu'il considère comme malhonnête.

D'aucuns considèrent en effet que l'utilisation du critère géographique évoqué par la CJUE exigerait automatiquement et implicitement que seule une partie du territoire soit couverte. Mais quelle étendue est alors acceptable? Il n'existe pas de nombre d'or pour la

per 1 000 inwoners overeenkomt met een zeer hoog aantal zware feiten. Dat hoge aantal wijst ook op een verankering van zware criminaliteit in het arrondissement. Die drempel heeft uiteraard ook gevolgen voor de veiligheid van de bevolking, en inzake bepaalde misdrijven voor de rechtmatige verwachtingen van de slachtoffers; niet alleen verwachten zij bijstand en redding, maar ook dat de daders van het misdrijf jegens hen worden opgespoord en vervolgd.

De adviezen van *Child Focus* en van het Instituut voor de gelijkheid van vrouwen en mannen sluiten daar naadloos bij aan.

(ii) Statistisch criterium ingevuld

De aanpak van deze doelgerichte bewaring van gegevens op basis van dit statistische criterium impliceert ook dat het gehele nationale grondgebied kan worden bestreken. Indien na een zorgvuldige telling in elk gerechtelijk arrondissement en elke politiezone blijkt dat de zware criminaliteit op elk van deze plaatsen voldoende hoog is, zullen de gegevens gericht worden bewaard, maar zullen de gevolgen ervan algemeen zijn. Zulks houdt in dat een gedifferentieerde maar algemene dataretentie tot de mogelijkheden behoort.

(iii) Quid met de Europese rechtspraak?

Deze aanpak is volgens de vice-eersteminister volledig ingebed in de eis van het HvJ-EU, dat in zijn arrest-*Quadrature du Net* zelf aangeeft dat bewaring op basis van een objectief geografisch criterium één van de opties is, en dat aan de lidstaten vraagt rekening te houden met de proportionaliteit van de maatregel naargelang van het nagestreefde doel. Meer bepaald bedoelt het Hof dat de bewaring noodzakelijk moet zijn en zo beperkt mogelijk in de tijd.

Bovendien vult de regering dit geografische criterium dynamisch en transparant in: de statistieken worden elk jaar opgesteld en gevalideerd door het Controleorgaan op de politionele informatie, en zullen bij ministerieel besluit worden gepubliceerd in het *Belgisch Staatsblad*.

Het is dus mogelijk heel het grondgebied te dekken. Sommigen zullen wellicht beweren dat de regeling op dit punt alleen al niet strookt met de rechtspraak. De regering is het niet eens met die redenering, die zij oneerlijk acht.

Sommigen menen inderdaad dat het gebruik van het geografische criterium waarover het HvJ-EU Hof spreekt, automatisch en impliciet zou vereisen dat slechts een deel van het grondgebied wordt bestreken. Maar hoeveel is dan aanvaardbaar? Er is geen gulden snede voor de

conservation des données qui indiquerait la proportionnalité absolue et maximale de la population couverte. Se satisfait-on de 91, 61 ou 41 % de la population? Ou seulement de 11 %, voire de 1 %?

Le gouvernement est fermement convaincu que si le caractère général et indifférencié de la conservation des données est rejeté dans les arrêts de la CJUE, c'est précisément parce qu'une telle conservation générale et indifférenciée ne répond pas "à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi". L'interprétation donnée par le gouvernement ne peut absolument pas être lue de cette manière. Des critères objectifs sont instaurés.

(iv) Principes d'atteinte à la vie privée: nécessité et caractère limité dans le temps

L'approche du gouvernement tient donc compte au maximum de la vie privée des citoyens, en ce sens que la conservation des données dans une zone géographique n'est organisée que lorsqu'elle est strictement nécessaire vu le haut taux de criminalité au sein de celle-ci. Ce haut taux de criminalité est objectivé selon des critères transparents et déterminés dans la loi.

En outre, ces données ne sont conservées que le temps nécessaire, lequel est mesuré à l'aulne de l'intensité de la menace pour la sécurité publique au sein de chaque arrondissement ou zone de police. Selon le vice-premier ministre, des critères statistiques objectifs et mesurables, dont l'exactitude sera en outre obligatoirement validée par un Organe indépendant, seront utilisés.

Modalités de conservation complémentaires

Outre le critère géographique, plusieurs autres critères permettent la conservation, sur la base des arrêts de la CJUE.

(i) Le quick freeze et le future freeze

Dans des dossiers spécifiques, les services pourront remettre une réquisition de conservation à un ou plusieurs opérateurs pour les données qui existent déjà à ce moment-là (*quick freeze*) ou une réquisition de conservation pour les données qui seront générées au cours d'une période à partir du moment où l'ordonnance est délivrée (*future freeze*).

Cette mesure peut être ordonnée vis-à-vis d'une personne ou d'un groupe de personnes, d'un lieu ou d'un moyen de communication. Il peut également s'agir de données que les opérateurs conservent à leurs propres fins.

bewaring van gegevens die de absolute en maximale evenredigheid van de bestreken bevolking zou aangeven. Zijn ze tevreden met 91, 61 of 41 % van de bevolking? Of slechts 11 %, of zelfs maar 1 %?

Het is de vaste overtuiging van de regering dat het algemene en ongedifferentieerde karakter van gegevensbewaring in de arresten van het HvJ-EU wordt verworpen, net omdat zo'n algemene en ongedifferentieerde bewaring niet "voldoet aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel". De invulling die de regering geeft, valt helemaal niet op die manier te lezen. Er worden objectieve criteria ingevoerd.

(iv) Beginselen van aantasting van de persoonlijke levenssfeer: noodzaak en beperkt in de tijd

De aanpak van de regering houdt dus zoveel mogelijk rekening met de persoonlijke levenssfeer van de burgers, in die zin dat de gegevens in een geografisch gebied alleen worden bewaard wanneer zulks, gezien de hoge criminaliteitscijfers in dat gebied, strikt noodzakelijk is. Die hoge criminaliteitscijfers worden geobjectiveerd op grond van transparante en wettelijk bepaalde criteria.

Voorts worden die gegevens alleen bewaard zolang dat nodig is, op grond van de intensiteit van de bedreiging voor de openbare veiligheid in elk gerechtelijk arrondissement of politiezone. De vice-eersteminister wijst erop dat objectieve en meetbare statistische criteria zullen worden gebruikt, waarvan de juistheid bovendien zal moeten worden gevalideerd door een onafhankelijk orgaan.

Aanvullende nadere regels voor bewaring

Bovenop het geografisch criterium komen nog een aantal criteria die retentie mogelijk maken, op basis van de arresten van het HvJ-EU.

(i) De quick freeze en de future freeze

In specifieke dossiers zullen de diensten aan één of meer operatoren een bewaarbevel kunnen geven, voor gegevens die op dat moment al bestaan (*quick freeze*) of een bewaarbevel voor de gegevens die gedurende een periode vanaf het moment van het bevelschrift gegenereerd zullen worden (*future freeze*).

Deze maatregel kan worden gelast met betrekking tot een persoon of een groep van personen, een plaats of een communicatiemiddel. Het kan ook gaan om gegevens die de operatoren voor eigen doeleinden bewaren.

Il va sans dire que cette mesure ne sera toutefois utile que dans un nombre limité de cas dans lesquels le magistrat pourra, sur la base d'autres preuves, détecter et suivre des suspects et dans lesquels il souhaitera en savoir davantage au sujet de leurs mouvements et de leurs contacts.

Cependant, les mesures de *quick freeze* et de *future freeze* ne permettent pas de lutter contre la criminalité grave et les menaces réelles et actuelles en matière de sécurité. Le vice-premier ministre illustre son propos: ordonner une mesure de *quick freeze* au moment de la détection des faits ou lors d'une enquête, par exemple en cas de plainte pour enlèvement ou lors de la découverte d'un cadavre ou encore lors d'une explosion à la suite d'un attentat est dans l'immense majorité des cas une mesure sans effet car trop tardive et ne permettra donc pas de participer à l'élucidation des faits et à la recherche de la vérité judiciaire. Ce sont notamment les contacts, antérieurs à la constatation du fait, d'une personne avec d'autres ou les données de localisation au moment des faits (et pas de leur constatation), qui permettent de démarrer une enquête.

(ii) Conservation autour de lieux stratégiques

La CJUE indique qu'il est également possible d'organiser à titre préventif une conservation des données autour de lieux spécifiques, notamment ceux qui, de par leur nature, sont particulièrement exposés à la criminalité grave ou vulnérables à des menaces pour la sécurité nationale ou qui constituent des lieux stratégiques. Le gouvernement a, en collaboration avec les services compétents, énuméré ces lieux dans le projet de loi:

— les bâtiments portuaires;

— les bâtiments des gares;

— les tribunaux;

— les centrales nucléaires;

— les ambassades;

— les bâtiments des aéroports.

La nécessité d'organiser une *data retention* pour chacun de ces lieux a été dûment motivée dans l'exposé des motifs.

Le vice-premier ministre précise que dès que ces lieux sont affectés à d'autres destinations que celles qui sont énumérées dans la loi, il n'y a plus lieu d'avoir une conservation des données. Ce principe figure aussi dans le projet de loi.

Deze maatregel zal echter allicht slechts nuttig zijn in een beperkt aantal gevallen waarin de magistraat, op basis van ander bewijs, verdachten kan opsporen en volgen en meer te weten wil komen over hun bewegingen en contacten.

Met maatregelen als *quick freeze* en *future freeze* kunnen zware criminaliteit en reële en actuele veiligheidsdreigingen echter niet worden tegengegaan. De vice-eersteminister illustreert zijn stelling als volgt: wanneer bij de vaststelling van feiten of bij een onderzoek, bijvoorbeeld wanneer een klacht wordt ingediend wegens ontvoering, een lijk wordt ontdekt of een bomaanslag wordt gepleegd, een *quick freeze* wordt bevolen, heeft zulks in de meeste gevallen geen effect. De maatregel komt immers te laat en kan dus niet bijdragen aan de opheldering van de feiten en de waarheidsvinding. Het zijn meer bepaald de contacten van een betrokkene met anderen – vóór dan wel na de vaststelling van de feiten – of de locatiegegevens op het ogenblik van de feiten (en niet de vaststelling ervan) die het mogelijk maken een onderzoek op te starten.

(ii) Bewaring in de omgeving van strategische plaatsen

Het HvJ-EU stipt aan dat het tevens mogelijk is een preventieve gegevensbewaring te organiseren in de omgeving van specifieke plaatsen, meer bepaald die plaatsen die door hun aard sterk zijn blootgesteld aan zware criminaliteit, die kwetsbaar zijn voor bedreigingen van de nationale veiligheid of die van strategisch belang zijn. De regering heeft die plaatsen in samenwerking met de bevoegde diensten in het wetsontwerp opgesomd:

— havenfaciliteiten;

— stationsgebouwen;

— rechtbanken;

— kerncentrales;

— ambassades;

— luchthavengebouwen.

De noodzaak om voor elk van die plaatsen aan dataretentie te doen, werd in de memorie van toelichting naar behoren verantwoord.

De vice-eersteminister stipt aan dat zodra die plaatsen een andere bestemming krijgen dan die welke in het wetsontwerp zijn opgesomd, de gegevensbewaring niet langer vereist is. Dat beginsel is ook in het wetsontwerp opgenomen.

(iii) Conservation généralisée et indifférenciée

Si le niveau de la menace de l'OCAM est établi à 3 ou 4 sur l'ensemble du territoire, ou si, en cas de menace grave pour la sécurité de l'État, les services de renseignement demandent à cet effet une méthode exceptionnelle de renseignement à la Commission BIM, une conservation généralisée et indifférenciée peut être mise en œuvre temporairement.

C'est également conforme à la jurisprudence.

Le vice-premier ministre rappelle à cet égard que l'OCAM établit actuellement le niveau général de la menace à 2, et à 3 à quelques endroits spécifiques, et ce, depuis la fin janvier 2018.

(iv) Rétention sur la base des catégories de personnes

La Cour de Justice de l'Union européenne offre également la possibilité d'organiser une conservation préventive sur la base de critères concernant des catégories de personnes, mais le gouvernement n'a explicitement pas retenu cette option afin d'éviter que certaines catégories de groupes cibles soient discriminées. Le risque est en effet de se retrouver dans des situations de profilage et de stigmatisation, ce qu'il faut bien évidemment éviter.

La conservation de données par les opérateurs à leurs propres fins

Le vice-premier ministre souligne que les données de trafic et de localisation sont de toute façon déjà aussi conservées par les opérateurs à leurs propres fins. Les opérateurs conservent les mêmes données à des fins de facturation, dans le cadre de la lutte contre la fraude et pour la sécurité de leurs propres réseaux.

Ces données peuvent également être réquisitionnées par la justice et les services de renseignement. La différence est que la durée de conservation varie selon l'opérateur, en fonction de la manière dont ils se sont organisés. Le projet de loi à l'examen prévoit également des modifications sur ce point.

Communication des données conservées

Le vice-premier ministre explique avoir maintenu les règles strictes sur la communication de données aux services judiciaires et de renseignement. En Belgique, les services de police n'ont aucune autonomie en la matière. Ce n'est que sur la base d'une autorisation écrite du procureur, justifiant la nécessité et la proportionnalité de cette communication, que les données d'identification sont communiquées à la police. Et ce n'est que sur la base d'un mandat d'un juge d'instruction que les

(iii) Algemene en ongedifferentieerde retentie

Wanneer het dreigingsniveau van het OCAD voor heel het grondgebied op 3 of 4 wordt ingeschaald, of wanneer de inlichtingendiensten bij een ernstige dreiging tegen de nationale veiligheid daartoe een uitzonderlijke inlichtingenmethode zouden aanvragen bij de BIM-commissie, kan tijdelijk een algemene en ongedifferentieerde retentie afgekondigd worden.

Ook dit is conform de rechtspraak.

In dat verband herinnert de vice-eersteminister eraan dat het algemene dreigingsniveau van het OCAD momenteel, en dat sinds eind januari 2018, ingeschaald is in niveau 2, met enkele specifieke plaatsen in niveau 3.

(iv) Retentie op basis van categorieën van personen

Het HvJ-EU heeft ook de optie gelaten een preventieve bewaring te organiseren op basis van criteria over categorieën van personen, maar daar heeft de regering expliciet niet voor gekozen om te voorkomen dat bepaalde categorieën van doelgroepen gediscrimineerd zouden worden. Dan dreigt men immers terecht te komen in situaties van profiling en stigmatisering, hetgeen uiteraard niet wenselijk is.

De bewaring van gegevens door de operatoren voor eigen doeleinden

De vice-eersteminister onderstreept dat de verkeers- en locatiegegevens sowieso ook al door de operatoren bewaard worden voor eigen doeleinden. De operatoren bewaren dezelfde gegevens voor facturatiedoeleinden, in het kader van de strijd tegen de fraude, alsook voor de beveiliging van hun eigen netwerken.

Deze gegevens kunnen ook gevorderd worden door het gerecht en de inlichtingendiensten. Het verschil is dat de bewaartijd varieert per operator, naargelang van hun eigen organisatie. Ook op dit punt voorziet dit wetsontwerp in wijzigingen.

Mededeling van de bewaarde gegevens

De vice-eersteminister legt uit dat de strenge regels betreffende de mededeling van gegevens aan de gerechtelijke en inlichtingendiensten werden behouden. In België hebben de politiediensten geen enkele autonomie ter zake. Pas na schriftelijke toestemming van de procureur, waarin de noodzaak en de proportionaliteit van die mededeling worden verantwoord, mogen de identificatiegegevens aan de politie worden meegedeeld. De locatie- en verkeersgegevens van de operatoren

données de localisation et de trafic des opérateurs sont communiquées à la police. La Belgique a également intégré un principe de proportionnalité, il y a déjà des années, en liant la gravité de l'infraction à la portée de l'enquête. Seuls les crimes les plus graves, comme le terrorisme, peuvent être retracés sur 12 mois. D'autres crimes, en fonction de leur gravité, peuvent être accessibles pendant neuf mois ou six mois. Les services de renseignement connaissent également ce principe, qui sera maintenu.

Vu que non seulement la vie privée est en jeu, mais aussi la protection des données qui sont conservées, le vice-premier ministre confirme que les règles de sécurité à l'égard des opérateurs de télécommunications ont été renforcées:

— l'opérateur doit disposer d'une équipe permanente qui traite les demandes des autorités judiciaires ou des services de renseignement;

— les membres de cette cellule sont soumis à un screening de sécurité;

— ces membres sont soumis au secret professionnel;

— enfin, les opérateurs doivent tenir un registre qui permet de vérifier quelles données ont été transmises à quel service et pourquoi.

Que fait l'Europe?

Au niveau européen, des débats ont été menés au sujet de la conservation des données à la suite des différents arrêts de la Cour de Justice de l'Union européenne. Lors de la réunion du Conseil Justice et Affaires intérieures en mars 2021, la présidence portugaise a lancé un débat concernant la disposition des différents États membres à élaborer une législation européenne. Il est apparu que la majorité des États membres sont favorables à une telle solution européenne. Un débat plus approfondi est toutefois nécessaire afin de définir les différents éléments de base, conformément à la jurisprudence de la Cour de Justice de l'Union européenne et aux droits fondamentaux européens.

Le gouvernement plaide pour une solution européenne pérenne qui permettrait d'avoir en matière de *data retention* les mêmes règles au niveau de l'ensemble des pays européens. Cependant, vu l'annulation partielle de la loi du 29 mai 2016, il n'était pas possible de laisser un vide juridique, qui créerait une grande insécurité.

worden alleen op basis van een mandaat van een onderzoeksrechter aan de politie meegedeeld. België heeft jaren geleden ook een evenredigheidsbeginsel in de regeling opgenomen, door de ernst van het strafbare feit te koppelen aan de reikwijdte van het onderzoek. Enkel bij de zwaarste misdaden, zoals terrorisme, kunnen de gegevens worden getraceerd over een periode van twaalf maanden). Gegevens over andere misdaden kunnen, naargelang van de ernst, gedurende negen of zes maanden toegankelijk blijven. Ook de inlichtingendiensten zijn vertrouwd met dat beginsel, dat behouden zal blijven.

Aangezien niet alleen de persoonlijke levenssfeer op het spel staat, maar ook de bescherming van de bewaarde gegevens, bevestigt de vice-eersteminister dat de veiligheidsregels voor de telecommunicatieoperatoren werden aangescherpt:

— de operator moet beschikken over een vast team dat de verzoeken van de gerechtelijke autoriteiten of de inlichtingendiensten behandelt;

— de medewerkers van die cel ondergaan een veiligheidsscreening;

— die medewerkers moeten zich houden aan het beroepsgeheim;

— de operatoren moeten ten slotte een register bijhouden waarmee kan worden nagegaan welke gegevens aan welke dienst werden bezorgd, en waarom.

Wat doet Europa?

Op Europees niveau zijn er naar aanleiding van de verschillende arresten van het HvJ-EU debatten gevoerd over de bewaring van gegevens. Tijdens de zitting van de Raad Justitie en Binnenlandse Zaken in maart 2021 heeft het Portugese voorzitterschap een debat op gang gebracht over de bereidheid van de verschillende lidstaten om een Europese wetgeving op uit te werken. Gebleken is dat de meeste lidstaten voorstander zijn van een dergelijke Europese oplossing. Er is echter een diepgaander debat nodig om de verschillende basiselementen vast te stellen, overeenkomstig de jurisprudentie van het HvJ-EU en de Europese grondrechten.

De regering pleit voor een duurzame Europese oplossing waarbij voor alle Europese landen dezelfde regels inzake gegevensbewaring zouden gelden. Gezien de gedeeltelijke nietigverklaring van de wet van 29 mei 2016 moest de aldus ontstane juridische leemte, die veel onzekerheid zou scheppen, echter worden weggewerkt.

Les avis concernant l'avant-projet

Après un passage en première lecture au Conseil des ministres, le gouvernement a demandé des avis au Conseil d'État, à l'Autorité de protection des données (APD), à l'Organe de contrôle de l'information policière (Ocip) et au Comité permanent R. Ces deux derniers organismes fonctionnent en tant qu'autorité de protection des données respectivement pour la police et les services de renseignement. Le gouvernement a également organisé une consultation publique afin de permettre aux opérateurs de fournir une contribution en tant que parties prenantes.

En outre, Child Focus et l'Institut pour l'égalité des femmes et des hommes ont également transmis un avis de leur propre initiative.

(i) L'Autorité de protection des données

Dans son avis, l'APD arguait d'abord que les pouvoirs publics pourraient prendre des mesures moins intrusives pour la vie privée, qui permettraient d'obtenir des résultats similaires voire meilleurs que la conservation de métadonnées et que ces solutions techniques sont en outre à la disposition des services de police et de renseignement, avec pour effet que les enquêtes devraient être plus rapides qu'auparavant.

Le gouvernement a soumis ce point de l'avis aux services de sécurité et aux autorités judiciaires, mais ceux-ci lui ont rétorqué que cela ne reflétait pas la réalité sur le terrain de la lutte contre le crime organisé ou le terrorisme. En effet, on y observe un éventail de moyens de communication, une criminalité polymorphe qui repose (entièrement ou partiellement) sur l'internet et une évolution dans la manière de collecter les preuves. Si les aveux et les témoignages étaient les moyens de collecte de preuves les plus courants il y a des dizaines d'années, ce n'est plus le cas aujourd'hui. Dans des enquêtes de cette nature, la collecte de preuves est régie par des moyens d'enquête techniques et méthodologiques.

Cette donnée est contrecarrée par une diminution de l'efficacité des interceptions de communications. Si près de 98 % des demandes d'interceptions de communication étaient mises en œuvre dans la demi-heure il y a quelques années (chiffres de 1996), ce chiffre a diminué drastiquement pour atteindre aujourd'hui des valeurs dépassant parfois à peine les 30 % (mesures de 2015). Le seul fait de disposer de plus de données est donc loin de faciliter la lutte contre la criminalité.

De adviezen inzake het voorontwerp

Na een passage op de Ministerraad in eerste lezing heeft de regering adviezen gevraagd aan de Raad van State, de Gegevensbeschermingsautoriteit (GBA), het Controleorgaan op de politionele informatie (COC) en het Vast Comité I. Deze laatste twee instellingen fungeren als gegevensbeschermingsautoriteit voor respectievelijk de politie en de inlichtingendiensten. De regering heeft ook een publieke consultatie georganiseerd om de operatoren als belanghebbenden de mogelijkheid te geven input aan te leveren.

Voorts hebben Child Focus en het Instituut voor de gelijkheid van vrouwen en mannen op eigen initiatief een advies bezorgd.

(i) De Gegevensbeschermingsautoriteit

In haar advies heeft de GBA eerst en vooral aangevoerd dat de overheid maatregelen moet nemen die minder intrusief zijn voor de privacy, die het mogelijk zouden maken een gelijkaardig of zelfs beter resultaat te boeken dan via de bewaring van metadata, en dat deze technische oplossingen bovendien ter beschikking staan van de politie- en inlichtingendiensten, waardoor de onderzoeken vlotter zouden moeten verlopen dan in het verleden.

De regering heeft dit punt van advies voorgelegd aan de veiligheidsdiensten en de gerechtelijke autoriteiten, maar kreeg daar te horen dat dit niet overeenstemt met de realiteit inzake de bestrijding van georganiseerde criminaliteit of terrorisme: er is een waaier aan communicatiemiddelen, van criminaliteit die (geheel of gedeeltelijk) via het internet wordt gepleegd en een zekere evolutie in de wijze waarop bewijsmateriaal wordt verzameld. Waar tientallen jaren geleden bekentenissen en getuigenissen de meest gebruikte manieren waren om bewijsmateriaal te verzamelen, is dit thans niet langer het geval. In dergelijke onderzoeken wordt het verzamelen van bewijsmateriaal aangestuurd door technische en methodologische onderzoeksmiddelen.

Dit gegeven wordt doorkruist door een afnemende doeltreffendheid van communicatie-interceptie. Terwijl enkele jaren geleden bijna 98 % van de verzoeken om interceptie van communicatie binnen een half uur operationeel werd uitgevoerd (cijfers van 1996), is dit cijfer drastisch gedaald tot waarden die soms nauwelijks boven de 30 % uitkomen (metingen van 2015). Men is dus ver verwijderd van een eenvoudiger bestrijding van de criminaliteit, enkel doordat er meer data beschikbaar zouden zijn.

En outre, l'APD entend en réalité par "méthodes alternatives moins intrusives" des moyens techniques tels que le logiciel Pegasus, qui seraient moins intrusifs au motif qu'ils ne visent qu'un seul individu. Sans réfuter ce point, le vice-premier ministre souligne toutefois que Pegasus est un type d'instrument permettant d'infecter l'appareil d'un individu à distance. Son action va donc bien au-delà de la seule interception de données de localisation, sans le contenu, d'une personne.

Selon le vice-premier ministre, il n'y a pas d'alternative à la *data retention* qui serait moins intrusive au niveau de la vie privée.

Ensuite, l'APD recommande au gouvernement d'établir ses statistiques à partir non pas du nombre d'infractions mais du nombre de condamnations. Le gouvernement ne suit cependant pas cet avis parce que, comme l'a déjà souligné la Cour de justice de l'Union européenne, il convient de tenir compte du risque accru de faits criminels. En effet, ce n'est pas parce qu'il n'y a pas de condamnation qu'aucune infraction n'a été commise.

La procédure de comptabilisation des infractions sera toutefois soumise pour contrôle au COC.

En ce qui concerne l'éventuelle couverture de l'ensemble du territoire, le vice-premier ministre a déjà indiqué que ce raisonnement était bancal. En effet, on ne peut pas se borner à regarder le résultat pour déterminer si les règles ont été suivies ou non. Si l'on appliquait ces principes à un pays comme la Suède ou l'Espagne, on obtiendrait un résultat tout à fait différent. Le fait est que la Belgique est un petit pays qui présente l'une des densités de population les plus fortes au monde.

Pour répondre à ces éléments de critique, le gouvernement a supprimé plusieurs catégories de lieux stratégiques. En outre, les lieux conservés ont tous été clairement définis dans l'exposé des motifs.

En ce qui concerne l'encryptage, le vice-premier ministre observe que cette question a été soulevée à plusieurs reprises dans la presse. Il affirme soutenir le chiffrement des communications, en ce compris *end-to end*, qui est un élément essentiel pour sécuriser les paiements et empêcher le *hacking* de communications privées. Le chiffrement est essentiel non seulement pour la protection de la vie privée, mais aussi pour garantir le potentiel économique du pays, pour maintenir la compétitivité des entreprises, pour respecter le secret médical et pour préserver les secrets de fabrication.

Bovendien bedoelt de GBA met "minder indringende alternatieve methoden" eigenlijk technische middelen als Pegasus, die minder intrusief zouden zijn omdat ze op slechts één individu gericht zijn. Zonder dat laatste punt te ontkennen, wijst de vice-eersteminister erop dat Pegasus het soort instrument is waarmee men vanop afstand iemands toestel kan besmetten; dit gaat als maatregel veel verder dan enkel de locatiegegevens van een persoon onderscheppen zonder de inhoud.

Volgens de vice-eersteminister is er geen alternatief voor de dataretentie dat minder intrusief zou zijn wat de persoonlijke levenssfeer betreft.

Voorts heeft de GBA de regering aangeraden voor de statistieken niet het aantal strafbare feiten te tellen, maar wel het aantal veroordelingen. De regering volgt dit advies niet omdat, zoals het HvJ-EU al stelde, er wordt gekeken naar het verhoogde risico op criminele feiten. Het is immers niet omdat er geen veroordeling is, dat er geen strafbaar feit werd gepleegd.

De procedure waarbij feiten worden geteld, wordt wel aan het COC ter controle voorgelegd.

Inzake de mogelijke dekking van het hele grondgebied gaf de vice-eersteminister al aan dat deze redenering niet sluitend is. Men kan niet enkel naar de uitkomst kijken om te beslissen of de regels gevolgd zijn. Pas de principes toe op een land als Zweden of Spanje, en men krijgt een heel ander resultaat. België is nu eenmaal een klein land, dat bij de dichtstbevolkte van de wereld hoort.

Als antwoord op deze elementen van kritiek heeft de regering verschillende categorieën van strategische plaatsen geschrapt. Degene die in aanmerking werden genomen, werden bovendien allemaal duidelijk beschreven in de memorie van toelichting.

De vice-eersteminister merkt op dat de versleuteling meermaals in de pers is aangekaart. Zij geeft aan voorstander te zijn van de versleuteling van informatie, met inbegrip van *end-to-end*encryptie, die essentieel is om betalingen te beveiligen en om hacking van privécommunicatie te voorkomen. Encryptie is niet alleen van essentieel belang voor de bescherming van de persoonlijke levenssfeer, maar ook om het economisch potentieel van het land te waarborgen, het concurrentievermogen van het bedrijfsleven te handhaven, het medisch beroepsgeheim in acht te nemen en de fabrieksgeheimen te vrijwaren.

L'article que propose le gouvernement sur l'encryptage réaffirme donc de manière claire et incontestable que l'encryptage est fortement encouragé. Son utilisation rencontre néanmoins trois limites fondamentales qui sont rappelées dans le présent projet:

— l'utilisation de l'encryptage ne peut pas empêcher les appels d'urgence;

— l'encryptage ne peut pas empêcher un opérateur de répondre à ses obligations en matière de *data rétention*;

— lorsque des cartes SIM étrangères sont actives sur notre réseau (appelées "*in-roamers*"), le cryptage de l'opérateur étranger ne doit pas rendre impossible la mise à disposition du contenu de la communication par l'opérateur belge. Dans les contrats d'itinérance avec les entreprises étrangères, les opérateurs belges doivent donc pouvoir faire appliquer cette disposition.

En ce qui concerne l'avis de l'APD sur l'accès au contenu de communications cryptées, le gouvernement a bien entendu le message. Le gouvernement est opposé à l'installation de portes dérobées non connues des opérateurs, qui permettraient d'exploiter les faiblesses des systèmes de communication. En d'autres termes, le gouvernement ne souhaite pas que l'interception et le décryptage de communications cryptées bien définies mette à mal le cryptage de l'ensemble du système.

Cela n'enlève toutefois rien au fait que les opérateurs, y compris les opérateurs étrangers qui fournissent des services de communication dans notre pays, sont en principe tenus de coopérer avec les services de police et les services judiciaires, conformément aux articles 90*ter* et 90*quater* du Code d'instruction criminelle.

(ii) Le COC et le Comité R

Les autorités de protection des données des services de police et de renseignement ont remis un avis sur la base duquel il est possible de travailler. Le COC soutient explicitement le fait que les auteurs du projet de loi à l'examen optent pour une exploration maximale des options que la Cour de justice de l'Union européenne fournit en matière de conservation des données.

Le COC a formulé plusieurs observations à propos de la comptabilisation de plusieurs faits dans la Banque de données nationale générale (BNB). Il y a été donné suite, notamment en instaurant des règles pour éviter les doublons. Le COC approuvera la procédure au préalable lors de la première utilisation des statistiques.

Het door de regering in uitzicht gestelde artikel over versleuteling beoogt dan ook nogmaals duidelijk en ontegensprekelijk te bevestigen dat versleuteling sterk wordt aangemoedigd. In dit wetsontwerp wordt evenwel eraan herinnerd dat bij het gebruik daarvan drie fundamentele beperkingen gelden:

— het gebruik van versleuteling mag noodoproepen niet in de weg staan;

— versleuteling mag een operator niet beletten zijn verplichtingen inzake dataretentie in acht te nemen;

— wanneer buitenlandse SIM-kaarten ("*in-roamers"*) op ons netwerk actief zijn, mag de encryptie van de buitenlandse operator niet beletten dat de Belgische operator de inhoud van zijn communicatie ter beschikking stelt. Bij de roamingovereenkomsten met de buitenlandse ondernemingen moeten de Belgische operatoren die bepaling dus kunnen doen toepassen.

Wat het advies van de GBA over de toegang tot de inhoud van geëncrypteerde communicatie betreft, heeft de regering de boodschap goed gehoord. De regering is tegen de installatie van *backdoors*, achterpoortjes in een systeem zonder medeweten van de operator, die de zwakke punten van een communicatiesysteem uitbuiten. Ze wil met andere woorden niet dat interceptie en decryptie van welbepaalde geëncrypteerde communicatie de encryptie van het ganse systeem op de helling zetten.

Maar dat neemt niet weg dat operatoren, ook buitenlandse operatoren die hier communicatie aanbieden, in principe gehouden zijn tot samenwerking met de politie- en gerechtelijke diensten, zoals bepaald in de artikelen 90*ter* en 90*quater* van het Wetboek van Strafvordering.

(ii) Het COC en het Comité I

De gegevensbeschermingsautoriteiten van de politie- en inlichtingendiensten hebben een zeer werkbaar advies uitgebracht. Het COC ondersteunt expliciet het feit dat de stellers van het wetsontwerp ervoor kiezen de opties voor dataretentie die het HvJ-EU aanreikt, maximaal te verkennen.

Het COC heeft enkele opmerkingen geformuleerd aangaande de telling van het aantal feiten in de Algemene Nationale Gegevensbank (ANG) van de politie. Aan deze opmerkingen werd gevolg gegeven. Zo werden er regels ingesteld teneinde dubbels te voorkomen. Het COC zal de procedure voorafgaandelijk goedkeuren bij de eerste aanwending van de statistieken.

Étant donné que les statistiques ne constituent pas des données à caractère personnel, le COC ne disposait pas en soi de compétences spécifiques à cet égard. Par conséquent, le présent projet de loi prévoit explicitement de doter le COC, aux fins de l'exercice de cette nouvelle tâche, de toutes les compétences initialement attribuées en matière de protection des données comme celles de rectification et d'injonction, de sorte que cet organe puisse vérifier que les statistiques produites annuellement sont adéquates, pertinentes et limitées à ce qui est nécessaire et le cas échéant, demander les rectifications nécessaires.

Sur la base de l'avis du Comité I, divers points ont été précisés dans la loi organique des services de renseignement.

(iii) Le Conseil d'État

En fait, le Conseil d'État n'a pas davantage formulé d'observations au sujet des principes de base de l'avant-projet. Le fil rouge de son avis était une demande de transparence et de cohérence dans la mise en œuvre des critères utilisés. Le gouvernement en a tenu rigoureusement compte et a conféré une base légale à l'ensemble des points. Un maximum d'informations seront publiées au *Moniteur belge* par la voie d'arrêtés royaux ou d'arrêtés ministériels.

Ainsi, chaque année, un arrêté ministériel signé par les ministres de la Justice et de l'Intérieur reprendra la liste des arrondissements judiciaires et des zones de police soumis à l'obligation de conservation, ainsi que leur durée de conservation.

Le gouvernement a également supprimé la rétroactivité à la demande du Conseil d'État.

Que fait la Justice en attendant la nouvelle loi?

Le ministère public invoque la législation Antigone, telle que fixée dans l'article 32 du TPCPP. Ce qui est important, c'est que la Cour de cassation a accepté ce point de vue dans un arrêt récent.

Concrètement, les métadonnées de communication conservées par les opérateurs et dès lors encore utilisées quotidiennement par la Justice et les juges sont acceptées comme preuves, pour autant que l'irrégularité commise n'ait pas nui à la fiabilité de la preuve ou que l'utilisation de la preuve ne soit pas contraire au droit à un procès équitable.

Aangezien de statistieken geen persoonsgegevens zijn, beschikte het COC op zich niet over specifieke bevoegdheden dienaangaande. Bijgevolg voorziet dit wetsontwerp, met het oog op de uitoefening van die nieuwe taak, uitdrukkelijk in de toekenning aan het COC van alle bevoegdheden die oorspronkelijk op het gebied van gegevensbescherming werden toegekend zoals die inzake rechtzetting en inzake bevel. Dat moet die instantie in staat stellen na te gaan of de jaarlijks opgemaakte statistieken passend, ter zake dienend en beperkt zijn tot wat noodzakelijk is, alsook, indien nodig, om de nodige rechtzettingen te kunnen verzoeken.

Op grond van het advies van Comité I zijn in de wet houdende regeling van de inlichtingen- en veiligheidsdiensten diverse punten verduidelijkt.

(iii) De Raad van State

Ook de Raad van State heeft eigenlijk geen opmerkingen over de basisprincipes van het voorontwerp geformuleerd. De rode draad doorheen zijn advies was een oproep tot transparantie en coherentie bij het uitwerken van de gehanteerde criteria. De regering heeft hier goed naar geluisterd en heeft alles een wettelijke basis gegeven. Een maximum aan informatie wordt gepubliceerd in het *Belgisch Staatsblad*, via koninklijke besluiten of ministeriële besluiten.

Zo zal een jaarlijks door de ministers van Justitie en van Binnenlandse Zaken ondertekend ministerieel besluit de lijst bevatten van de gerechtelijke arrondissementen en van de politiezones waarvoor de bewaarverplichting geldt, evenals de desbetreffende bewaartermijnen.

Op verzoek van de Raad van State heeft de regering ook de retroactiviteit laten vallen.

Wat doet justitie in afwachting van de nieuwe wet?

Het openbaar ministerie beroept zich op de zogenaamde Antigoon-wetgeving, zoals bepaald in artikel 32 van de Voorafgaande Titel van het Wetboek van Strafvordering. Belangrijk is dat het Hof van Cassatie die zienswijze in een recent arrest heeft aanvaard.

Concreet worden de metadata van communicatie bewaard door de operatoren dan ook nog dagelijks gebruikt door justitie en door de rechters aanvaard als bewijsstuk voor zover de begane onregelmatigheid de betrouwbaarheid van het bewijs niet heeft aangetast of het gebruik van het bewijs niet in strijd is met het recht op een eerlijk proces.

Conclusion

Le gouvernement a repris la nouvelle approche de la conservation des métadonnées qui est exigée par la Cour de Justice de l'Union européenne. Il s'est concerté pour ce faire avec des experts, tant des services de sécurité (police, justice, services de renseignement) que du monde universitaire. Le vice-premier ministre souhaite remercier ces experts pour leur expertise et leur implication, ainsi que sa collègue en charge des Télécommunications pour sa coopération étroite et intense.

Enfin, le vice-premier ministre rappelle avoir aussi intégré, parmi les autorités publiques pouvant demander des données de communications électroniques, un nouvel acteur, le Centre pour la Cybersécurité Belgium (CCB), qui joue un rôle important, en sa qualité de centre national de réponse aux incidents de sécurité informatique, au niveau de la détection, de l'observation et de l'analyse des problèmes de sécurité informatique. Le CCB a aussi besoin de ces métadonnées des communications pour jouer pleinement son rôle. L'actualité et le conflit entre le Russie et l'Ukraine rappellent que cet ajout était juste et fondé car la menace cyber est bien réelle et actuelle. Il est dès lors nécessaire de se doter des moyens pour y faire face.

Conclusie

De regering heeft de nieuwe aanpak van de bewaring van metadata, die door het HvJ-EU is geëist, overgenomen. Zij heeft hiervoor overlegd met deskundigen, zowel van de veiligheidsdiensten (politie, justitie, inlichtingendiensten) als van de academische wereld. De vice-eersteminister wil hen danken voor hun deskundigheid en hun inzet, alsook zijn collega bevoegd voor Telecommunicatie, voor de nauwe en intensieve samenwerking.

Tot slot herinnert de vice-eersteminister eraan dat zij aan de overheidsinstanties die elektronische-communicatiegegevens kunnen opvragen, een nieuwe actor heeft toegevoegd, namelijk het Centrum voor Cybersecurity België (CCB), dat in zijn hoedanigheid van nationaal *Computer Security Incident Response Team* (CSIRT) een belangrijke rol speelt bij de opsporing, observatie en analyse van informaticaveiligheidsproblemen. Het CCB heeft die communicatiemetagegevens ook nodig om zijn rol onverkort te kunnen vervullen. De actualiteit en het conflict tussen Rusland en Oekraïne herinneren eraan dat die toevoeging terecht en gegrond was, daar de cyberdreiging wel degelijk reëel en actueel is. Derhalve is het noodzakelijk zich met middelen toe te rusten om die dreiging aan te kunnen.

III. — **DISCUSSION GÉNÉRALE**

A. Réunion du 26 avril 2022

1. ***Questions et observations des membres***

Mme Sophie De Wit (N-VA) fait observer que la législation de réparation en matière de conservation des données, annoncée de longue date, s'est fait quelque peu attendre. L'intervenante espère que la nouvelle tentative détaillée résistera cette fois à l'examen de la Cour constitutionnelle.

Le cadre proposé dans le projet de loi est en effet crucial pour lutter contre la criminalité. Pour les personnes actives sur le terrain, apprendre que l'accès aux données n'allait plus de soi suite à l'annulation d'une législation antérieure a été une pilule amère à avaler.

L'intervenante comprend les arguments concernant la vie privée et la proportionnalité. Il est important de trouver un bon équilibre opérationnel.

Parmi tous les avis détaillés reçus, notamment celui du Conseil d'État, Mme De Wit estime que celui des

III. — **ALGEMENE BESPREKING**

A. **Vergadering van 26 april 2022**

1. ***Vragen en opmerkingen van de leden***

Mevrouw Sophie De Wit (N-VA) merkt op dat de lang aangekondigde herstelwetgeving inzake dataretentie enige tijd op zich heeft laten wachten. Het lid hoopt dat de gedetailleerde nieuwe poging deze keer de toets van het Grondwettelijk Hof zal doorstaan.

Het voorliggende kader is immers cruciaal voor de aanpak van de criminaliteit. Voor de betrokkenen in het veld was het een opdoffer dat de toegang tot gegevens niet meer evident bleek na de vernietiging van eerdere wetgeving.

De spreekster heeft begrip voor de argumenten inzake privacy en proportionaliteit. Het is belangrijk een goed werkend evenwicht te vinden.

Naast de uitgebreide adviezen van onder meer de Raad van State is het advies van de procureurs-generaal

procureurs généraux et des juges d'instruction, qui vont devoir appliquer cette législation, est également essentiel.

Les données seront conservées par les opérateurs sur une base géographique. Cela entraînera inévitablement une toute nouvelle approche pour les opérateurs en ce qui concerne la gestion des données de localisation et de trafic et leur échange avec les autorités.

Dans l'exposé des motifs, on peut lire que le législateur a pris connaissance des difficultés techniques et opérationnelles rencontrées par les opérateurs pour mettre en œuvre la conservation ciblée sur base géographique. De quelles difficultés s'agit-il exactement? A-t-on cherché à les aplanir? On a certes cherché un autre moyen de conserver les données et de contourner d'éventuels obstacles, mais la situation pourrait bien devenir problématique si cela s'avère impossible dans la pratique.

En matière de cybercriminalité et de sécurité en ligne, la législation existante, notamment la loi du 13 juin 2005 relative aux communications électroniques, est fortement remaniée. La tentative d'affaiblir le cryptage n'a finalement pas été retenue dans le projet de loi à l'examen, ce que le groupe N-VA considère comme une bonne chose. Le 17 décembre 2021, le Conseil des ministres a toutefois décidé d'examiner la possibilité de compléter la loi du 13 juin 2005 par une disposition concernant l'accès au contenu de communications cryptées. Pourquoi le gouvernement entend-il malgré tout examiner cette possibilité et où en est cet examen au stade actuel?

La législation est également modifiée en vue de lutter contre la fraude et l'utilisation malveillante du réseau. Le cadre juridique actuel est insuffisant pour réagir avec rapidité et efficacité. Le projet de loi à l'examen prévoit une obligation générale pour les opérateurs de prendre des mesures appropriées, proportionnées, préventives et curatives de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés. Le texte donne une énumération de mesures possibles, susceptibles d'être précisées par le Roi. En cas de défaillance de l'opérateur, l'Institut belge des services postaux et des télécommunications (IBPT) pourra imposer des instructions contraignantes. De quelles mesures appropriées, proportionnées, préventives et curatives s'agit-il concrètement? Suffira-t-il de continuer à travailler avec les exemples de mesures donnés dans le projet de loi? Quel est le critère pour déterminer si un opérateur est défaillant? Quelles sont exactement les instructions contraignantes qui pourront être imposées? Une plus grande clarté s'impose.

en de onderzoeksrechters, die met de wetgeving aan de slag moeten, eveneens cruciaal.

Gegevens zullen op geografische basis door operatoren bewaard worden. Dit leidt voor de operatoren onvermijdelijk tot een volledig nieuwe aanpak bij het beheer van locatie- en verkeersgegevens en de uitwisseling met de autoriteiten.

In de memorie van toelichting staat dat de wetgever kennis heeft genomen van de technische en operationele moeilijkheden die de operatoren hebben ondervonden om de gerichte bewaring op geografische basis te verrichten. Over welke moeilijkheden gaat het precies? Werden ze aangepakt? Er werd dan wel een andere manier gezocht om gegevens te bewaren en eventuele struikelblokken uit de weg te gaan, maar het wordt problematisch als dat in de praktijk onmogelijk blijkt.

Op het vlak van cybercriminaliteit en onlineveiligheid wordt er flink gesleuteld aan de bestaande wetgeving, waaronder de wet van 13 juni 2005 betreffende elektronische communicatie. De poging om encryptie af te zwakken werd uiteindelijk niet opgenomen in het voorliggende wetsontwerp, wat de N-VA-fractie een goede zaak vindt. Op 17 december 2021 besliste de Ministerraad echter alsnog na te gaan of de wet van 13 juni 2005 aangevuld kan worden met een bepaling over de toegang tot de inhoud van geëncrypteerde communicatie. Waarom wil de regering dit alsnog onderzoeken en wat is de huidige stand van het onderzoek?

De wetgeving wordt daarenboven aangepast om fraude en kwaadwillig gebruik van het netwerk aan te pakken. Het huidige juridisch kader is ontoereikend om snel en doeltreffend te reageren. Het voorliggende wetsontwerp voorziet in een algemene verplichting voor de operatoren om gepaste, evenredige, preventieve en curatieve maatregelen te nemen om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen, alsook te voorkomen dat de eindgebruikers nadeel ondervinden of lastiggevallen worden. Er worden mogelijke maatregelen opgesomd die door de Koning gepreciseerd kunnen worden. Als de operator zou tekortschieten, zou het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) alsnog dwingende instructies kunnen opleggen. Over welke gepaste, evenredige, preventieve en curatieve maatregelen gaat dit concreet? Zal het volstaan om met de voorbeeldmaatregelen verder te werken? Wat is het criterium om te bepalen of een operator tekortschiet? Welke dwingende instructies kunnen precies opgelegd worden? Meer duidelijkheid is geboden.

L'exposé des motifs indique par ailleurs que la Cour de justice de l'Union européenne (CJUE) ne s'est pas encore prononcée sur l'obligation pour les opérateurs de conserver certaines données relatives au trafic ou à la localisation dans le cadre de la lutte contre la fraude ou de la sécurité du réseau. L'autorité de protection des données (APD) s'interroge tant sur la proportionnalité que sur la nécessité de cette conservation des données. Exiger des opérateurs qu'ils stockent systématiquement les données de localisation et de trafic de tous les utilisateurs de communications électroniques constitue une ingérence dans les droits et le respect de la vie privée des personnes concernées. Le gouvernement souligne que la CJUE ne s'est pas encore prononcée à cet égard. Il est néanmoins important que les mesures proposées résistent au futur test auquel elles seront soumises. Le gouvernement peut-il rassurer les membres de la commission à cet égard? Il serait en effet insensé de devoir à nouveau élaborer une nouvelle législation en la matière dans un avenir proche.

Dans son avis, l'APD avait clairement fait part de certaines inquiétudes. En réponse à cet avis, le projet de loi à l'examen contient la disposition selon laquelle les données de communication de la personne dont émane la communication doivent être obligatoirement conservées, mais pas celles du destinataire (la victime de l'utilisation malveillante ou de la fraude). Toutefois, les données de localisation du destinataire seront bel et bien conservées si cela s'avère utile pour la détection ou l'analyse de la fraude ou de l'utilisation malveillante du réseau. L'intervenante se demande sur quelle base on appréciera si c'est "utile"? En effet, comme la conservation de ces données n'est pas obligatoire, ce qui n'est pas conservé sera perdu à jamais. Alors, soit on conserve tout et on consulte les données quand c'est utile, soit on fixe à l'avance un critère d'utilité.

En outre, la possibilité est donnée aux opérateurs de conserver également d'autres données qui pourraient leur être utiles dans le cadre de la lutte contre la fraude et l'utilisation malveillante du réseau. Pourquoi cette possibilité leur est-elle offerte? De quelles données s'agit-il? Sur quelle base un opérateur pourra-t-il décider qu'il est intéressant de conserver certaines données? Un fil conducteur clair est indispensable.

Le projet de loi à l'examen précise qu'il appartiendra aux autorités compétentes, et non à l'opérateur, d'établir la réalité d'une utilisation malveillante du réseau. En cas de suspicion de fraude ou d'utilisation malveillante du réseau, les opérateurs pourront transmettre l'ensemble des données conservées légalement à ce sujet. Le Roi précisera et étendra les données de trafic dont la conservation doit être considérée comme nécessaire. L'exposé des motifs indique que "la pratique devra donc

In de memorie van toelichting staat eveneens dat het Hof van Justitie van de Europese Unie (HvJ-EU) zich nog niet heeft uitgesproken over de verplichting voor operatoren om bepaalde verkeers- of locatiegegevens te bewaren in het kader van de bestrijding van fraude of in het kader van netwerkveiligheid. De Gegevensbeschermingsautoriteit (GBA) plaatst vraagtekens bij zowel de evenredigheid als de noodzakelijkheid. Als operatoren ertoe verplicht worden systematisch de locatie- en verkeersgegevens van alle elektronische communicatiegebruikers te bewaren, vormt dat een inmenging in de rechten en de eerbiediging van de persoonlijke levenssfeer. De regering benadrukt dat het HvJ-EU voorlopig nog geen uitspraak heeft gedaan. Het is echter belangrijk dat de voorliggende maatregelen in de toekomst de toets zullen doorstaan. Kan de regering de commissieleden geruststellen over het bewandelen van deze piste? Het kan niet de bedoeling zijn over afzienbare tijd opnieuw gewijzigde wetgeving te moeten uitwerken.

Uit het advies van de GBA bleek voorts de nodige bezorgdheid. In navolging van het advies bevat het voorliggende wetsontwerp de bepaling dat de communicatiegegevens van de persoon van wie de communicatie uitgaat verplicht bewaard moeten worden, maar niet van de geadresseerde (het slachtoffer van het kwaadwillig gebruik of van de fraude). De locatie van de geadresseerde zou echter wel bewaard worden indien dat nuttig blijkt om fraude en kwaadwillig gebruik van het netwerk op te sporen of te analyseren. Hoe wordt echter beoordeeld wanneer dit "nuttig" is? De bewaring is immers geen verplichting, en wat niet bewaard wordt, is voorgoed weg. Ofwel wordt alles bewaard en geraadpleegd wanneer het nuttig is, ofwel wordt op voorhand een criterium vastgesteld.

Bovendien wordt aan de operatoren de mogelijkheid geboden om ook andere gegevens te bewaren die wat hen betreft nodig zouden kunnen zijn in de strijd tegen fraude en kwaadwillig gebruik van het netwerk. Waarom wordt deze mogelijkheid open gelaten? Over welke gegevens gaat het? Op welke basis zal een operator kunnen beslissen wat interessant is om bij te houden? Een duidelijke leidraad is cruciaal.

Het voorliggende wetsontwerp geeft aan dat het aan de bevoegde autoriteiten is om kwaadwillig gebruik van het netwerk aan te tonen, en niet aan de operator. Als er een vermoeden van fraude of kwaadwillig gebruik bestaat, kunnen de operatoren alle wettelijk bewaarde gegevens in dat verband doorsturen. De Koning zal de verkeersgegevens waarvan de bewaring noodzakelijk wordt geacht verder preciseren en uitbreiden. "De praktijk zal dus moeten worden geëvalueerd om vast te stellen of

être évaluée pour déterminer si un tel arrêté royal est nécessaire". Mme De Wit se félicite que le gouvernement prévoie une évaluation de la nouvelle législation. Comment les ministres envisagent-ils cette évaluation? Dans quel délai sera-t-elle réalisée? En effet, l'opportunité pour le Roi de préciser certains éléments dépend de cette évaluation. Dans l'intervalle, l'opérateur devra continuer à évaluer s'il existe une suspicion et s'il convient de transmettre certaines données. Sur quels critères ces possibilités de décision étendues se fondent-elles?

Pour conclure, l'intervenante revient sur les modifications apportées à la loi du 5 août 1992 sur la fonction de police. De nouvelles dispositions habilitent la cellule des personnes disparues de la police fédérale à requérir des données relatives aux communications électroniques des personnes disparues. Les conditions matérielles et procédurales de l'accès à ces données sont établies dans la loi sur la fonction de police et un organe est chargé de contrôler ces demandes. Les nouvelles dispositions à l'examen reproduisent en grande partie les compétences actuelles de la cellule des personnes disparues – déjà prévues par la loi du 13 juin 2005 relative aux communications électroniques et remplacées par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques – bien qu'elles aient été annulées par la Cour constitutionnelle. Le gouvernement ne prend-il pas un risque? Est-ce suffisant pour résister à l'examen de la Cour constitutionnelle?

Mme De Wit conclut en faisant observer qu'une grande liberté d'action est conférée aux opérateurs. Il est essentiel de savoir au préalable sur la base de quels critères cette décision a été prise.

M. Albert Vicaire (Ecolo-Groen) souligne le travail effectué par les deux cabinets ministériels pour préparer et rédiger le projet de loi. Il estime qu'il s'agit d'un texte à la fois important et complexe, qui essaie de trouver un équilibre entre les besoins économiques et de sécurité d'une part et ceux de protection de la vie privée d'autre part. À ses yeux, le texte atteint son objectif. L'option de protéger l'acteur le plus faible lui semble importante. Les notions d'utilité publique, comme le transfert des données vers les autorités publiques en cas de besoin, sont bien cadrées.

M. Vicaire attendra l'ensemble des avis pour compléter son analyse.

M. Patrick Prévot (PS) souligne qu'il s'agit d'un dossier qui mêle des concepts technologiques avancés à des principes de protection de la vie privée, encadré par une jurisprudence étayée. Il rappelle qu'il appartient

een dergelijk koninklijk besluit noodzakelijk is", aldus de memorie van toelichting. Mevrouw De Wit is verheugd dat de regering in een evaluatie van de nieuwe wetgeving voorziet. Hoe zien de ministers deze evaluatie? Binnen welke termijn zal ze plaatsvinden? Daarvan hangt immers af of de Koning bepaalde zaken verder kan preciseren. In afwachting moet de operator nog steeds oordelen of er een vermoeden bestaat en of er gegevens doorgestuurd worden. Op basis van welke criteria verlopen deze verregaande beslissingsmogelijkheden?

Tot slot gaat de spreekster in op de aanpassingen van de wet van 5 augustus 1992 op het politieambt. Nieuwe bepalingen verlenen aan de Cel Vermiste Personen van de federale politie de bevoegdheid om gegevens met betrekking tot de elektronische communicatie van vermiste personen op te vorderen. Materiële en procedurele voorwaarden voor de toegang tot die gegevens worden vastgelegd in de wet op het politieambt, en een controleorgaan houdt toezicht op de vorderingen. De voorliggende nieuwe bepalingen nemen bestaande bevoegdheden van de Cel Vermiste Personen – reeds bepaald bij de wet van 13 juni 2005 betreffende de elektronische communicatie en vervangen bij de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie – grotendeels over, hoewel ze vernietigd werden door het Grondwettelijk Hof. Neemt de regering geen risico? Is dit voldoende om de toets van het Grondwettelijk Hof te doorstaan?

Mevrouw De Wit besluit dat operatoren heel wat handelingsvrijheid krijgen. Het is cruciaal om op voorhand te weten op basis van welke criteria dat gebeurt.

De heer Albert Vicaire (Ecolo-Groen) wijst op het werk dat de twee ministeriële kabinetten hebben verricht om het wetsontwerp voor te bereiden en op te stellen. Hij geeft aan dat het wetsontwerp zowel belangrijk als complex is, en dat het poogt een evenwicht te vinden tussen economische en veiligheidsbelangen enerzijds en de bescherming van het privéleven anderzijds. Volgens hem bereikt de tekst zijn doel. De keuze om de zwakste partij te beschermen lijkt hem belangrijk. De gevallen van openbaar nut, zoals de overdracht van gegevens naar de overheidsinstanties indien dat nodig is, zijn duidelijk omschreven.

Voor een volledige analyse wacht de heer Vicaire tot alle adviezen zijn binnengelopen.

De heer Patrick Prévot (PS) beklemtoont dat het een door een onderbouwde rechtspraak geschraagd dossier betreft waarin geavanceerde technologische concepten worden gepaard aan de principes van de bescherming

au législateur de ne pas noyer le débat derrière cette apparente technicité. Les enjeux de ce projet de loi pour la démocratie sont fondamentaux: comment assurer le droit à la sécurité de tout un chacun sans tomber dans de la surveillance généralisée de la population. La liberté individuelle protège le droit d'être et d'agir selon ses propres envies et ses choix. Le droit à la protection de la vie privée crée cet espace où chacun agit librement parce qu'il sait qu'il ne doit rendre de comptes à personne. C'est souvent de là que le progrès arrive: il y a un intérêt individuel et collectif à protéger la vie privée des concitoyens.

L'intervenant estime que la lutte contre la criminalité doit être aussi une préoccupation de tous les instants. Les nouvelles technologies offrent des outils de communication inédits aux criminels et il est logique que la société puisse retourner ces outils contre les criminels. Il cite les faits liés aux terrorisme, à la traite des êtres humains ou à la pédophilie: il y a lieu dans ces domaines de démanteler les réseaux, ce qui est l'essence même d'une politique policière intelligente et efficace.

Les métadonnées sont des sources incontournables pour les services de police et de renseignement. Il y a là un équilibre à trouver entre ces deux objectifs et il s'agit d'un exercice difficile. M. Prévot espère que le projet de loi tel que proposé – qui semble mieux équilibré – ne conduira pas à une troisième annulation par la Cour constitutionnelle. La conservation unique et indifférenciée sur tout le territoire n'est plus le principe retenu. Les durées de conservation des données varient en fonction de leur nature: ce sont désormais les circonstances qui déterminent la couverture géographique éventuelle des territoires sur lesquels les données sont collectées. Cette attention portée au détail offre plus de garanties aux citoyens, ce dont le gouvernement a bien pris conscience par son ambition de répondre aux arrêts de la CJUE.

M. Erik Gilissen (VB) souligne l'importance de la lutte contre la criminalité et le terrorisme ainsi que de la possibilité de retrouver les enfants disparus, mais préconise parallèlement une solution équilibrée qui accorde l'attention requise au respect de la vie privée.

Le postulat du projet de loi à l'examen est que la conservation des données doit être l'exception et non la règle, et qu'elle doit être soumise à des critères clairs et objectifs. Le texte autorise toutefois, sur la base d'une série de critères, une conservation généralisée et indifférenciée sur l'ensemble du territoire belge.

van het privéleven. Hij herinnert eraan dat het de taak van de wetgever is om het debat niet te verdrinken in deze schijnbare techniciteit. De inzet van dit wetsontwerp voor de democratie is groot: hoe kan het recht op veiligheid van eenieder worden gewaarborgd zonder te vervallen in algemeen toezicht op de bevolking? De individuele vrijheid beschermt het bestaansrecht van eenieder, alsook het recht om te doen wat hij zelf wil en kiest. Het recht op de bescherming van het privéleven creëert die ruimte waarin eenieder vrij handelt omdat hij weet dat hij niemand rekenschap verschuldigd is. Vaak is dat de aanzet tot vooruitgang: zowel het individu als de samenleving hebben belang bij de bescherming van het privéleven van de medeburgers.

De spreker meent dat de bestrijding van de criminaliteit eveneens een permanente zorg moet zijn. Criminelen beschikken dankzij de nieuwe technologieën over volkomen nieuwe communicatiemiddelen, en het is dan ook niet meer dan logisch dat de samenleving deze instrumenten ook tégen hen kan gebruiken. De spreker verwijst naar terroristische daden, naar mensenhandel of naar pedofilie: in die domeinen moeten de netwerken worden opgerold, hetgeen de essentie is van een intelligent en doeltreffend politiebeleid.

De metagegevens zijn noodzakelijke bronnen voor de politie- en de inlichtingendiensten. Deze twee doelstellingen moeten in balans worden gebracht – geen makkelijke oefening. De heer Prévot hoopt dat het wetsontwerp zoals het thans voorligt – en dat evenwichtiger lijkt – niet zal leiden tot een derde vernietiging door het Grondwettelijk Hof. Dit wetsontwerp gaat niet langer uit van de veralgemeende en ongedifferentieerde bewaring op het hele grondgebied. De termijnen voor de gegevensbewaring variëren naargelang van de aard van de gegevens: voortaan zullen de omstandigheden de eventuele geografische dekking bepalen van de gebieden waarin de gegevens worden verzameld. Deze aandacht voor details biedt de burger meer waarborgen; uit het streven van de regering om tegemoet te komen aan de arresten van het HvJ-EU, blijkt dat ze zulks beseft.

De heer Erik Gilissen (VB) benadrukt het belang van misdaadbestrijding, bestrijding van terrorisme en de mogelijkheid om vermiste kinderen op te sporen, maar pleit tegelijk voor een evenwicht met de nodige aandacht voor de privacy.

Het uitgangspunt van het voorliggende wetsontwerp is dat de bewaring van gegevens de uitzondering moet zijn en niet de regel, en aan duidelijke en objectieve criteria onderworpen moet zijn. Toch biedt de tekst mogelijkheden om op basis van enkele criteria over te gaan tot een algemene en ongedifferentieerde gegevensbewaring over het hele Belgische grondgebied.

Dans l'exposé des motifs, le gouvernement indique qu'il n'est pas impossible que l'entièreté du territoire national soit visé par une conservation des données. Une conservation ciblée, fondée sur des facteurs objectifs visant, par exemple, certaines catégories de personnes ou certains groupes de personnes, sera possible. Un autre passage de ce document indique toutefois que la conservation de données ne visera jamais des individus ou des groupes spécifiques. Par qui la composition d'un groupe ou d'une catégorie sera-t-elle déterminée? Tous les utilisateurs de smartphones pourront-ils par exemple constituer une catégorie? Il conviendrait de préciser la définition de la taille du groupe et la manière dont les groupes seront identifiés.

Par dérogation à l'article 122 de la loi du 13 juin 2005 relative aux communications électroniques, les opérateurs pourront prendre connaissance du contenu des communications pour détecter toute fraude et toute forme d'utilisation malveillante. Il conviendra d'appliquer cette disposition avec prudence. En effet, contrôler automatiquement les SMS au moyen de filtres ou de mots clés en vue de lutter contre les SMS frauduleux et permettre aux collaborateurs des opérateurs de consulter les communications personnelles sont deux choses différentes.

L'exposé des motifs indique par ailleurs que les opérateurs pourront conserver d'autres données pouvant s'avérer nécessaires pour ce qui les concerne. Il s'agit d'une description très vague.

Par ailleurs, les développements indiquent que sans la conservation généralisée et indifférenciée des données de communication, de nombreuses données pourraient ne pas être disponibles, ce qui pourrait causer la perte de preuves essentielles. C'est pourquoi une conservation large est préconisée.

En outre, l'intervenant fait observer que les délais de conservation peuvent chaque fois être prolongés pour une période identique, et donc de manière *quasi* illimitée.

Le projet de loi à l'examen oblige les opérateurs à créer des bases de données complexes. Une obligation de conservation ciblée géographiquement est une donnée complexe que les serveurs, les bases de données ou tout autre système ne sont pas encore en mesure de traiter actuellement. Ces bases de données ne sont pas non plus prévues pour le gel des données (*quick freeze*) et pour la conservation ciblée. Le coût de ces systèmes et de ces modifications est élevé et il faut du temps pour les mettre en œuvre correctement. Quelles sont les garanties que ces coûts ne seront finalement pas répercutés sur le consommateur?

In de memorie van toelichting stelt de regering dat het niet onmogelijk is dat het gehele nationale grondgebied onder de gegevensbewaring valt. Er kan een gerichte bewaring gebeuren op basis van objectieve factoren, zoals categorieën van personen of bepaalde groepen van personen. Nochtans staat elders in hetzelfde document dat gegevensbewaring nooit gericht zal zijn op bepaalde personen of groeperingen. Wie bepaalt de omschrijving van een groep of een categorie? Kunnen alle personen met een smartphone bijvoorbeeld een categorie vormen? De omschrijving van de grootte van een groep, en van de manier waarop die groep bepaald wordt, moet duidelijker.

Operatoren mogen in afwijking van artikel 122 van de wet van 13 juni 2005 betreffende de elektronische communicatie kennis nemen van de inhoud van communicatie om fraude en vormen van kwaadwillig gebruik op te sporen. Met deze bepaling moet voorzichtig omgegaan worden. Het automatisch screenen van sms-berichten op basis van filters of sleutelwoorden om frauduleuze berichten tegen te gaan is iets anders dan medewerkers van operatoren die persoonlijke communicatie zouden kunnen inkijken.

De memorie van toelichting stelt voorts dat operatoren de mogelijkheid krijgen andere gegevens te bewaren die wat hen betreft nodig kunnen blijken. Dit is een zeer vage omschrijving.

Verder is in de memorie van toelichting te lezen dat het zonder de algemene en ongedifferentieerde bewaring van communicatiegegevens mogelijk is dat vele gegevens niet beschikbaar zijn, waardoor potentieel essentieel bewijsmateriaal verloren zal gaan. Er wordt bijgevolg gepleit voor een bewaring in de brede zin.

De spreker stelt daarnaast vast dat de bewaringstermijnen telkens voor eenzelfde periode, en dus quasi onbeperkt, kunnen worden verlengd.

Het voorliggende wetsontwerp verplicht operatoren tot het opzetten van complexe databanken. Een bewaarplicht op geografische wijze is een ingewikkeld gegeven waarvoor de servers, databanken of andere systemen op dit ogenblik niet klaar zijn. Tevens zijn deze databanken niet voorzien op de *quick freeze* en "targeted" bewaring. Aan dergelijke systemen en aanpassingen is een hoge kostprijs verbonden en er is tijd nodig om ze correct te implementeren. Welke garanties zijn er dat deze kosten uiteindelijk niet zullen worden doorgerekend aan de consument?

Dans quelle mesure le projet de loi à l'examen correspond-il aux législations similaires des autres États membres de l'Union européenne? Tous les pays de l'Union européenne devraient appliquer la même réglementation. La fourniture de certaines données provenant de services cryptés n'est-elle pas contraire au Règlement général sur la protection des données (RGPD)?

Enfin, les médecins et les avocats s'inquiètent de ce que leur secret professionnel n'est maintenu qu'en partie, à savoir uniquement pour les messages émanant d'eux, et pas pour ceux des patients ou des clients. Même lorsqu'il n'existe aucune indication d'un quelconque lien avec des faits punissables, ces messages pourraient être passés au crible. Il convient d'opérer une distinction entre les messages ordinaires et les communications relevant du secret professionnel, qui comprennent donc également les messages que les patients et les clients envoient à leurs médecins et à leurs avocats.

Mme Nathalie Gilson (MR) rappelle qu'il fallait donner suite à la décision de la Cour constitutionnelle et à la jurisprudence de la CJUE. Elle souligne que la Cour constitutionnelle suggérait certaines pistes alternatives, notamment sur la conservation ciblée sur une base géographique. Elle observe que ce sont les pistes qui ont été suivies et développées dans le projet de loi. Il s'agit à présent d'une conservation différenciée selon des critères géographiques par arrondissement et par zone de police en fonction de statistiques de criminalité et de listes de lieux stratégiques (aéroport, ambassades, assemblées parlementaires etc.) qui, au vu de l'importance pour la sécurité nationale, font l'objet d'une rétention pour une durée de douze mois. Pour elle, le projet de loi s'appuie sur un traitement plus adapté aux circonstances.

Parmi les avis reçus par la commission, elle pointe celui de la Police fédérale qui estime que le texte proposé par le gouvernement prévoit un dispositif complexe mais qui a le mérite de réussir à atteindre judicieusement et de manière innovante le très difficile équilibre entre les impératifs de protection de la vie privée et les nécessités opérationnelles et pratiques auxquelles un service de police œuvrant dans un état démocratique est soumis. Elle estime normal que les personnes habilitées au sein du *Centre for Cyber Security Belgium* (CCB) reçoivent la possibilité de demander des données d'identification, de trafic et de localisation aux opérateurs dans le cadre de la prévention et de la détection des infractions en matière de cyber criminalité et de la prévention de menaces contre la sécurité publique, ainsi que pour l'examen d'une éventuelle défaillance de la sécurité des réseaux ou de services de communication électronique. L'intervenante

In hoeverre stemt het voorliggende wetsontwerp overeen met gelijkaardige wetgeving in andere EU-lidstaten? In alle EU-landen zou dezelfde regelgeving moeten gelden. Is het verstrekken van bepaalde gegevens uit geëncrypteerde diensten niet in strijd met de Algemene Verordening Gegevensbescherming (AVG)?

Artsen en advocaten uiten tot slot hun bezorgdheid over het feit dat hun beroepsgeheim maar gedeeltelijk gevrijwaard wordt, namelijk enkel voor de berichten die van hen uitgaan, niet voor de berichten van patiënten en cliënten. Zelfs wanneer er geen aanwijzing is dat zij iets te maken hebben met strafbare feiten, zouden deze berichten gescreend kunnen worden. Er moet een onderscheid gemaakt worden tussen gewone berichten en communicatie die onder het beroepsgeheim valt, waaronder dus ook berichten die patiënten en cliënten naar hun arts en advocaat sturen.

Mevrouw Nathalie Gilson (MR) stelt dat er tegemoet moest worden gekomen aan het arrest van het Grondwettelijk Hof en aan de rechtspraak van het HvJ-EU. Ze geeft aan dat het Grondwettelijk Hof enkele alternatieve pistes suggereerde, meer bepaald over de gerichte bewaring op geografische basis. Ze stelt vast dat die pistes werden gevolgd en uitgewerkt in het wetsontwerp. Het gaat thans om een gedifferentieerde bewaring volgens geografische criteria per arrondissement en per politiezone, op grond van criminaliteitsstatistieken en van lijsten van strategische plaatsen (luchthaven, ambassades, parlementaire assemblees enzovoort) die, gelet op het belang voor de nationale veiligheid, het voorwerp uitmaken van een bewaring gedurende een termijn van twaalf maanden. Volgens de spreekster is het wetsontwerp gebaseerd is op een verwerking die beter op de omstandigheden is afgestemd.

Van de adviezen die de commissie heeft ontvangen, gaat de spreekster in op dat van de federale politie. In dat advies wordt gesteld dat de door de regering voorgelegde tekst voorziet in een complexe regeling, waarmee echter wél op oordeelkundige en vernieuwende wijze het zeer moeilijke evenwicht wordt bewerkstelligd tussen de vereisten inzake de bescherming van het privéleven eensdeels en de operationele en de praktische noden anderdeels waaraan een politiedienst in een democratische Staat is onderworpen. De spreekster vindt het normaal dat de gemachtigden binnen het Centrum voor Cybersecurity België (CCB) de mogelijkheid krijgen om identificatie-, verkeers- en locatiegegevens op te vragen bij de operatoren in het kader van het voorkomen en het opsporen van misdrijven inzake cybercriminaliteit, de preventie van dreigingen inzake de openbare veiligheid, alsook de analyse van eventuele beveiligingsproblemen

rappelle l'explosion des fraudes par Internet, qui est un enjeu prégnant et essentiel pour le moment.

Mme Gilson souligne que le législateur a opté pour une obligation de moyens permettant de manière strictement nécessaire, proportionnée et limitée aux opérateurs de pouvoir conserver les données au-delà des zones géographiques strictement limitées. Par ailleurs, elle rappelle que l'IBPT contrôlera le respect de cette obligation de moyens.

Le groupe MR soutiendra le projet de loi car l'équilibre semble atteint entre la meilleure sécurité et une prévention des risques, tout en préservant la vie privée et les libertés individuelles.

M. Koen Geens (CD&V) souligne que le texte à l'examen s'efforce à nouveau de trouver un équilibre délicat entre le respect de la vie privée et la sécurité. Il n'est pas simple de traduire l'équilibre entre ces deux valeurs dans des textes de loi qui devront résister à l'examen des plus hautes instances judiciaires. L'intervenant déplore que, dans ce domaine, l'Union européenne soit nettement moins efficace que les États-Unis. Lorsqu'il en va de la sécurité, l'Europe doit en effet se mesurer à ce pays. Les États-Unis fournissent le savoir-faire nécessaire pour suivre le rythme des organisations criminelles.

Le Conseil européen plaide depuis des années en faveur d'une réglementation en matière de preuves électroniques, alors qu'aux États-Unis, ce domaine est déjà régi depuis quatre ans par le *Cloud Act*. Il en va de même pour la conservation des données. M. Geens espère que le très lent processus décisionnel européen changera à l'avenir. Toute impunité et toute gestion laxiste de ces matières sont en effet à proscrire. Il est important de garder à l'esprit que les normes doivent être appliquées sur le terrain par des policiers, et non par les conseillers de la Cour de justice de l'Union européenne.

Dans son arrêt du 5 avril 2022 dans l'affaire C-140/20 (*The Commissioner of the Garda Síochána e.a.*), la Cour de justice de l'Union européenne a opéré une distinction assez singulière entre la sécurité nationale et la criminalité grave. Lorsqu'il y va de la sécurité nationale, plus de choses sont permises. Cette distinction est peut-être possible en théorie, mais l'intervenant évoque l'exemple pratique de la guerre contre la drogue (*war on drugs*) menée dans le port d'Anvers et dans le Limbourg du Nord, à laquelle participent également d'autres pays et des services de police ou de renseignement étrangers. Cet exemple relève-t-il de la criminalité grave ou de la

bij elektronische-communicatienetwerken of -diensten. De spreekster wijst op de hand over hand toenemende internetfraude, momenteel een prangend en essentieel probleem.

Mevrouw Gilson merkt op dat de wetgever heeft gekozen voor een middelenverbintenis die het de operatoren op strikt noodzakelijke, evenredige en beperkte wijze mogelijk maakt om gegevens buiten strikt afgebakende geografische gebieden te kunnen bewaren. Voorts herinnert zij eraan dat het BIPT toezicht zal houden op de inachtneming van die middelenverbintenis.

De MR-fractie zal het wetsontwerp steunen omdat het evenwicht tussen de beste veiligheid en het voorkomen van risico's lijkt te zijn gevonden, met vrijwaring van het privéleven en de individuele vrijheden.

De heer Koen Geens (CD&V) stipt aan dat de voorliggende tekst opnieuw een delicaat evenwicht tussen privacy en veiligheid probeert te bereiken. Het is niet eenvoudig het evenwicht tussen beide waarden te vertalen in wetteksten die de toetsing van de hoogste rechters moeten doorstaan. De spreker betreurt dat de Europese Unie op dit vlak veel minder slagkrachtig is dan de Verenigde Staten. Wanneer de veiligheid ter discussie staat, moet Europa zich immers met dat land meten. De VS leveren de nodige knowhow om gelijke tred te houden met misdaadorganisaties.

In de Europese Raad wordt al jaren gepleit voor een regeling inzake *e-evidence*, terwijl dit in de Verenigde Staten al vier jaar geregeld is door middel van de *Cloud Act*. Hetzelfde geldt voor dataretentie. De heer Geens hoopt dat er in de toekomst verandering komt in het zeer trage tempo van de Europese besluitvorming. Straffeloosheid en een lakse omgang met deze materies zijn immers uit den boze. Het is belangrijk in het achterhoofd te houden dat de normen moeten toegepast worden door politiemensen in het veld, en niet door de raadsheren van het Hof van Justitie van de Europese Unie.

In zijn arrest van 5 april 2022 in de zaak C-140/20 (*The Commissioner of the Garda Síochána e.a.*) maakte het HvJ-EU een merkwaardig onderscheid tussen nationale veiligheid en zware criminaliteit. In het kader van nationale veiligheid is meer toegelaten. Dit onderscheid is misschien mogelijk in theorie, maar de spreker wijst op het praktijkvoorbeeld van de *war on drugs* in de Antwerpse haven en Noord-Limburg, waarbij andere landen en ook buitenlandse politie- of inlichtingendiensten betrokken zijn. Valt dat onder zware criminaliteit of onder nationale veiligheid? Het zou betekenen dat de Veiligheid van de Staat, bevoegd voor het laatstgenoemde domein,

sécurité nationale? Cela signifierait que la Sûreté de l'État, compétente dans le second domaine, pourrait probablement conserver des données plus facilement que la police dans le cadre de la lutte contre la criminalité grave.

M. Geens espère que l'arrêt précité de la Cour de justice de l'Union européenne fournira enfin une réponse définitive. La nécessité de devoir chaque fois refaire le travail législatif crée, dans l'intervalle, de l'insécurité juridique. Le fait que le projet de loi à l'examen soit le fruit d'un long processus montre que l'équilibre entre les valeurs "respect de la vie privée" et "sécurité" est très sensible dans la société. Lorsqu'un attentat est commis ou lorsqu'un enfant est enlevé, cet équilibre semble toutefois ne plus être de mise. Les services de sécurité sont chaque fois le bouc émissaire lorsque des faits de ce type ne sont pas détectés à temps.

La Cour constitutionnelle a rendu, le 18 novembre 2021, un arrêt (n° 158/2021) relatif aux cartes SIM anonymes. Après l'affaire de Verviers, on s'est efforcé de supprimer l'anonymat de ces cartes. À l'époque, le débat à propos de la sécurité et du respect de la vie privée a été si houleux que la législation s'est encore fait attendre un an. Dans l'intervalle, les cartes SIM anonymes étaient dépassées dans les milieux terroristes, ce qui montre que les pouvoirs publics courent après les faits. La Cour constitutionnelle estime que la législation n'est pas étanche, en ce qu'elle ne prévoit pas quelles données d'identification sont recueillies et quels documents d'identification entrent en ligne de compte. Les amendements tendant à régler ces problèmes seront bientôt présentés.

La Cour de justice de l'Union européenne a avancé un critère géographique pour la conservation de données. Dans un petit pays à très forte densité de population comme la Belgique, cela donne inévitablement lieu à des discussions. La différenciation au travers du recours aux statistiques est intéressante lorsqu'il existe des différences importantes. Or, le territoire belge est d'une nature telle qu'il n'est pas évident de mettre en œuvre cette différenciation. L'intervenant espère que le fait que l'approche géographique pourrait avoir comme conséquence d'impliquer l'ensemble du territoire ne pose pas de problème, pour le gouvernement, à l'égard de la jurisprudence de la Cour de justice de l'Union européenne.

À cela s'ajoute le problème de l'encryptage. Les utilisateurs des services cryptés comptent sur le fait qu'il n'est pas possible de décrypter les communications personnelles. Or, c'est parfois nécessaire. L'intervenant se félicite dès lors que l'autorisation de chiffrement soit soumise à trois restrictions: le chiffrement ne peut pas

waarschijnlijk makkelijker aan dataretentie kan doen dan de politie bij de bestrijding van zware criminaliteit.

De heer Geens hoopt dat het genoemde arrest van het HvJ-EU eindelijk uitsluitsel biedt. De noodzaak om het wetgevend werk telkens te moeten overdoen zorgt in tussentijd voor rechtsonzekerheid. Het feit dat het voorliggende wetsontwerp de vrucht van een lang proces is, toont aan dat het evenwicht tussen de waarden privacy en veiligheid zeer gevoelig ligt in de samenleving. Op het moment dat er een aanslag wordt gepleegd, of bij de ontvoering van een kind, lijkt dat echter niet meer aan de orde. De veiligheidsdiensten zijn telkens kop van Jut wanneer dergelijke feiten niet tijdig gedetecteerd worden.

Het Grondwettelijk Hof velde op 18 november 2021 een arrest (nr. 158/2021) over anonieme simkaarten. Na de zaak-Verviers werd gepoogd deze te de-anonimiseren. Ook toen was het debat over veiligheid en privacy dermate heftig dat de wetgeving nog een jaar op zich liet wachten. Anonieme simkaarten waren ondertussen voorbijgestreefd in terroristische milieus. Dit toont aan dat de overheid achter de feiten aanloopt. Volgens het Grondwettelijk Hof is de wetgeving niet waterdicht in zoverre niet bepaald wordt welke identificatiegegevens verzameld worden en welke identificatiedocumenten in aanmerking komen. De amendementen om deze problemen recht te zetten, zullen weldra worden ingediend.

Het HvJ-EU reikte een geografisch criterium aan voor het bewaren van gegevens. In een klein en zeer dichtbevolkt land zoals België leidt dat onvermijdelijk tot discussie. Differentiëren door het gebruik van statistieken is interessant wanneer er grote verschillen zijn. Het Belgische grondgebied is echter van die aard dat het niet evident is deze differentiatie door te voeren. De spreker hoopt dat het feit dat de geografische aanpak tot gevolg zou kunnen hebben dat het hele grondgebied wordt betrokken in de ogen van de regering geen probleem vormt ten aanzien van de rechtspraak van het HvJ-EU.

Encryptie is een volgend probleem. Gebruikers van geëncrypteerde diensten rekenen erop dat het decrypteren van persoonlijke communicatie niet mogelijk is, maar in sommige gevallen kan dat toch noodzakelijk zijn. De spreker is dan ook verheugd dat versleuteling is toegelaten met drie beperkingen: ze mag de hulpdiensten

entraver les services de secours, il ne peut pas empêcher un opérateur de remplir ses obligations en matière de conservation des données et l'encryptage ne peut pas empêcher l'interception légale.

Sur le territoire belge, il est relativement facile de constater que c'est le cas (l'intervenant renvoie à jurisprudence dite "Yahoo" à cet égard), mais c'est toutefois problématique au niveau extraterritorial, *a fortiori* dès lors que les normes 5G ne prévoient plus de *local breakout* vers les opérateurs européens. Il sera donc crucial de veiller autant que possible, lors de la conclusion de contrats de *roaming* entre des opérateurs belges et des acteurs étrangers comme AT&T, à ce que la législation belge relative à l'encryptage puisse être appliquée.

M. Geens comprend que l'on redoute les abus. Un contrôle hiérarchique sera toutefois exercé dans la plupart des cas, sauf en cas de disparition inquiétante, mais en pareil cas, tout le monde convient que la sécurité de la personne disparue l'emporte sur la réglementation la plus stricte. La disparition de Théo Hayez a montré que la localisation des personnes à l'aide de nouveaux moyens techniques constitue l'un des moyens les plus intéressants pour les retrouver.

L'APD est très critique dans son avis n° 108/2021 du 28 juin 2021. Le gouvernement a-t-il suivi certains points de cet avis et, dans l'affirmative, de quelle manière? L'APD souligne "que si cela s'avère nécessaire en vue de lutter contre la criminalité grave, les autorités peuvent "hacker" les appareils téléphoniques pendant leur utilisation […] ou encore faire appel à des techniques particulières de recherche (comme l'infiltration, l'observation à l'aide de moyens techniques, le recours aux indicateurs, …). L'Autorité fait observer que ces différents moyens, qui sont mis à la disposition des autorités répressives, rendent, sans doute, la lutte contre la criminalité grave plus facile qu'auparavant et qu'en tout cas, il n'existe aucune preuve du contraire."

Le point de vue de l'APD est étonnant. Le ministre de la Justice estime-t-il que le projet de loi à l'examen permettra de combattre la criminalité grave plus facilement qu'auparavant, comme l'indique l'avis?

La conservation des données est mise à profit dans un très grand nombre de dossiers qui aboutissent à une condamnation. Les données ainsi réunies ne sont pratiquement jamais rejetées par les cours et tribunaux. Comment l'expliquer? Si certaines enquêtes étaient totalement ou partiellement annulées, ce ne serait pas bon pour la sécurité et la lutte contre la criminalité grave.

niet belemmeren, ze mag de operator niet beletten zijn verplichtingen inzake dataretentie na te leven en encryptie mag de legale interceptie niet verhinderen.

Voor het Belgische grondgebied kan dit vrij makkelijk vastgelegd worden (waarbij de spreker verwijst naar de Yahoo-rechtspraak van het Hof van Cassatie), maar extraterritoriaal is dit problematisch, zeker omdat de 5G-standaarden in geen *local breakout* naar Europese operatoren meer voorzien. Het zal bijgevolg cruciaal zijn dat er bij het sluiten van roamingcontracten door Belgische operatoren met buitenlandse spelers, zoals AT&T, maximaal voor wordt gezorgd dat de Belgische wetgeving inzake encryptie toegepast kan worden.

De heer Geens heeft begrip voor de angst voor misbruik. In de meeste gevallen is er echter een hiërarchische controle, behalve bij een onrustwekkende verdwijning, maar op een dergelijk moment bestaat er consensus dat de veiligheid van de betrokken persoon voorgaat op de strengste regelgeving. De verdwijning van Théo Hayez heeft aangetoond dat de lokalisatie van personen met nieuwe technische middelen een van de interessantste manieren is om mensen terug te vinden.

De GBA is zeer kritisch in haar advies nr. 108/2021 van 28 juni 2021. Heeft de regering punten uit dit advies opgevolgd, en zo ja, hoe? De GBA wijst erop "dat de autoriteiten, indien nodig ter bestrijding van zware criminaliteit, telefoontoestellen kunnen "hacken" terwijl deze in gebruik zijn (…) of speciale onderzoekstechnieken kunnen toepassen (zoals infiltratie, observatie met technische middelen, gebruik van indicatoren, enz.) De Autoriteit merkt op dat deze verschillende middelen, waarover de handhavingsautoriteiten beschikken, het ongetwijfeld gemakkelijker maken om zware criminaliteit te bestrijden dan voorheen en dat er in ieder geval geen bewijs is van het tegendeel.".

Het standpunt van de GBA is verbazend. Is de minister van Justitie van oordeel dat door het voorliggende wetsontwerp de zware criminaliteit makkelijker dan vroeger bestreden kan worden, zoals in het advies wordt gesuggereerd?

In een indrukwekkend aantal dossiers die leiden tot een veroordeling wordt gebruik gemaakt van dataretentie. De op deze manier verzamelde gegevens worden vrijwel nooit geweerd door de hoven en rechtbanken. Hoe kan dit worden verklaard? Indien onderzoeken geheel of gedeeltelijk nietig verklaard zouden worden, zou dat voor de veiligheid en de bestrijding van de zware criminaliteit geen goede zaak zijn.

Contrairement à l'APD, l'Organe de contrôle de l'information policière (COC) a remis un avis encourageant sur le projet de loi à l'examen. Il a cependant émis quelques réserves à propos des données que la Banque de données Nationale Générale (BNG) doit fournir. Comment le ministre répondra-t-il aux observations du COC?

Le ministre a-t-il en outre déjà pris des mesures à propos de la collecte des données et des chiffres concernant la criminalité sur la base desquels les arrondissements judiciaires ou les zones de police seront sélectionnés? L'intervenant renvoie à l'application de l'article 90*ter* du Code d'Instruction criminelle.

Dans son arrêt du 5 avril 2022 (C-140/20), la Cour de justice de l'Union européenne a de nouveau validé l'approche géographique de la conservation des données. La Cour indique dans le paragraphe 80 de cet arrêt que "les autorités nationales compétentes peuvent prendre une mesure de conservation ciblée fondée sur un critère géographique, tel que notamment le taux moyen de criminalité dans une zone géographique, sans qu'elles disposent nécessairement d'indices concrets portant sur la préparation ou la commission, dans les zones concernées, d'actes de criminalité grave". C'est une bonne chose pour la sécurité. Le ministre part-il du principe que cette zone géographique pourra couvrir l'ensemble du territoire?

Enfin, M. Geens se félicite que le projet de loi soit à l'examen et espère qu'il sera adopté rapidement.

M. Nabil Boukili (PVDA-PTB) estime que la conservation des données télécom et leur transmission aux autorités constituent des ingérences extrêmement importantes dans la vie privée, comme le rappellent l'Autorité de protection des données (APD) et Mme Forget notamment. À ce titre, l'intervenant observe que l'APD insiste pour prendre le temps de la réflexion avant d'approuver ce projet de loi, où deux logiques s'affrontent: d'une part, la nécessité de disposer d'un certain nombre de données, prises de façon ciblée, pour lutter notamment contre la criminalité grave et organisée ou la délinquance financière. D'autre part, comme le rappelle la jurisprudence, il ne peut exister de conservation généralisée et indifférenciée des données télécom: c'est d'ailleurs pour cette raison que deux lois similaires au présent projet de loi ont déjà été annulées par la Cour constitutionnelle. Une balance doit donc être réalisée entre ces deux logiques. À ce stade, M. Boukili estime qu'elle n'a pas été correctement pondérée.

Anders dan de GBA heeft het Controleorgaan op de politionele informatie (COC) een bemoedigend advies afgeleverd met betrekking tot het voorliggende wetsontwerp. Niettemin wordt enig voorbehoud gemaakt met betrekking tot de gegevens die door de Algemene Nationale Gegevensbank (ANG) moeten worden aangeleverd. Hoe zal de minister tegemoetkomen aan de opmerkingen van het COC?

Heeft de minister voorts reeds maatregelen genomen in het kader van het verzamelen van de gegevens en de criminaliteitscijfers op basis waarvan de gerechtelijke arrondissementen of de politiezones zullen worden geselecteerd? De spreker verwijst naar de toepassing van artikel 90*ter* van het Wetboek van Strafvordering.

In zijn arrest van 5 april 2022 (C-140/20) heeft het HvJ-EU de geografische benadering van dataretentie nogmaals gevalideerd. Het Hof stelt in paragraaf 80 van dit arrest dat de bevoegde nationale autoriteiten "een gerichte bewaringsmaatregel kunnen nemen op basis van een geografisch criterium, zoals met name het gemiddeld criminaliteitscijfer in een geografische zone, zonder noodzakelijkerwijs concrete aanwijzingen te hebben dat er in die zones zware misdaden worden voorbereid of gepleegd". Dit is een goede zaak voor de veiligheid. Gaat de minister ervan uit dat deze geografische zone het volledige grondgebied zal kunnen dekken?

De heer Geens is tot slot verheugd dat het wetsontwerp ter bespreking voorligt en hoopt dat het snel wordt aangenomen.

De heer Nabil Boukili (PVDA-PTB) meent dat de bewaring van telecomgegevens en het feit dat men ze aan de overheid bezorgt, neerkomt op een heel verregaande vorm van inmenging in de persoonlijke levenssfeer, zoals ook de Gegevensbeschermingsautoriteit (GBA) en mevrouw Forget hebben aangestipt. De spreker merkt daarbij op dat de GBA erop aandringt dat voldoende bedenktijd te nemen alvorens het wetsontwerp aan te nemen. Dat wetsontwerp behelst immers een water- en een vuurcomponent: eensdeels moet men kunnen beschikken over een aantal gegevens die op gerichte wijze worden verzameld, teneinde meer bepaald de zware en georganiseerde criminaliteit en financiële delinquentie aan te pakken; anderdeels kan er, zoals de rechtspraak ook aangeeft, geen sprake van zijn dat telecomgegevens op veralgemeende wijze en ongedifferentieerd worden bijgehouden. Om die reden heeft het Grondwettelijk Hof trouwens al twee wetten vernietigd die bij het wetsontwerp aanleunen. Er moet dus een evenwicht tussen die beide componenten worden gevonden. Tot dusver is er volgens de heer Boukili geen correct evenwicht.

M. Boukili explique que son groupe ne peut adhérer à la logique sous-jacente à ce texte et au mécanisme qu'il met en place. À ses yeux, le projet de loi impose la surveillance généralisée et indifférenciée de certains lieux. Il vise notamment le mécanisme du nouvel article 126/1, en projet, de la loi du 13 juin 2005 (article 9 du projet de loi), qui impose aux opérateurs de conserver les données de toutes les communications effectuées à partir ou vers l'une des zones géographiques qu'il délimite. Cette délimitation se fera sur la base de deux critères. D'une part, le projet de loi impose la collecte des données de certaines zones considérées comme soumises à un risque élevé de criminalité grave (comme les gares ou les aéroports). D'autre part, en plus de ces zones, une conservation systématique sera imposée sur les arrondissements sujets à un taux important "d'infractions graves", en fonction d'une moyenne, et pour une durée dépendant du taux d'infractions enregistrées dans la Banque de données nationale générale (BNG).

Il est donc prévu de procéder à la surveillance constante et généralisée de certains quartiers, y compris des habitants n'ayant rien à se reprocher qui y vivraient ou même qui transiteraient par-là, sur la base du nombre d'infractions constatées par la police. Pour l'intervenant, il s'agit de la création d'une société à deux vitesses, ainsi que l'application d'une punition collective puisque les citoyens seront surveillés qu'ils aient quelque chose à se reprocher ou non. Il ne peut adhérer à cette logique qui va à l'encontre du principe de la minimisation des données et de la nécessité de cibler et de limiter strictement ce type d'ingérence particulièrement grave dans la vie privée. Mettre sous surveillance généralisée des populations entières n'est pas acceptable dans un état de droit.

Sur l'étendue de la surveillance, particulièrement sur le plan géographique, les critères permettant la surveillance de certaines zones sont particulièrement larges, de sorte qu'une partie importante du territoire national sera en fait concernée. La notion "d'infractions graves" est elle-même très large et reprend entre autres des faits tels que le vol, la détention de stupéfiants, ou encore la fraude informatique. Plus fondamentalement, le critère ne se base pas sur le nombre de "faits commis", mais sur les données reprises dans la BNG, banque de données de la police qui reprend tous les faits constatés ou suspectés, tels qu'ils sont qualifiés en début d'enquête. Cette BNG recense 3 millions de personnes en 2019. Comme l'indique lui-même l'Organe de contrôle de l'information policière (COC), "ce n'est un secret pour personne qu'il y avait assez bien de friture sur la ligne en

De heer Boukili legt uit dat zijn fractie zich niet kan vinden in de logica achter dit wetsontwerp noch in de regeling die het tot stand wil brengen. Volgens hem heeft het wetsontwerp tot doel bepaalde plaatsen te onderwerpen aan een veralgemeend en ongedifferentieerd toezicht. De spreker verwijst meer bepaald naar het ontworpen nieuwe artikel 126/1 van de wet van 13 juni 2005 (artikel 9 van het wetsontwerp), waarbij de operatoren verplicht zouden worden tot het bijhouden van de gegevens van alle communicatie van en naar bepaalde afgebakende geografische zones. Die afbakening zou gebeuren op basis van twee criteria. Ten eerste wil het wetsontwerp de verplichting opleggen om gegevens te verzamelen in bepaalde gebieden waarvan wordt aangenomen dat er een hoog risico op zware criminaliteit is (zoals stations of luchthavens). Ten tweede zou het stelselmatig bijhouden van gegevens niet alleen verplicht zijn in de voormelde gebieden, maar ook in bepaalde arrondissementen met een hoog percentage aan ernstige misdrijven, op basis van een gemiddelde en voor een termijn die afhankelijk is van het percentage misdrijven dat wordt geregistreerd in de Algemene Nationale Gegevensbank (ANG).

Het zou dus de bedoeling zijn dat bepaalde wijken, waar ook mensen wonen of langskomen die niets te verwijten valt, onder permanent en algemeen toezicht komen te staan op basis van het aantal door de politie vastgestelde inbreuken. Volgens de spreker schept men op die manier een samenleving met twee versnellingen die in collectieve straffen voorziet: de burgers zouden immers onder toezicht staan, ongeacht of ze al dan niet iets hebben mispeuterd. De spreker kan niet instemmen met die regeling, die indruist tegen het beginsel van de minimale gegevensverwerking en tegen het feit dat een dergelijke bijzonder ingrijpende vorm van inmenging in de persoonlijke levenssfeer strikt gericht moet worden gebruikt en beperkt. In een rechtsstaat is het onaanvaardbaar dat hele bevolkingsgroepen onder algemeen toezicht worden geplaatst.

Betreffende de reikwijdte van het toezicht, inzonderheid op geografisch gebied, is het zo dat de criteria op basis waarvan bepaalde gebieden zouden kunnen worden bewaakt, heel ruim worden opgevat, waardoor een aanzienlijk deel van het nationaal grondgebied onder die regeling zou vallen. Het begrip "ernstige misdrijven" is op zich al heel ruim en omvat onder meer feiten als diefstal, het bezit van verdovende middelen of nog informaticafraude. Een fundamenteler probleem is dat het criterium niet is gebaseerd op het aantal "gepleegde feiten", maar op de gegevens van de ANG, de databank van de politie waarin alle vastgestelde en vermeende feiten zijn opgenomen zoals ze bij de aanvang van het onderzoek zijn gekwalificeerd. In die ANG stonden in 2019 drie miljoen personen geregistreerd. Het Controleorgaan op de politionele informatie (COC) geef zelf aan dat

ce qui concerne l'exactitude (permanente) des enregistrements policières". Dans son rapport annuel de 2020, le COC indique que "la BNG contient de nombreuses inexactitudes et/ou erreurs" comme "la qualification erronée donnée aux faits".

En outre, la liste des lieux "sensibles" qui seront surveillés en permanence est longue et comprend une bonne partie des voies de communication par lesquelles transitent la majorité des citoyens, comme les gares, les aéroports ou encore les autoroutes et les parkings attenants. Toutes les personnes qui transitent par ces lieux verront leurs données conservées, qu'elles aient quelque chose à se reprocher ou non.

M. Boukili rappelle que la conservation généralisée et indifférenciée des données n'est pas permise par la jurisprudence européenne. Il y a lieu de vérifier si, en approuvant ce projet, on ne rentre pas de nouveau dans cette surveillance généralisée. Ces critères particulièrement larges font craindre qu'une bonne partie du territoire national soit concernée par cette mesure de surveillance. Il souhaiterait savoir quel est le pourcentage du territoire et les chiffres de population qui seront concernés par cette surveillance: il s'agit d'une exigence de l'APD, qui demande la transparence sur ces deux chiffres.

Il aimerait par ailleurs connaître le réaction du gouvernement aux remarques du COC sur la faible fiabilité des données reprises dans la BNG.

Sur l'étendue des faits pour lesquels on peut être surveillé, il observe que la surveillance de zones géographiques se fera sur la base des données de la BNG. Or celles-ci concernent de façon indifférenciée des infractions simplement suspectées, mais aussi éventuellement classées sans-suite, ou ayant fait l'objet d'un non-lieu ou d'un acquittement; il ne s'agit donc pas des faits commis, jugés et ayant abouti à une condamnation. Il s'inquiète du fait que des populations entières soient surveillées sur la base de simples soupçons. Il se demande comment le gouvernement articule cela avec le principe de la minimisation des données et avec l'exigence de proportionnalité.

Outre cette remarque qui concerne la surveillance "ciblée" des quartiers, d'autres articles du projet de loi réintroduisent en fait une surveillance généralisée sur l'ensemble du territoire; l'intervenant vise ici les modifications apportées aux articles 122 (notamment les paragraphes §§ 4, 4/1 et 4/2, en projet), 123, 126 et 127 de la loi du 13 juin 2005 (articles 5, 6, 8 et 10 du

het "een publiek geheim [is] dat er nogal wat ruis op de lijn zit wat de (blijvende) correctheid van de politionele registraties betreft.". In zijn jaarverslag van 2020 stipt het COC aan dat "de ANG heel wat onnauwkeurigheden en/of fouten bevat", zoals "de onjuiste kwalificatie van de feiten".

Bovendien is de lijst van "gevoelige" plaatsen die permanent zouden worden bewaakt lang en omvat ze veel van de verbindingswegen waarvan de meeste burgers gebruik maken, zoals treinstations, luchthavens, autosnelwegen en de bijbehorende parkeerterreinen. Van alle mensen die daar langs komen zouden de gegevens worden bijgehouden, of ze nu iets mispeuterd hebben of niet.

De heer Boukili wijst erop dat de Europese rechtspraak het algemeen en ongedifferentieerd bijhouden van gegevens niet toestaat. Men dient zich ervan te vergewissen dat men, door dit wetsontwerp aan te nemen, zich niet opnieuw gaat bezondigen aan dergelijk veralgemeend toezicht. De bijzonder ruim opgevatte criteria doen vrezen dat een groot deel van het nationale grondgebied onder die toezichtmaatregel zal vallen. De spreker wil weten welk percentage van het grondgebied en de bevolking onder dergelijk toezicht zou vallen. Dat is overigens ook een eis van de GBA, die transparantie over deze twee cijfers vraagt.

Voorts vraagt de heer Boukili de regering naar een reactie op de opmerkingen van de COC over de lage betrouwbaarheid van de gegevens van de ANG.

Wat de reikwijdte betreft van de feiten waarvoor men kan worden gemonitord, merkt de spreker op dat het toezicht op geografische zones zou worden uitgevoerd op basis van de gegevens van de ANG. Die gegevens kunnen echter betrekking hebben op vermoedelijke inbreuken of inbreuken, maar ook op inbreuken die werden geseponeerd, waarvoor de dader buiten vervolging werd gesteld of werd vrijgesproken. Het betreft in dezen dus geen feiten die werden gepleegd, voor de rechter gebracht en tot een veroordeling hebben geleid. De spreker maakt zich zorgen dat hele bevolkingsgroepen aldus zouden worden gemonitord op grond van loutere vermoedens. Hij vraagt zich af hoe de regering dat kan rijmen met het principe dat gegevens minimaal moeten worden bijgehouden en met de evenredigheidsvereiste.

De spreker heeft niet alleen bedenkingen bij het "gerichte" toezicht op wijken, maar ook bij het feit dat andere artikelen van het wetsontwerp in feite opnieuw een veralgemeend toezicht op het volledige grondgebied beogen in te voeren. Hij doelt daarmee op de wijzigingen die zouden worden aangebracht aan de artikelen 122 (meer bepaald de ontworpen paragrafen §§ 4, 4/1 en

projet de loi). Les opérateurs devront, selon l'article 122, § 4, en projet, conserver les données de localisation et autres données de trafic nécessaires afin d'analyser et de détecter des fraudes et des malveillances. Comme l'indique l'APD, cette finalité est légitime. Cependant il faut encore que la conservation des données prévue soit nécessaire et proportionnée à atteindre son objectif.

L'intervenant estime que c'est là que le bât blesse: l'article 122, § 4, en projet, crée une obligation de conservation systématique des données de localisation et de trafic de l'ensemble des utilisateurs, qui n'est pas admise par la CJUE. A ses yeux, cette conservation de données est beaucoup trop large par rapport à l'objectif poursuivi. Il relève de surcroît que les données conservées en application de cette disposition peuvent être communiquées aux autorités et pour les finalités visées au nouvel article 127/1, en projet (article 11 du projet de loi), notamment aux autorités répressives et aux services de renseignement. Comme l'indique l'APD, le projet aboutit donc *de facto* "à réintroduire une obligation de conservation généralisée et indifférenciée des données pour lutter contre la criminalité", ce qui a déjà été censuré par la CJUE et par la Cour constitutionnelle.

La même remarque vaut pour les autres articles cités puisqu'ils reprennent cette possibilité de transmission aux autorités.

Sur la question de l'étendue des données collectées, M. Boukili relève que le projet de loi impose la collecte systématique et indifférenciée des données de souscription et des données d'identification des abonnés. La liste des données va plus loin que ce qui est autorisée par la CJUE, qui n'autorise une collecte indifférenciée que pour les adresses IP (c'est une exception au régime selon lequel la collecte doit être ciblée). Le projet de loi va plus loin, en étendant la conservation des données par exemple à l'identifiant créé pour chaque communication, à la date de début de l'abonnement, aux données relatives au type de paiement etc.

Au-delà de poser des problèmes au regard des droits humains, M. Boukili estime que le système instauré par la loi est impraticable. Mme Forget souligne ces difficultés pour les opérateurs tels que Facebook, WhatsApp ou encore Skype, qui seront soumis aux mêmes obligations que les opérateurs télécom en suivant ce projet de loi. Ces services ne sont pas nécessairement en mesure de

4/2), 123, 126 en 127 van de wet van 13 juni 2005 (artikelen 5, 6, 8 en 10 van het wetsontwerp). Volgens het ontworpen artikel 122, § 4, zouden de operatoren de vereiste locatie- en andere verkeersgegevens moeten bewaren om gevallen van fraude en kwaadwilligheid te analyseren en op te sporen. Zoals de GBA aangeeft, is dat een rechtmatig doel. Niettemin dient de in uitzicht gestelde bewaring van de gegevens noodzakelijk te zijn en moet ze in verhouding staan tot het vooropgestelde doel.

Volgens de spreker knelt net daar het schoentje: het ontworpen artikel 122, § 4, strekt ertoe de verplichting in te stellen tot het stelselmatig bewaren van de locatie- en verkeersgegevens van alle gebruikers, wat niet mag volgens het HvJ-EU. De spreker geeft aan dat de bewaring van die gegevens veel te ver gaat in verhouding tot het nagestreefde doel. Hij merkt bovendien op dat de gegevens die met toepassing van die bepaling worden bewaard, aan de overheid kunnen worden bezorgd, en wel voor de in het nieuwe ontworpen artikel 127/1 (artikel 11 van het wetsontwerp) bepaalde doeleinden; zulks houdt in dat de gerechtelijke instanties en de inlichtingendiensten ze in bezit kunnen krijgen. Zoals de GBA aangeeft, leidt het wetsontwerp bijgevolg tot de "herinvoering, *de facto*, van verplichtingen inzake de veralgemeende en ongedifferentieerde bewaring van de gegevens", wat reeds door het HvJ-EU en het Grondwettelijk Hof werd gelaakt.

Dezelfde opmerking geldt voor de andere aangehaalde artikelen, aangezien ook die in de mogelijkheid voorzien om gegevens aan overheden te bezorgen.

Wat de reikwijdte van de verzamelde gegevens betreft, merkt de heer Boukili op dat het wetsontwerp zou voorzien in de stelselmatige en ongedifferentieerde verzameling van de abonnements- en identiteitsgegevens van de abonnees. De lijst van de gegevens is ruimer dan die welke het HvJ-EU toestaat; van het HvJEU mogen alleen gegevens met betrekking tot IP-adressen ongedifferentieerd worden verzameld (een uitzondering op de regel volgens welke de verzameling gericht dient te zijn). Het wetsontwerp gaat een stap verder, door de gegevensbewaring te verruimen tot bijvoorbeeld de identificatiecodes die voor elke communicatie wordt gecreëerd, de aanvangsdatum van het abonnement, de gegevens inzake de betalingskanalen enzovoort.

Volgens de heer Boukili rijzen er met het wetsontwerp niet alleen problemen met betrekking tot de mensenrechten, maar is de erin voorgestelde regeling bovendien niet werkbaar. Mevrouw Forget wijst op de problemen die de implementering ervan zou meebrengen voor operatoren zoals Facebook, WhatsApp of Skype, die op grond van dit wetsontwerp aan dezelfde verplichtingen zouden

déterminer la localisation de l'utilisateur de sorte qu'ils devraient alors collecter et conserver l'ensemble des données sur le territoire belge, ce qui n'est pas permis par la jurisprudence européenne.

En conclusion, l'intervenant fait part d'une remarque importante de l'APD: la conservation des données doit rester l'exception, et non devenir la règle. La Cour constitutionnelle a rappelé, dans son arrêt du 21 avril 2021, qu'il faut un "changement de perspective" par rapport au choix effectué à l'époque par le législateur. Or, à ses yeux, le nouveau projet de loi n'opère pas complètement ce changement de perspective: il impose de nouvelles mesures de conservation de données qui pourraient aboutir à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données.

L'intervenant regrette que le projet de loi crée de nombreux traitements de données et des ingérences importantes dans la vie privée et la protection des données personnelles. Les données collectées et communiquées sont très larges, tout comme les motifs pour lesquels elles peuvent être collectées et communiquées (facturation, profilage, recherche d'infractions, poursuite des fraudes etc.). Rien qu'à voir le tableau récapitulatif dressé par l'APD, il constate que la collecte des données devient la règle, et non l'exception. Le projet limitera également l'usage de la cryptographie, ce qui revient à considérer *a priori* tout le monde comme suspect.

Pour toutes ces raisons, le groupe PVDA-PTB n'apportera pas son soutien au texte.

Mme Kathleen Verhelst (Open Vld) observe, sur la base des avis volumineux et des intérêts divergents, que le projet de loi à l'examen est un exercice d'équilibre très délicat. Les droits fondamentaux des citoyens doivent être défendus, alors que les points de vue des différentes instances d'avis divergent souvent ou semblent parfois contradictoires. L'élaboration de ce projet de loi a donc dû être un défi intellectuel.

Dans son avis, l'association professionnelle des opérateurs évoque la nécessité d'un cadre légal stable. Le gouvernement crée-t-il cette fois une base légale adéquate pour la conservation des données, compte tenu des arrêts antérieurs de la Cour constitutionnelle?

Une autre préoccupation libérale est le respect de la vie privée: moins on conserve de données, mieux

worden onderworpen als de telecomoperatoren. Die diensten zijn niet noodzakelijk bij machte de locatie van de gebruiker te bepalen, zodat ze bijgevolg alle voor het Belgische grondgebied beschikbare gegevens zouden moeten verzamelen en bewaren, wat dan weer in strijd is met de Europese rechtspraak.

Tot slot haalt de spreker een belangrijke opmerking van de GBA aan, namelijk dat de bewaring van de gegevens de uitzondering moet blijven en niet de regel mag worden. Het Grondwettelijk Hof heeft er in zijn arrest van 21 april 2021 op gewezen dat een "verandering van gezichtspunt" is vereist ten aanzien van de keuze die de wetgever destijds heeft gemaakt. Volgens de spreker volgt het wetsontwerp het Hof echter niet onverkort en beoogt het nieuwe maatregelen voor gegevensbewaring op te leggen, die uiteindelijk zouden kunnen leiden tot de feitelijke herinvoering van verplichtingen inzake de veralgemeende en ongedifferentieerde bewaring van gegevens.

De spreker betreurt dat het wetsontwerp beoogt talloze vormen van gegevensverwerking in te stellen en verregaand zou ingrijpen in het privéleven en in de bescherming van de persoonsgegevens. Het spectrum van de te verzamelen en te bezorgen gegevens is zeer breed, net zoals de doeleinden waarvoor dat zou gebeuren (facturatie, profilering, onderzoek naar inbreuken, vervolging van fraude enzovoort). Op grond van de door de GBA gemaakte overzichtstabel stelt de spreker vast dat gegevensverzameling de regel wordt, en geenszins de uitzondering zou zijn. Het wetsontwerp staat tevens een beperkt gebruik van versleuteling voor, waardoor dat iedereen *a priori* als verdacht zou worden beschouwd.

Om al de voormelde redenen zal de PVDA-PTB-fractie het wetsontwerp niet steunen.

Mevrouw Kathleen Verhelst (Open Vld) stelt op basis van de volumineuze adviezen en de uiteenlopende belangen vast dat het voorliggende wetsontwerp een zeer delicate evenwichtsoefening betreft. De grondrechten van de burgers moeten verdedigd worden, terwijl de standpunten van de verschillende adviesinstanties vaak uit elkaar liggen of soms tegengesteld lijken. Het moet dan ook een intellectuele uitdaging geweest zijn om tot dit wetsontwerp te komen.

De beroepsvereniging van operatoren verwijst in haar advies naar de nood aan een stabiel wettelijk kader. Creëert de regering deze keer een afdoende wettelijke basis voor de bewaring van gegevens, met de eerdere arresten van het Grondwettelijk Hof in het achterhoofd?

Een andere liberale bezorgdheid is de privacy: hoe minder gegevensbewaring, hoe beter. Mevrouw Verhelst

c'est. Mme Verhelst comprend toutefois que la liberté personnelle s'arrête là où commence celle des autres citoyens. C'est pourquoi le groupe Open Vld accepte que l'on conserve des données à caractère personnel dans certaines circonstances dans le cadre de la sécurité publique et nationale – et uniquement dans ce contexte. Comme cela est néanmoins perçu comme une intrusion dans la vie privée, ce qui est confirmé par la jurisprudence, l'intervenante demande que des garanties suffisantes soient mises en place pour protéger réellement ces données, et que l'on prévoie une réglementation très stricte des cas dans lesquels l'accès peut être accordé.

Enfin, Mme Verhelst aimerait savoir quelles sont aujourd'hui les conséquences sur le terrain de l'annulation de la législation précédente. Cela signifie-t-il qu'aucune donnée n'est plus disponible pour le moment?

M. Ben Segers (Vooruit) souligne que la législation sur la conservation des données était fondée sur une obligation de conservation indifférenciée: toutes les données de tous les utilisateurs étaient conservées, indépendamment de l'identité de ces personnes, de l'endroit où elles se trouvaient ou des moments où elles communiquaient. Cet élément est loin de faire l'unanimité et a déjà été remis en question à plusieurs reprises par la CJUE et la Cour constitutionnelle belge.

Récemment, la CJUE a prononcé l'arrêt "*The Commissioner of the Garda Síochána and Others*" du 5 avril 2022 (C-140/20), dans laquelle elle réaffirme que le droit de l'UE s'oppose à la conservation généralisée et indifférenciée des données de trafic et de localisation des communications électroniques aux fins de la lutte contre les infractions graves. La Cour préconise de prendre une mesure de conservation ciblée fondée sur un critère géographique, tel que notamment le taux moyen de criminalité dans une zone géographique, sans disposer nécessairement d'indices concrets portant sur la préparation ou la commission, dans les zones concernées, d'actes de criminalité grave. Elle ajoute qu'une telle mesure de conservation ciblée visant des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages, permet aux autorités compétentes de recueillir des informations sur la présence en ces lieux des personnes y utilisant un moyen de communication électronique, et d'en tirer, aux fins de la lutte contre la criminalité grave, des conclusions sur leur présence et leur activité dans ces lieux.

C'est le point de départ utilisé dans le projet de loi à l'examen. Le groupe Vooruit est très heureux qu'une base soit enfin recréée pour conserver les données de télécommunications dans certaines circonstances. En

begrijpt echter dat persoonlijke vrijheid limieten kent, met name daar waar de vrijheid van andere burgers begint. Daarom gaat de Open Vld-fractie ermee akkoord om in het kader van openbare en nationale veiligheid – en enkel in die context – onder bepaalde omstandigheden persoonsgegevens te bewaren. Omdat dit toch ervaren wordt als een intrusie in het privéleven, wat door de rechtspraak wordt bevestigd, vraagt de spreekster te waken over voldoende waarborgen om deze gegevens daadwerkelijk te beschermen, alsook de gevallen waarin men toegang kan krijgen, zeer strikt te reguleren.

Tot slot verneemt mevrouw Verhelst graag wat vandaag in het veld de gevolgen zijn van de vernietiging van de eerdere wetgeving. Betekent dit dat er momenteel geen data meer beschikbaar zijn?

De heer Ben Segers (Vooruit) stipt aan dat de dataretentiewetgeving gebaseerd was op een ongedifferentieerde bewaarplicht: alle gegevens van alle gebruikers werden bijgehouden, ongeacht wie deze personen waren, waar ze zich bevonden of op welke tijdstippen ze communiceerden. Dit element is niet zonder controverse en werd reeds meermaals ter discussie gesteld door het HvJ-EU en het Belgische Grondwettelijk Hof.

Onlangs werd het arrest "*The Commissioner of the Garda Síochána e.a.*" van 5 april 2022 (C-140/20) uitgesproken, waarin het HvJ-EU opnieuw bevestigt dat het Unierecht zich verzet tegen algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens over elektronische communicatie ter bestrijding van ernstige strafbare feiten. Het Hof pleit ervoor een gerichte bewaringsmaatregel te nemen op basis van een geografisch criterium, zoals het gemiddelde criminaliteitscijfer in een bepaalde geografische zone, zonder noodzakelijkerwijs concrete aanwijzingen te hebben dat er in die zones zware misdaden worden voorbereid of gepleegd. Het voegt daaraan toe dat de bevoegde autoriteiten met een dergelijke bewaringsmaatregel voor plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of voor strategische plekken zoals vliegvelden, stations, zeehavens of tolzones, informatie kunnen verkrijgen over de aanwezigheid op die plekken van personen die daar een elektronisch communicatiemiddel gebruiken, en daaruit met het oog op de bestrijding van zware criminaliteit conclusies kunnen trekken over hun aanwezigheid en activiteit aldaar.

Deze kapstok wordt in het voorliggende wetsontwerp gebruikt. De Vooruit-fractie is zeer tevreden dat er eindelijk opnieuw een basis wordt gecreëerd om telecommunicatiegegevens onder bepaalde omstandigheden te

effet, il s'agit d'un élément crucial dans de nombreuses enquêtes criminelles. L'intervenant est donc convaincu que le projet de loi à l'examen offre un bon équilibre entre la mise à disposition de données pour les enquêtes criminelles, d'une part, et la protection de la vie privée des citoyens, d'autre part.

M. Stefaan Van Hecke (Ecolo-Groen) souligne l'importance du projet de loi à l'examen, qui fait suite à l'annulation des deux lois précédentes. Celles-ci ont donné lieu à des débats animés. La question centrale est toujours l'équilibre très difficile à trouver entre la protection de la vie privée, d'une part, et la nécessité de conserver et d'utiliser certaines données essentielles à la lutte contre la criminalité grave, d'autre part.

Le droit au respect de la vie privée est crucial et très important. Mais il y a aussi d'autres droits et intérêts à prendre en compte.

M. Van Hecke évoque quelques cas récents de disparition de mineurs qui ont fait grand bruit et qui ont malheureusement connu une issue fatale. Naturellement, lorsqu'elles sont confrontées à un cas de disparition, la police et la justice veulent savoir le plus rapidement possible où se trouve la personne disparue et les auteurs potentiels. Contrairement à ce qui se passait il y a quelques décennies, elles peuvent faire appel aux nouvelles technologies (notamment les données télécoms, mais aussi les caméras ANPR, etc.) pour tenter de retracer le trajet des personnes impliquées.

Ces moyens technologiques qui permettent de progresser rapidement dans certains dossiers pénaux graves sont disponibles. Il existe par ailleurs une importante jurisprudence en matière de protection de la vie privée qui s'oppose à la conservation et à l'utilisation sans retenue des données de télécommunications. En l'espèce, il convient de trouver un équilibre. Ce n'est assurément pas une tâche aisée.

Si l'on entend utiliser les données de télécommunications dans le cadre d'enquêtes pénales, il faut néanmoins que ces données soient disponibles. Si une plainte arrive aujourd'hui au sujet d'un enlèvement éventuel qui a eu lieu quelques jours plus tôt, les mesures de *quick freeze* et de *future freeze* ne sont guère utiles. Certes, ces mesures permettent de savoir où se trouve actuellement un auteur potentiel, mais pas où il se trouvait au moment des faits. La conservation des données est donc un outil important pour les services de police et les services judiciaires, même s'il ne constitue pas la panacée à lui seul.

bewaren. Dit is namelijk een cruciaal element in heel wat strafonderzoeken. De spreker is er dan ook van overtuigd dat het voorliggende wetsontwerp een goed evenwicht biedt tussen het beschikbaar stellen van gegevens voor strafonderzoeken enerzijds en de bescherming van de privacy van de burger anderzijds.

De heer Stefaan Van Hecke (Ecolo-Groen) onderstreept het belang van het voorliggende wetsontwerp, dat het gevolg is van de vernietiging van de twee voorgaande wetten. Die gaven aanleiding tot hevige debatten. Centraal staat telkens weer de bijzonder moeilijke afweging tussen de bescherming van de privacy eensdeels en anderdeels de noodzaak om bepaalde gegevens die essentieel zijn voor het bestrijden van zware criminaliteit, te bewaren en te gebruiken.

Het recht op privacy is cruciaal en zwaarwichtig, maar er zijn ook andere rechten en belangen die in aanmerking moeten worden genomen.

De heer Van Hecke verwijst naar enkele recente ophefmakende verdwijningszaken waarin minderjarigen waren betrokken, en die helaas een fatale afloop kenden. Uiteraard willen politie en gerecht, wanneer zij met een verdwijningszaak worden geconfronteerd, zo snel mogelijk weten waar de verdwenen persoon en potentiële daders zich bevinden. Anders dan enkele decennia geleden, kunnen zij een beroep doen op nieuwe technologieën (met name telecomdata, maar ook ANPR-camera's enzovoort) om te trachten het traject van de betrokkenen te traceren.

Die technologische middelen om snel vooruitgang te boeken in bepaalde zware strafdossiers zijn voorhanden. Anderzijds is er een belangrijke privacyrechtspraak die zich verzet tegen ongebreidelde bewaring en gebruik van telecomdata. Daarin dient een evenwicht te worden gezocht. Dit is voorwaar geen eenvoudige opdracht.

Als men telecomgegevens wil gebruiken in strafonderzoeken, moeten die gegevens wel voorhanden zijn. Als er vandaag een klacht binnenloopt over een mogelijke ontvoering die enkele dagen eerder plaatsvond, zetten de *quick freeze* en de *future freeze* weinig zoden aan de dijk. Men kan wel nagaan waar een potentiële dader zich thans bevindt, maar niet waar hij op het ogenblik van de feiten was. Bewaring van gegevens is dus een belangrijk, zij het niet alleenzaligmakend, hulpmiddel voor politie- en gerechtelijke diensten.

La CJUE suggère, comme on le sait, de fixer un critère géographique sur la base duquel les données peuvent être conservées légalement. M. Van Hecke émet certaines réserves sur ce critère. Non seulement il engendre un haut degré de complexité, mais plus fondamentalement, il risque d'être source d'inégalités. L'utilisation du critère géographique permettra de délimiter des zones où les données de télécommunications peuvent être conservées et d'autres zones où ce n'est pas le cas. Il y a fort à parier que les grandes villes relèveront de la première catégorie et les zones rurales, de la seconde. Il n'est pas possible de prédire avec certitude où certains faits criminels se produiront. Si un enfant est enlevé dans une zone urbaine, la police et la justice seront probablement en mesure d'utiliser les données de télécommunications. Si le même drame se produit en Ardenne, ce ne sera peut-être pas le cas. Ne risque-t-on pas de créer une inégalité dans le droit des victimes et de leurs familles à une intervention rapide et adéquate de l'appareil de sécurité, en faisant appel aux technologies disponibles? Il ne fait aucun doute que tous les services, quelles que soient les possibilités de conservation des données, feront tout leur possible pour résoudre l'affaire, mais certains risquent de manquer d'outils technologiques pour progresser rapidement.

Bien que cela n'aille pas dans le sens de la jurisprudence, ni de la CJUE ni de la Cour constitutionnelle, l'intervenant préconise de centrer le débat sur la question de savoir qui peut utiliser quelles données dans quelles conditions et à quelles fins, plutôt que sur le principe de la conservation des données lui-même. Il ne fait aucun doute que l'accès aux données conservées doit être strictement encadré. Mais si les données ne sont pas conservées, elles ne peuvent pas être utilisées, quelle que soit la rigueur avec laquelle cet accès est réglementé.

Selon M. Van Hecke, le texte à l'examen constitue une tentative louable de trouver un équilibre, dans le cadre créé par la jurisprudence, entre le droit au respect de la vie privée, d'une part, et les droits des victimes et le droit à la sécurité, d'autre part. Cet équilibre, compte tenu du contexte, a été atteint au maximum. L'épaisseur du document parlementaire DOC 55 2572/001 atteste que le gouvernement n'a pris aucun risque. Le groupe Ecolo-Groen soutiendra le projet de loi. L'intervenant forme le vœu que la réglementation en projet résistera à un nouveau contrôle juridictionnel au regard des droits fondamentaux.

Het HvJ-EU reikt, zoals bekend, een geografisch criterium aan op basis waarvan gegevens op een geoorloofde wijze bewaard kunnen worden. De heer Van Hecke heeft bepaalde bedenkingen bij dit criterium. Niet alleen leidt het tot een hoge mate van complexiteit, het dreigt ook, meer fundamenteel, potentiële ongelijkheden te creëren. De aanwending van het geografisch criterium zal ertoe leiden dat gebieden zullen worden afgebakend waar telecomgegevens zullen kunnen worden bewaard, en andere gebieden waar dat niet het geval is. De kans is reëel dat de grote steden in de eerste categorie zullen vallen, en rurale streken in de laatste. Het valt niet met zekerheid te voorspellen waar bepaalde criminaliteit zich zal voordoen. Als er een kind wordt ontvoerd in een stedelijke regio, zullen politie en gerecht wellicht een beroep kunnen doen op telecomdata. Als hetzelfde gebeurt in de Ardennen, zal dat mogelijk niet het geval zijn. Dreigt niet het risico dat er een ongelijkheid wordt gecreëerd inzake het recht van slachtoffers en hun familieleden op een snel en adequaat optreden door het veiligheidsapparaat, mét gebruik van de voorhanden zijnde technologieën? Het leidt geen twijfel dat alle diensten, los van de mogelijkheden inzake gegevensbewaring, hun uiterste best zullen doen om de zaak op te lossen, maar sommige diensten zullen misschien de technologische hulpmiddelen ontberen om snel vooruitgang te kunnen boeken.

Hoewel dit niet de teneur is van de rechtspraak, noch van het HvJ-EU, noch van het Grondwettelijk Hof, pleit de spreker ervoor het debat toe te spitsen op de vraag wie welke gegevens mag gebruiken onder welke voorwaarden en voor welke doeleinden, veeleer dan op het principe van de gegevensbewaring zelf. Het staat buiten kijf dat de toegang tot de bewaarde gegevens uiterst stringent moet worden omkaderd. Maar als er geen gegevens bewaard worden, kunnen ze ook niet aangewend worden, hoe streng die toegang ook gereguleerd moge zijn.

De voorliggende tekst is volgens de heer Van Hecke een verdienstelijke poging om, binnen het door de rechtspraak geschapen kader, een evenwicht te vinden tussen het recht op privacy enerzijds, en anderzijds de rechten van slachtoffers en het recht op veiligheid. Dit evenwicht is, de context in acht genomen, maximaal bereikt. De omvang van het parlementair stuk DOC 55 2572/001 toont aan dat de regering niet over één nacht ijs is gegaan. De Ecolo-Groen-fractie zal het wetsontwerp steunen. De spreker drukt de hoop uit dat de ontworpen regeling een nieuwe rechterlijke toetsing aan de grondrechten zal doorstaan.

2. ***Réponses des vice-premiers ministres***

Mme Petra De Sutter, vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste, répondra aux questions des membres qui concernent essentiellement les modifications en projet de la loi du 13 juin 2005.

Mme De Wit a évoqué les éventuelles difficultés techniques et opérationnelles que rencontreraient les opérateurs pour conserver les données en fonction de la localisation, conformément à l'article 126/1 en projet (article 9 du projet de loi). Il est vrai que les opérateurs devront adapter leurs systèmes informatiques. C'est pourquoi le projet de loi prévoit une période transitoire de cinq ans pour l'introduction de la conservation ciblée sur une base géographique, pour ce qui concerne les zones spécifiques visées à l'article 126/1, § 3, alinéa 1er, 3° à 5°, en projet. Les opérateurs ont bien entendu été consultés à ce sujet.

L'article 121/8, § 1er, en projet, de la loi du 13 juin 2005 (article 4 du projet de loi) traite des mesures contre la fraude et l'utilisation malveillante des réseaux. L'article se fonde sur l'actuel article 107/2 de la loi susvisée, qui transpose à son tour l'article 40, paragraphe 1er, de la directive (UE) 2018/1972. L'article en projet prévoit une obligation générale pour les opérateurs de prendre les mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés. Un exemple d'une telle mesure (préventive) est l'utilisation de filtres "anti-spam" permettant de notifier au destinataire le caractère potentiellement frauduleux ou malveillant de certaines communications entrantes. De manière similaire aux dispositions de l'article 107/2 de la loi du 13 juin 2005 relatives à la sécurité des réseaux, la disposition en projet fait des opérateurs les premiers responsables de l'appréciation des mesures à prendre. En cas de défaillance de l'opérateur, l'IBPT dispose du pouvoir de lui donner des instructions contraignantes. En outre, le Roi est habilité à préciser les mesures à prendre par les opérateurs par voie réglementaire. Le système est donc suffisamment flexible, et c'est bien nécessaire, compte tenu de la diversité des types de fraude et de leur caractère évolutif.

Afin d'apporter une plus grande sécurité juridique aux opérateurs lorsqu'ils sont confrontés à des cas graves de fraude ou d'utilisation malveillante, le second paragraphe de l'article 121/8 en projet énonce certains exemples de mesures pouvant être prises tant au niveau du réseau

2. ***Antwoorden van de vice-eersteministers***

Mevrouw Petra De Sutter, vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post, zal antwoorden op de vragen van de leden die het nauwst aansluiten bij de ontworpen wijzigingen van de wet van 13 juni 2005.

Mevrouw De Wit verwees naar de mogelijke technische en operationele moeilijkheden voor operatoren om gegevens op basis van locatie te bewaren overeenkomstig het ontworpen artikel 126/1 (artikel 9 van het wetsontwerp). Het klopt dat de operatoren hun IT-systemen zullen moeten aanpassen. Om die reden voorziet het wetsontwerp in een overgangsperiode van vijf jaar voor de invoering van de gerichte bewaring op geografische basis, wat de specifieke zones in het ontworpen artikel 126/1, § 3, eerste lid, 3° tot 5°, betreft. Uiteraard werden de operatoren hieromtrent geconsulteerd.

Het ontworpen artikel 121/8, § 1, van de wet van 13 juni 2005 (artikel 4 van het wetsontwerp) handelt over maatregelen tegen fraude en kwaadwillig gebruik op de netwerken. Het artikel is gebaseerd op het bestaande artikel 107/2 van voornoemde wet, dat op zijn beurt een omzetting is van artikel 40, eerste lid, van Richtlijn (EU) 2018/1972. Het ontworpen artikel voert een algemene verplichting in voor de operatoren om de gepaste, evenredige, preventieve en curatieve maatregelen te nemen, rekening houdend met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en te voorkomen dat de eindgebruikers nadeel ondervinden of lastiggevallen worden. Een voorbeeld van zo'n (preventieve) maatregel is het gebruik van antispamfilters die het mogelijk maken de ontvanger kennis te geven van de potentieel frauduleuze of kwaadwillige aard van sommige binnenkomende berichten. Op gelijkaardige wijze als de bepalingen van artikel 107/2 van de wet van 13 juni 2005 inzake netwerkveiligheid, maakt de ontworpen bepaling van de operatoren de eerste verantwoordelijken om te oordelen over de te nemen maatregelen. In geval van tekortkoming van de operator beschikt het BIPT over het recht hem dwingende instructies op te leggen. Bovendien is de Koning gemachtigd de door de operatoren te nemen maatregelen reglementair te preciseren. Het systeem is dus voldoende flexibel, wat ook nodig is, gezien de veelheid aan fraudevormen en het evolutieve karakter daarvan.

Om de operatoren meer rechtszekerheid te geven wanneer ze worden geconfronteerd met ernstige gevallen van fraude of kwaadwillig gebruik, lijst de tweede paragraaf van het ontworpen artikel 121/8 bepaalde voorbeeldmaatregelen op, zowel op netwerkniveau

(blocage des numéros, de services, des URL, de noms de domaine, d'adresses IP ou de tout autre élément d'identification de la communication électronique) qu'au niveau de l'utilisateur final (comme la désactivation complète ou partielle de certains services ou équipements).

Bien sûr, le gouvernement croit et espère que le texte à l'examen est compatible avec le droit européen. Toutefois, la vice-première ministre ne souhaite pas préjuger des futures décisions éventuelles de la CJUE sur cette question.

En ce qui concerne l'avis de l'APD sur la conservation des communications sortantes – qui est obligatoire, mais pas, en règle générale, pour les destinataires –, la vice-première ministre note qu'il est dans l'intérêt des victimes de fraude que les données sur les appels frauduleux soient conservées. Avec ces informations, les victimes peuvent alors s'adresser au service de médiation pour les télécommunications pour obtenir l'identité de l'appelant, qu'elles peuvent ensuite utiliser pour déposer plainte auprès de la police. Le projet de loi prévoit donc la conservation des données des appels entrants pendant douze mois, afin que le service de médiation puisse remplir sa mission.

En ce qui concerne les autres données relatives à la lutte contre la fraude, ce sont en premier lieu les opérateurs qui sont à la manœuvre, comme indiqué ci-dessus. Le projet de loi préconise une approche flexible, afin que les opérateurs puissent apporter une réponse appropriée aux formes de fraude en constante évolution.

M. Gilissen a demandé si les opérateurs, en dérogation à la version en projet de l'article 122, peuvent prendre connaissance du contenu de la communication, et indique qu'il faut faire preuve de la plus grande prudence dans ce cas. La vice-première ministre répond que cela est réglé dans la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques. Elle convient que cette possibilité doit être utilisée avec prudence.

M. Gilissen a ensuite fait référence à la possibilité, inscrite dans l'article 122, § 4, alinéa 2, en projet (article 5, 4°, du projet de loi), pour les opérateurs de conserver et de traiter d'autres données jugées nécessaires pour lutter contre la fraude ou l'utilisation malveillante. Le député considère que cette disposition est définie de manière très large. La vice-première ministre souligne que le projet de règlement ePrivacy 2021 offre une certaine flexibilité à cet égard. Toutefois, il ne s'agit pas d'un chèque en blanc. Par exemple, la nécessité est un critère important.

(blokkering van nummers, diensten, URL's, domeinnamen, IP-adressen of elk ander element ter identificatie van de elektronische communicatie) als op het niveau van de eindgebruiker (zoals het volledig of gedeeltelijk deactiveren van bepaalde diensten of apparatuur).

Vanzelfsprekend meent en hoopt de regering dat de voorliggende tekst compatibel is met het Europees recht. De vice-eersteminister wil evenwel niet vooruitlopen op eventuele toekomstige beslissingen ter zake van het HvJ-EU.

Wat het advies van de GBA inzake de bewaring van uitgaande communicatie betreft – die verplicht is, maar in de regel niet voor geadresseerden – merkt de vice-eersteminister op dat het in het belang is van de slachtoffers van fraude dat de gegevens omtrent frauduleuze oproepen bewaard worden. Daarmee kunnen de slachtoffers dan naar de Ombudsdienst voor Telecommunicatie stappen, teneinde de identiteit van de beller te verkrijgen, waarmee ze dan een klacht kunnen indienen bij de politie. Het wetsontwerp voorziet dus in het bewaren van gegevens van inkomende oproepen voor twaalf maanden, zodat de Ombudsdienst zijn opdracht kan vervullen.

Met betrekking tot andere gegevens in de strijd tegen fraude zijn in eerste instantie de operatoren aan zet, zoals hierboven aangegeven. Het wetsontwerp staat een flexibele aanpak voor, zodat de operatoren een passend antwoord kunnen bieden op de steeds veranderende vormen van fraude.

De heer Gilissen vroeg of operatoren, in afwijking van de ontworpen versie van artikel 122, kennis kunnen nemen van de inhoud van de communicatie, en gaf aan dat hierbij desgevallend de grootste voorzichtigheid is geboden. De vice-eersteminister antwoordt dat een en ander is geregeld in de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie. Zij is het ermee eens dat omzichtig moet worden omgesprongen met deze mogelijkheid.

De heer Gilissen verwijst voorts naar de mogelijkheid, vervat in het ontworpen § 4, tweede lid, van artikel 122 (artikel 5, 4° van het wetsontwerp), voor operatoren om andere gegevens te bewaren en te verwerken die voor de bestrijding van fraude of kwaadwillig gebruik nodig worden geacht. Het lid acht deze bepaling erg breed omschreven. De vice-eersteminister wijst erop dat het voorstel van verordening ePrivacy 2021 ter zake enige flexibiliteit biedt. Dit is echter geen blanco cheque. Zo is de noodzakelijkheid een belangrijk criterium. Enkel

Seules les données qui sont nécessaires pour atteindre les objectifs susmentionnés pourront être conservées.

M. Gilissen a également noté que le texte à l'examen obligera les opérateurs à mettre en place de nouvelles bases de données complexes et a souhaité savoir comment éviter que les coûts qui en découlent ne soient répercutés sur les consommateurs. La vice-première ministre ne nie pas que le projet de loi représente un défi pour les opérateurs, mais souligne qu'ils ont pu partager leurs points de vue et leurs préoccupations dans le cadre d'une consultation publique qui s'est déroulée du 7 mai au 4 juin 2021. Leurs commentaires ont bel et bien été pris en compte. Les ajustements que les opérateurs doivent effectuer ne vont pas au-delà de ce qui est nécessaire. On a également prévu une période transitoire d'un an pour les nouvelles données et de cinq ans pour la conservation ciblée sur une base géographique. Cela permettra aux opérateurs d'étaler les coûts dans le temps. Il va sans dire que ces coûts ne doivent pas être supportés par les consommateurs.

La vice-première ministre et l'IBPT suivent de près la situation dans les autres États membres de l'UE. Jusqu'à présent, seuls la France et le Danemark ont adapté leur législation en fonction de la jurisprudence européenne.

M. Boukili a posé plusieurs questions sur la conservation des données prévue dans les articles 122, 123 et 126 en projet de la loi du 13 juin 2005. La conservation des données par les opérateurs pour leurs propres besoins n'est possible que dans des cas bien définis, à savoir dans le cadre de la lutte contre la fraude et de l'utilisation malveillante du réseau, ainsi que pour la facturation, le marketing et la sécurité des réseaux. Dans ces trois derniers cas, il s'agit d'une conservation des données généralisée et non obligatoire, qui n'a pas été remise en cause par la jurisprudence européenne ni par l'avis de l'APD.

En ce qui concerne la conservation obligatoire de certaines données dans le cadre de la lutte contre la fraude et l'utilisation malveillante du réseau, la vice-première ministre indique que, contrairement à ce que prétend l'APD dans son avis, il n'existe pas de moyen moins intrusif que la conservation de certaines données de trafic et de localisation. En effet, la fraude et l'utilisation malveillante ne peuvent être étudiées que sur la base de données historiques. Par exemple, sans données historiques, il ne serait pas possible pour une victime de prouver l'existence d'un harcèlement téléphonique, une infraction qui s'étale intrinsèquement dans le temps. Les seules données qui doivent être conservées sont

gegevens die nodig zijn om voornoemde doeleinden te bereiken, zullen bewaard kunnen worden.

De heer Gilissen merkte daarnaast op dat de voorliggende tekst operatoren ertoe zal nopen nieuwe, complexe databanken op te richten; hij wilde weten hoe voorkomen kan worden dat de daarmee gepaard gaande kosten afgewenteld zullen worden op de consument. De vice-eersteminister ontkent niet dat het wetsontwerp een uitdaging vormt voor de operatoren, maar wijst erop dat zij hun standpunten en bekommernissen hebben kunnen delen in het kader van een openbare raadpleging die werd gehouden van 7 mei tot 4 juni 2021. Er werd wel degelijk rekening gehouden met hun opmerkingen. De aanpassingen die de operatoren moeten doorvoeren, gaan niet verder dan wat nodig is. Er werd ook in een overgangsperiode voorzien van één jaar voor nieuwe gegevens en van vijf jaar voor de gerichte bewaring op geografische basis. Dat zal de operatoren in staat stellen de kosten te spreiden in de tijd. Het spreekt voor zich dat deze kosten niet bij de consumenten mogen terechtkomen.

De vice-eersteminister en het BIPT volgen de situatie in andere EU-lidstaten op de voet. Vooralsnog hebben enkel Frankrijk en Denemarken hun wetgeving aangepast aan de Europese rechtspraak.

De heer Boukili stelde diverse vragen omtrent de gegevensbewaring bepaald in de ontworpen versies van de artikelen 122, 123 en 126 van de wet van 13 juni 2005. De bewaring van gegevens door operatoren voor eigen doeleinden kan enkel in welomschreven gevallen, met name in de strijd tegen fraude en kwaadwillig gebruik van het netwerk, evenals voor facturatie, marketing en netwerkbeveiliging. In die laatste drie gevallen gaat het om een veralgemeende, niet-verplichte gegevensbewaring, die niet ter discussie is gesteld in de Europese rechtspraak noch in het advies van de GBA.

Inzake de verplichte bewaring van bepaalde gegevens in de strijd tegen fraude en kwaadwillig gebruik van het netwerk, geeft de vice-eersteminister aan dat, anders dan de GBA beweert in haar advies, er geen minder indringend middel is dan de bewaring van bepaalde verkeers- en lokalisatiegegevens. Fraude en kwaadwillig gebruik kunnen immers enkel aan de hand van historische gegevens worden onderzocht. Zonder historische gegevens zou het voor een slachtoffer bijvoorbeeld niet mogelijk zijn het bestaan van pesterijen via de telefoon, een strafbaar feit dat intrinsiek in de tijd is gespreid, te bewijzen. De enige gegevens waarvan de bewaring verplicht is, zijn die welke reeds door de operatoren

celles déjà traitées par les opérateurs à travers leurs systèmes de gestion internes (à savoir les systèmes de facturation).

En ce qui concerne l'article 126, en projet, de la loi du 13 juin 2005 (article 8 du projet de loi), la vice-première ministre indique que la CJUE n'a pas interdit la conservation généralisée et indifférenciée des données d'identification. Au contraire, la Cour a jugé dans son arrêt *Ministerio Fiscal (*C-207/16) qu'il convient de considérer ce type de données comme portant moins atteinte à la vie privée que d'autres métadonnées.

M. Boukili estime que la liste des données conservées va plus loin que ce que la CJUE avait considéré comme admissible. Il convient toutefois d'observer que la Cour n'agit pas en tant que législateur mais qu'elle donne une réponse aux questions préjudicielles qui lui sont adressées. L'arrêt est dès lors loin de couvrir tous les cas envisageables.

Le membre fait en outre observer que le texte à l'examen contraindra *de facto* les fournisseurs de services par contournement comme Skype, WhatsApp et FaceTime à conserver l'ensemble des données sur la totalité du territoire. Ces fournisseurs seront effectivement soumis au projet de loi à l'examen. Ils ne devront cependant conserver que les données qu'ils auront générées ou traitées. Il va de soi qu'ils ne devront pas conserver des données qu'ils ne possèdent pas. Par ailleurs, les services par contournement peuvent certes localiser des communications au travers des adresses IP, mais de façon moins précise que les opérateurs.

M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice et de la Mer du Nord, indique qu'il existe en substance trois modèles pour la mise en balance de la sécurité et de la vie privée. La Russie et la Chine sont des États contrôleurs: ce ne sont pas les opérateurs mais le gouvernement qui conserve toutes sortes de données et les entreprises privées sont obligées de partager les informations dont elles disposent avec les autorités.

Ce modèle n'est nullement comparable à celui en vigueur en Europe, où les opérateurs sont tenus de conserver certaines données. Ils ne peuvent être contraints de les partager avec les services de sécurité que sur décision de justice.

Il y a également le "système du filet jeté à la mer" américain: une conservation des données généralisée et systématique pour des raisons de sécurité. Ce système

worden verwerkt via hun interne beheerssystemen (met name facturatiesystemen).

Aangaande het ontworpen artikel 126 van de wet van 13 juni 2005 (artikel 8 van het wetsontwerp) stelt de vice-eersteminister dat het HvJ-EU de veralgemeende en ongedifferentieerde bewaring van identificatiegegevens niet heeft verboden. Integendeel, in zijn arrest *Ministerio Fiscal (*C-207/16) heeft het Hof geoordeeld dat deze gegevens beschouwd moeten worden als minder indringend ten aanzien van het privéleven dan andere metagegevens.

De heer Boukili meent dat de lijst van de bewaarde gegevens verder gaat dan wat het HvJ-EU toelaatbaar achtte. Nochtans moet opgemerkt worden dat het Hof niet optreedt als wetgever, maar een antwoord biedt op de prejudiciële vragen die hem worden voorgelegd. Het arrest dekt dus allerminst alle denkbare gevallen.

Hetzelfde lid betoogde dat de voorliggende tekst aanbieders van *over-the-top*-diensten (OTT-diensten), zoals Skype, WhatsApp en FaceTime, er *de facto* toe zal verplichten alle gegevens over het gehele grondgebied te bewaren. Het klopt dat deze aanbieders onder het wetsontwerp vallen. Zij moeten echter enkel de door hen gegenereerde of verwerkte gegevens bewaren. Gegevens die ze niet hebben, moeten ze niet bewaren. Overigens kunnen OTT-diensten communicaties wel degelijk lokaliseren, met name aan de hand van IP-adressen, zij het op een minder precieze manier dan operatoren.

De heer Vincent Van Quickenborne, vice-eersteminister en minister van Justitie en Noordzee, wijst erop dat wat de afweging tussen veiligheid en privacy betreft, er *grosso modo* drie verschillende modellen bestaan. In Rusland en China kent men een controlestaat. Niet de operatoren, maar de overheid houdt allerlei gegevens bij; particuliere bedrijven worden verplicht informatie waarover ze beschikken te delen met de overheid.

Dat model is hier geenszins aan de orde. In Europa worden operatoren verplicht bepaalde gegevens te bewaren. Het is pas na een rechterlijke tussenkomst dat ze kunnen worden gedwongen die te delen met de veiligheidsdiensten.

Dan is er nog het Amerikaanse "sleepnetsysteem": een veralgemeende en systematische gegevensbewaring ten behoeve van de veiligheid. Dat is niet zonder risico,

n'est pas sans risque, certainement dans l'hypothèse où un régime moins démocratique venait à prendre le pouvoir.

Le gouvernement cherche à atteindre un équilibre entre la sécurité et le respect de la vie privée. Les autorités publiques belges ont déjà été rappelées deux fois à l'ordre par la Cour constitutionnelle. La troisième tentative sera-t-elle la bonne? Le vice-premier ministre se montre en tout cas optimiste. Il y a de grandes chances que la nouvelle législation soit de nouveau contestée par la Cour constitutionnelle. Le résultat de ce type de procédure est toujours incertain, mais le vice-premier ministre est convaincu que la réglementation en projet repose sur des bases plus solides que les précédentes.

Sur la base de la jurisprudence constante de la CJUE, la conservation généralisée et indifférenciée des données est contraire au respect de la vie privée. Après la première annulation de la législation relative à la conservation des données, on a essayé d'y remédier en différenciant l'accès aux données selon la nature des faits (infractions terroristes: douze mois; criminalité organisée: neuf mois; autre criminalité soumise à une peine d'emprisonnement d'un an ou plus: six mois). Cette adaptation n'a pas convaincu la Cour, qui a jugé non seulement qu'il convient de prévoir un cadre clair pour l'accès aux données, mais aussi que la conservation ne peut pas être généralisée et indifférenciée. Le projet de loi à l'examen donne suite à ces observations de la Cour.

Dans son arrêt le plus récent sur cette matière, *The Commissioner of An Garda Síochána et d'autres* (C-140/20), la CJUE souligne que "les autorités nationales compétentes peuvent prendre […] une mesure de conservation ciblée fondée sur un critère géographique, tel que notamment le taux moyen de criminalité dans une zone géographique, sans qu'elles disposent nécessairement d'indices concrets portant sur la préparation ou la commission, dans les zones concernées, d'actes de criminalité grave" (paragraphe 80). La législation en projet se conforme en tout point à cette observation. Il va de soi que l'on ne peut pas affirmer avec certitude que cette nouvelle législation passera le test de la jurisprudence européenne, mais il est clair que le texte à l'examen s'écarte de la philosophie de la conservation généralisée et indifférenciée en faveur d'un système à plusieurs niveaux.

Comme déjà expliqué, une conservation des métadonnées de communication sera organisé et la durée de cette conservation sera déterminée, par arrondissement judiciaire, sur la base d'un pourcentage statistique d'actes criminels graves fixé dans la loi. Dès que trois infractions graves par tranche de mille habitants sont commises en moyenne par an dans un arrondissement judiciaire, des

zeker niet wanneer er ooit een minder democratisch regime aan de macht zou komen.

De regering streeft een evenwicht na tussen veiligheid en privacy. De Belgische overheid is al tweemaal teruggefloten door het Grondwettelijk Hof. Derde keer, goede keer? De vice-eersteminister toont zich alvast optimistisch. De kans is groot dat de nieuwe wetgeving opnieuw zal aangevochten worden voor het Grondwettelijk Hof. De uitkomst van zulke procedures is altijd onzeker, maar de vice-eersteminister is ervan overtuigd dat de ontworpen regeling een stevigere basis heeft dan haar voorgangers.

Volgens de vaste rechtspraak van het HvJ-EU is het algemeen en ongedifferentieerd bewaren van gegevens in strijd met de privacy. Na de eerste vernietiging van de dataretentiewetgeving heeft men getracht hieraan een mouw te passen door de toegang tot de gegevens te differentiëren naargelang van de aard van de feiten (terroristische misdrijven: twaalf maanden; georganiseerde criminaliteit: negen maanden; andere criminaliteit, onderworpen aan een gevangenisstraf van één jaar of meer: zes maanden). Dit heeft niet gewerkt; het Hof heeft geoordeeld dat niet enkel de toegang tot de gegevens goed omkaderd moet worden, maar ook dat de bewaring niet algemeen en ongedifferentieerd mag zijn. Het voorliggende wetsontwerp komt daaraan tegemoet.

In zijn jongste arrest over deze materie, *The Commissioner of the Garda Síochána e.a.* (C-140/20), benadrukt het HvJ-EU dat "de bevoegde nationale autoriteiten […] een gerichte bewaringsmaatregel kunnen nemen op basis van een geografisch criterium, zoals met name het gemiddelde criminaliteitscijfer in een geografische zone, zonder noodzakelijkerwijs concrete aanwijzingen te hebben dat er in die zones zware misdaden worden voorbereid of gepleegd" (paragraaf 80). De ontworpen regeling sluit hierbij naadloos aan. Uiteraard kan niet met zekerheid gesteld worden dat de nieuwe regeling de toets van de Europese rechtspraak zal doorstaan, maar het is duidelijk dat met de voorliggende tekst afgestapt wordt van de filosofie van de algemene en ongedifferentieerde bewaring ten voordele van een gelaagd systeem.

Zoals reeds uitgelegd, wordt er een bewaring georganiseerd van de metadata van communicatie, en de duur ervan, per gerechtelijk arrondissement, aan de hand van een bij de wet vastgesteld statistisch percentage van zware criminele feiten. Vanaf het moment dat er gemiddeld drie zware strafbare feiten per 1 000 inwoners per jaar in een gerechtelijk arrondissement gepleegd

données sont conservées dans cet arrondissement. Pour Anvers, Bruxelles et Charleroi, ce seuil signifie que ces trois dernières années, respectivement 5 609, 3 655 et 1 752 infractions graves doivent avoir été commises en moyenne par an. C'est un chiffre considérable. Il n'est pas du tout impensable que ce seuil ne sera pas atteint dans certains arrondissements. Le gouvernement ne prend donc pas ce sujet à la légère.

Le délai de conservation sera déterminé par arrondissement en toute transparence au moyen de critères objectifs. Le COC jouera un rôle important à cet égard.

Plusieurs membres ont demandé si le gouvernement avait pris à cœur les avis relatifs à l'avant-projet, en particulier l'avis de l'APD. Le vice-premier ministre leur répond par l'affirmative. Le texte de l'avant-projet de loi était très différent de celui qui a été finalement déposé à Chambre. C'est ainsi par exemple que le rapport d'évaluation annuel à la Chambre des représentants, visé à l'article 126/1, § 6, de la loi du 13 juin 2005 en projet (article 9 du projet de loi), a été inclus sur recommandation de l'APD.

Le vice-premier ministre aborde ensuite la question de l'encryptage. Cet élément a effectivement été supprimé de l'avant-projet de loi, notamment à la suite de l'avis de l'APD. Il s'agit d'une matière extrêmement complexe. À la demande du juge d'instruction, les opérateurs qui proposent le chiffrement de bout en bout doivent fournir des métadonnées. Ce n'est pas sujet à discussion, contrairement à l'interception de la communication elle-même. D'aucuns prétendent qu'il est aujourd'hui technologiquement impossible de permettre l'interception sans compromettre la confidentialité. Le gouvernement a donc jugé opportun d'omettre délibérément la disposition en question dans le projet de loi à l'examen. Cela ne signifie aucunement que le gouvernement évite toute discussion à ce sujet. Il faut savoir que l'alternative à l'interception d'informations cryptées implique le recours à des méthodes particulièrement intrusives, telles que l'utilisation du logiciel Pegasus. Est-ce cela que nous voulons? Il est un fait que certaines personnes utilisent aujourd'hui délibérément des messages cryptés pour commettre des actes criminels graves. D'autre part, il faut éviter que la confidentialité du système soit complètement compromise. Le vice-premier ministre n'est pas favorable aux "portes dérobées" (*backdoors*), mais il reconnaît la nécessité de trouver des méthodes pour traiter ces informations de manière intelligente et avec les garanties nécessaires. Le vice-premier ministre voudrait que la Belgique prenne l'initiative au niveau européen pour trouver une solution dans ce dossier. Il s'agit certes d'un défi technologique à l'échelle mondiale,

worden, worden er in dat arrondissement data bewaard. Voor Antwerpen, Brussel en Charleroi impliceert deze drempel dat er zich in de afgelopen drie jaar gemiddeld respectievelijk 5 609, 3 655 en 1 752 zware strafbare feiten per jaar moeten hebben voorgedaan. Dat is aanzienlijk; het is allerminst ondenkbaar dat voornoemde drempel in bepaalde arrondissementen niet zal worden gehaald. De regering gaat hier dus geenszins licht over.

De bepaling van de bewaringstermijn voor een welbepaald arrondissement zal gebeuren aan de hand van objectieve criteria en in alle transparantie. Er zal hierin een belangrijke rol weggelegd zijn voor het COC.

Verschillende leden vroegen of de regering de adviezen inzake het voorontwerp, met name van de GBA, ter harte heeft genomen. De vice-eersteminister antwoordt bevestigend. De tekst van het voorontwerp van wet verschilt in aanzienlijke mate van de tekst die is ingediend bij de Kamer. Zo werd het in het ontworpen artikel 126/1, § 6, van de wet van 13 juni 2005 (artikel 9 van het wetsontwerp) bedoelde jaarlijkse evaluatieverslag aan de Kamer van volksvertegenwoordigers opgenomen op aanbeveling van de GBA.

Vervolgens snijdt de vice-eersteminister het onderwerp van de encryptie aan. Dit element werd inderdaad uit het voorontwerp van wet gelicht, onder meer naar aanleiding van het advies van de GBA. Het betreft een uiterst complex vraagstuk. Op vordering van de onderzoeksrechter moeten exploitanten die *end-to-end* encryptie aanbieden, metadata aanleveren. Daarover bestaat geen discussie, in tegenstelling tot de onderschepping van de communicatie zelf. Sommigen beweren dat het vandaag technologisch onmogelijk is onderschepping toe te laten zonder de vertrouwelijkheid op de helling te zetten. De regering achtte het daarom opportuun de bewuste bepaling achterwege te laten in het voorliggende wetsontwerp. Dit betekent evenwel geenszins dat zij de discussie hieromtrent uit de weg gaat. Men moet beseffen dat het alternatief voor het onderscheppen van geëncrypteerde informatie impliceert dat men zijn toevlucht moet nemen tot bijzonder indringende methodes, zoals de *Pegasus*-software. Is het dat wat we willen? Het is een feit dat bepaalde personen vandaag de dag bewust gebruikmaken van geëncrypteerde boodschappen om zware criminaliteit te plegen. Anderzijds moet worden voorkomen dat de vertrouwelijkheid van het systeem volledig in het gedrang komt. De vice-eersteminister is geen voorstander van een *backdoor*; maar er moeten methodes te vinden zijn om slim, met de nodige waarborgen, om te gaan met die informatie. De vice-eersteminister pleit ervoor dat België op Europees vlak het voortouw zou nemen om in dit dossier een oplossing te vinden. Het gaat om een

mais notre pays peut heureusement compter sur des experts de classe mondiale.

À la question de Mme De Wit concernant les adaptations proposées de la loi du 5 août 1992 sur la fonction de police, le vice-premier ministre répond que la Cour constitutionnelle a annulé l'ensemble de la législation relative à la conservation des données de 2016, y compris les dispositions qui habilitaient la Cellule des personnes disparues de la Police fédérale à requérir des données concernant les communications électroniques de personnes disparues. Le gouvernement a dès lors décidé de rétablir les dispositions en question dans la loi sur la fonction de police au lieu de les rétablir dans la loi sur les télécommunications. Ni le Conseil d'État, ni l'APD, ni le COC n'ont émis de critiques envers la disposition en question, qui figure à l'article 22 du projet de loi. Il est exact qu'un officier de police judiciaire peut demander directement les informations auprès des opérateurs, mais les garanties nécessaires ont bel et bien été prévues. L'officier en question devra ainsi transmettre immédiatement la demande au COC qui procédera à des contrôles *ex post.*

M. Gilissen a évoqué la possibilité d'une conservation ciblée sur la base de facteurs objectifs, comme certaines catégories de personnes. Il estime qu'il convient de préciser ce point. Le vice-premier ministre confirme que la Cour de justice de l'Union européenne ne rejette pas cette possibilité, mais que le gouvernement belge ne l'a délibérément pas utilisée, jugeant qu'elle serait trop stigmatisante. Quel signal enverrait-on en tant qu'autorité si, par exemple, les données de toutes les personnes ayant un casier judiciaire étaient conservées? Le vice-premier ministre considère que les critères choisis par le gouvernement sont plus appropriés afin de garantir la sécurité. Il souligne également que le *quick freeze* et le *future freeze* sont possibles dans des dossiers spécifiques.

S'agissant de la question de M. Gilissen concernant les durées de conservation, qui selon lui peuvent être prolongées à chaque fois pour une même période, et donc de manière quasi illimitée, le vice-premier ministre indique que la durée d'un ordre de conservation peut être prolongée dans un dossier spécifique, mais que les durées générales de conservation (six, neuf ou douze mois) constituent la norme et ne peuvent pas être prolongées automatiquement. Il rappelle également que la durée de conservation dans un arrondissement donné est fixée tous les ans.

Le même intervenant a également demandé si la fourniture de certaines données provenant de services cryptés n'était pas contraire au RGPD. L'accès au contenu des communications est actuellement défini

mondiale technologische uitdaging. Gelukkig kan ons land bogen op experten van wereldformaat.

Op de vraag van mevrouw De Wit aangaande de ontworpen aanpassingen van de wet van 5 augustus 1992 op het politieambt, antwoordt de vice-eersteminister dat het Grondwettelijk Hof in 2021 de gehele dataretentiewetgeving uit 2016 vernietigde, inclusief de bepalingen die de Cel Vermiste Personen van de federale politie de bevoegdheid gaven om gegevens met betrekking tot de elektronische communicatie van vermiste personen op te vorderen. De regering heeft daarop beslist de bewuste bepalingen te herstellen in de wet op het politieambt, in plaats van in de telecomwet. Noch de Raad van State, noch de GBA, noch het COC heeft kritiek geleverd op de bewuste bepaling, vervat in artikel 22 van het wetsontwerp. Het klopt dat een officier van gerechtelijke politie de informatie rechtstreeks bij de operatoren kan opvragen, maar er werd wel degelijk voorzien in de nodige waarborgen; zo moet die officier het verzoek onmiddellijk doorsturen naar het COC, dat dan *ex post* controles zal uitvoeren.

De heer Gilissen verwees naar de mogelijkheid van een gerichte bewaring op basis van objectieve factoren, waaronder bepaalde categorieën van personen. Volgens hem dient dit duidelijker te worden omschreven. De vice-eersteminister bevestigt dat het HvJ-EU die mogelijkheid openlaat, maar dat de Belgische regering hiervan bewust geen gebruik heeft gemaakt, oordelend dat dit te stigmatiserend zou zijn. Welk signaal geeft men als overheid als men bijvoorbeeld de gegevens zou bewaren van alle mensen met een strafblad? De door de regering gekozen criteria zijn volgens de vice-eersteminister geschikter om de veiligheid te garanderen. Hij wijst er tevens op dat in specifieke dossiers de *quick freeze* en de *future freeze* ter beschikking staan.

Aangaande de vraag van de heer Gilissen inzake de bewaringstermijnen, die volgens hem telkens voor eenzelfde periode, en dus quasi onbeperkt, kunnen worden verlengd, geeft de vice-eersteminister aan dat de termijn van een bevel tot bewaring in een specifiek dossier kan worden verlengd, maar dat de algemene bewaringstermijnen (zes, negen of twaalf maanden) de norm uitmaken en niet automatisch kunnen worden verlengd. Hij herinnert er ook aan dat de bepaling van de bewaringstermijn in een gegeven arrondissement een jaarlijks weerkerende oefening is.

Hetzelfde lid vroeg ook of het verstrekken van bepaalde gegevens uit geëncrypteerde diensten niet in strijd is met de AVG. De toegang tot de inhoud van communicatie wordt vandaag bepaald door artikel 90*ter* van het

par l'article 90*ter* du Code d'instruction criminelle, sur la base de l'article 21 du Code judiciaire. La téléphonie classique est d'ailleurs aussi protégée au moyen d'une sécurité physique et d'un cryptage. Son interception constitue une mesure nécessaire et proportionnelle, pour autant qu'il existe des garanties suffisantes.

M. Gilissen s'est inquiété de ce que la réglementation en projet puisse porter atteinte au secret professionnel des médecins et des avocats, opérant à cet égard une distinction entre les communications entrantes et sortantes. AVOCATS.BE s'est également montré critique en la matière. Le vice-premier ministre fait d'abord observer que l'article 88*bis*, § 3, en projet, du Code d'instruction criminelle n'opère pas la distinction précitée. Les services de renseignement peuvent requérir des opérateurs qu'ils conservent les données de catégories professionnelles protégées, mais ne peuvent demander et traiter ces données qu'en respectant des conditions strictes. Le secret professionnel ne peut être levé qu'à des conditions très strictes. Une dispense générale de conservation des données pour l'ensemble des communications des catégories professionnelles protégées n'est toutefois pas autorisée. En effet, les médecins et les avocats peuvent être victimes d'actes de criminalité grave ou peuvent s'y livrer.

Le vice-premier ministre remercie Mme Gilson pour son soutien au texte à l'examen. Il est exact que la Belgique innove en proposant une conservation des données sur la base d'un critère géographique objectif, ce qui n'est pas passé inaperçu dans d'autres pays. De nombreux pays ont contacté les autorités belges à ce propos.

Le vice-premier ministre partage l'avis de M. Geens selon lequel il n'est pas toujours simple de distinguer la (menace pour la) sécurité nationale, d'une part, et la criminalité grave, d'autre part. Or, cette distinction est présente dans la jurisprudence de la Cour de justice de l'Union européenne, mais également dans celle de la Cour européenne des droits de l'homme. Les menaces pour la sécurité nationale font l'objet d'un suivi par les services de renseignement. Il s'agit notamment du terrorisme, de l'extrémisme et de l'espionnage: des phénomènes qui peuvent saper la stabilité de l'État de droit. D'ailleurs, certaines formes de criminalité grave peuvent également aboutir à ce résultat. Dans ce cas, les services de renseignement mettront en garde et interviendront.

La Cour de justice de l'Union européenne accorde un niveau moins élevé à la criminalité grave: contrairement à ce qui est le cas pour la menace grave pour la sécurité nationale, la Cour n'accepte, pour ce type de criminalité, aucune conservation générale et indifférenciée. Le projet de loi à l'examen en tient compte.

Wetboek van Strafvordering, op basis van artikel 21 van het Gerechtelijk Wetboek. Klassieke telefonie wordt overigens ook beveiligd met fysieke beveiliging en encryptie. Interceptie ervan is een noodzakelijke en proportionele maatregel, gesteld dat er voldoende waarborgen zijn.

De heer Gilissen uitte zijn bezorgdheid over de potentiële aantasting door de ontworpen regeling van het beroepsgeheim van artsen en advocaten, daarbij een onderscheid makend tussen uitgaande en inkomende communicatie. Ook AVOCATS.BE toonde zich ter zake kritisch. De vice-eersteminister merkt vooreerst op dat het ontworpen artikel 88*bis*, § 3, van het Wetboek van Strafvordering voormeld onderscheid niet maakt. Inlichtingendiensten kunnen operatoren vorderen om de gegevens van beschermde beroepsgroepen te bewaren, maar kunnen ze slechts onder strenge voorwaarden opvragen en verwerken. Het beroepsgeheim kan slechts onder zeer strikte voorwaarden worden opgeheven. Een algemene dataretentievrijstelling voor alle communicatie van beschermde beroepsgroepen is echter niet geoorloofd. Artsen en advocaten kunnen immers het slachtoffer worden van zware criminaliteit, of kunnen zich hieraan bezondigen.

De vice-eersteminister dankt mevrouw Gilson voor haar steunbetuiging aan de voorliggende tekst. Het klopt dat België pioniert met de gegevensbewaring op grond van een objectief geografisch criterium. Dit is in andere landen niet onopgemerkt gebleven; nogal wat landen contacteerden de Belgische overheid hieromtrent.

De vice-eersteminister is het eens met de heer Geens dat het onderscheid tussen enerzijds (bedreiging voor de) nationale veiligheid en anderzijds zware criminaliteit niet steeds gemakkelijk te maken is. Toch is dit onderscheid aanwezig in de rechtspraak van het HvJ-EU, maar ook in die van het Europees Hof voor de Rechten van de Mens. Dreigingen tegen de nationale veiligheid worden opgevolgd door de inlichtingendiensten. Het gaat onder meer om terrorisme, extremisme en spionage: fenomenen die de stabiliteit van de rechtsstaat kunnen ondermijnen. Bepaalde vormen van zware criminaliteit hebben dat vermogen overigens ook. In dat geval zullen de inlichtingendiensten waarschuwen en optreden.

Het HvJ-EU schaalt zware criminaliteit lager in; anders dan voor ernstige dreiging tegen de nationale veiligheid aanvaardt het Hof hiervoor geen algemene en ongedifferentieerde bewaring. Het wetsontwerp houdt hiermee rekening.

Concernant la question de savoir si l'application du critère géographique peut avoir pour effet de couvrir l'ensemble du pays, le vice-premier ministre répond par l'affirmative à M. Geens en renvoyant à l'arrêt récent de la CJUE dans l'affaire *The Commissioner of the Garda Síochána e.a.* (C-140/20). Dans les États membres faiblement peuplés comme la Suède, la situation est différente. Les seuils en question ont été soigneusement élaborés.

En ce qui concerne l'application extraterritoriale des restrictions à la liberté d'encryptage, le vice-premier ministre rappelle que le paragraphe 4 de l'article 107/5 en projet (article 3 du projet de loi) permettra aux opérateurs belges d'exiger, dans les accords avec les opérateurs étrangers, qu'ils soient en mesure de respecter les mêmes dispositions légales que pour leurs propres utilisateurs, et donc que l'interception puisse avoir lieu en Belgique. En l'absence de cette disposition, dans certains cas, seul l'opérateur étranger ou une puissance étrangère (par le biais d'une demande d'entraide judiciaire) serait en mesure d'intercepter un utilisateur étranger dans notre pays. Ce serait préjudiciable pour la souveraineté nationale.

Le vice-premier ministre reconnaît, comme l'a noté M. Geens, que l'APD émet de nombreuses critiques dans son avis n° 108/2021. Sur certains points, le gouvernement a suivi l'APD, mais pas sur d'autres. Elle l'a suivi en ce qui concerne les portes dérobées (*backdoors*) (voir ci-dessus), le rapport d'évaluation annuel (*idem*), l'obligation de conserver les données sur le territoire de l'Union européenne, l'adaptation des articles 122 et 123 en projet de la loi télécom, et la nécessité d'organiser un contrôle préalable par une juridiction ou par une autorité administrative indépendante.

Sur d'autres points, cependant, le gouvernement n'a pas suivi l'APD. Par exemple, l'APD a critiqué l'interdiction d'utiliser des systèmes pouvant empêcher l'identification de l'utilisateur final. Le gouvernement n'était pas du tout d'accord avec cela. Le vice-premier ministre établit un parallèle avec les conducteurs d'une voiture tenus d'avoir un numéro de châssis et une plaque d'immatriculation. Ces éléments peuvent tout autant porter atteinte au respect de la vie privée. Selon le vice-premier ministre, il s'agit de trouver un équilibre, ce que le gouvernement a réussi à faire avec le texte à l'examen.

L'APD a également critiqué le seuil de trois infractions graves pour 1 000 habitants par an. Selon l'APD, seules les condamnations doivent être prises en compte. En l'occurrence également, le gouvernement a maintenu sa position. En effet, il peut arriver qu'une infraction grave, par exemple un meurtre, n'entraîne pas de condamnation.

Op de vraag van de heer Geens of de toepassing van het geografisch criterium tot gevolg kan hebben dat het hele land wordt bestreken, antwoordt de vice-eersteminister bevestigend, onder verwijzing naar het recente arrest van het HvJ-EU in de zaak *The Commissioner of the Garda Síochána e.a.* (C-140/20). In dunbevolkte lidstaten zoals Zweden ligt dat anders. De bewuste drempels werden zorgvuldig uitgewerkt.

Wat de extraterritoriale toepassing van de beperkingen inzake de vrijheid van versleuteling betreft, wijst de vice-eersteminister erop dat paragraaf 4 van het ontworpen artikel 107/5 (artikel 3 van het wetsontwerp) Belgische operatoren in staat stelt om, in overeenkomsten met buitenlandse operatoren, af te dwingen dat ze kunnen voldoen aan dezelfde wettelijke bepalingen als voor hun eigen gebruikers en dat interceptie dus in België zelf moet kunnen gebeuren. Het ontbreken van deze bepaling zou immers betekenen dat in sommige gevallen enkel de buitenlandse operator of een buitenlandse mogendheid (via een rechtshulpverzoek) het onderscheppen van een buitenlandse gebruiker in ons land mogelijk zou kunnen maken. Dit zou nadelig zijn voor de nationale soevereiniteit.

De vice-eersteminister erkent, zoals opgemerkt door de heer Geens, dat de GBA de kritiek niet spaart in haar advies nr. 108/2021. Op sommige punten is de regering de GBA gevolgd, op andere niet. Tot die eerste categorie behoren met name de *backdoors* (cf. *supra*), het jaarlijks evaluatieverslag (*idem*), de verplichting de gegevens te bewaren op het grondgebied van de Europese Unie, de aanpassing van de ontworpen artikelen 122 en 123 van de telecomwet en de noodzaak om voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit te organiseren.

Op andere punten is de regering de GBA echter niet gevolgd. Zo had de GBA kritiek op het verbod op het gebruik van systemen die de identificatie van de eindgebruiker kunnen verhinderen. De regering was het daar hoegenaamd niet mee eens. De vice-eersteminister trekt een parallel met bestuurders van een auto, die verplicht voorzien moet zijn van een chassisnummer en een nummerplaat, en die evenzeer inbreuken op de privacy inhouden. Het komt erop aan een evenwicht te vinden, aldus de vice-eersteminister, waarin de regering met de voorliggende tekst is geslaagd.

De GBA was ook kritisch over de drempel van drie zware strafbare feiten per 1 000 inwoners per jaar. Volgens de GBA mag men enkel veroordelingen in aanmerking nemen. Ook hier is de regering op haar standpunt gebleven. Het is immers mogelijk dat een zwaar strafbaar feit, bijvoorbeeld een moord, niet leidt

Cela ne signifie pas que cette infraction ne doive pas être prise en compte. Compte tenu des observations du COC, le projet de loi prévoit cependant une meilleure structuration de l'information et confie un rôle de supervision à cet organe de contrôle.

M. Geens a demandé comment il se fait que les données réunies au moyen de la conservation des données ne sont pratiquement jamais écartées par les cours et les tribunaux. Selon le vice-premier ministre, cela peut s'expliquer en partie par le fait que la méthode qui est actuellement utilisée par la police et la justice pour accéder aux données de télécommunications est transparente et prévoit suffisamment de garanties. Les demandes introduites par les enquêteurs pour procéder à des réquisitions de données de télécommunications sont enregistrées dans un procès-verbal. C'est sur la base de ce procès-verbal et de l'appréciation des faits que le juge d'instruction, dans le cas de données de localisation, ou le procureur du Roi, dans le cas de données d'identification, établira ou non une réquisition. Cette réquisition doit être motivée. Ces demandes du pouvoir judiciaire sont centralisées par l'intermédiaire d'un point de contact unique, désigné par le Roi. Les exploitants disposent d'une cellule *ad hoc*, dotée de personnel trié sur le volet, qui traite les demandes précitées. Les demandes sont consignées dans les journaux des exploitants. Les résultats des demandes font l'objet de procès-verbaux repris dans le dossier judiciaire. Ils sont accessibles à toutes les parties durant la procédure pénale devant le tribunal et peuvent être contestés en première instance, en appel et même en cassation.

Comme M. Geens l'a souligné à juste titre, l'Organe de contrôle de l'information policière (COC) a rendu un avis encourageant que le gouvernement a pris à cœur. Le vice-premier ministre est parfaitement conscient qu'il convient de garantir la qualité et l'exactitude des données qui seront utilisées pour le comptage des infractions pénales, visées à l'article 90*ter* du Code d'instruction criminelle. C'est pourquoi il a demandé à la Police fédérale d'appliquer une série de principes lors du comptage des infractions pénales. Seul le premier procès-verbal est pris en compte, afin d'éviter qu'une infraction pénale soit comptée plusieurs fois. Plusieurs phases de contrôle humain et procédural ont lieu tout au long du processus, depuis la rédaction du procès-verbal jusqu'au comptage statistique des infractions pénales. Ce dernier se déroule dans l'environnement statistique de la police fédérale, soit le *Management Information System.* Les statistiques sont validées au préalable par le COC, qui se voit d'ailleurs attribuer de nouvelles compétences afin de prendre des mesures en vue de renforcer la qualité des statistiques.

tot een veroordeling. Dat betekent niet dat dat feit buiten beschouwing moet blijven. Op aangeven van het COC werd in het wetsontwerp wel voorzien in een betere structurering van informatie en een toezichthoudende rol voor dit controleorgaan.

De heer Geens vroeg hoe het kwam dat middels dataretentie verzamelde gegevens vrijwel nooit geweerd worden door de hoven en rechtbanken. Volgens de vice-eersteminister kan dit deels worden verklaard doordat de methode die vandaag gebruikt wordt om inzage te krijgen in telecomgegevens door politie en justitie, transparant is en voldoende waarborgen bevat. Zo worden de verzoeken van onderzoekers om over te gaan tot vorderingen van telecomgegevens in een proces-verbaal opgenomen. Het is op basis van dat proces-verbaal en de inschatting van de feiten dat de onderzoeksrechter, bij locatiegegevens, of de procureur des Konings, bij identificatiegegevens, al dan niet een vordering zal opmaken. Die vordering dient gemotiveerd te worden. Deze verzoeken van de rechterlijke macht worden gekanaliseerd via een *single-point-of-contact*, dat door de Koning wordt aangewezen. De exploitanten beschikken over een *ad-hoc*cel, met gescreend personeel, die voormelde verzoeken behandelen. De verzoeken zijn terug te vinden in de logboeken van de exploitanten. De resultaten van de verzoeken zijn het voorwerp van processen-verbaal die in het gerechtelijk dossier worden opgenomen. Ze zijn tijdens de strafprocedure voor de rechtbank toegankelijk voor alle partijen en kunnen worden betwist in eerste aanleg, in hoger beroep en zelfs in cassatie.

Het COC heeft, zoals de heer Geens terecht opmerkte, een bemoedigend advies verleend dat de regering ter harte heeft genomen. De vice-eersteminister is er zich terdege van bewust dat de kwaliteit en de juistheid van de gegevens die zullen worden gebruikt voor de telling van de strafbare feiten, zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering, gegarandeerd moet zijn. Om die reden heeft hij de federale politie gevraagd bij het tellen van de strafbare feiten een aantal principes toe te passen. Enkel het eerste proces-verbaal wordt in aanmerking genomen, om te voorkomen dat een strafbaar feit meerdere malen zou meetellen. In het hele proces vinden verschillende fases van menselijke en procedurele controle plaats, te beginnen met de redactie van het proces-verbaal tot en met de statistische telling van de strafbare feiten. Die laatste gebeurt in het *Management Information System* van de federale politie. De statistieken worden vooraf gevalideerd door het COC, dat overigens nieuwe bevoegdheden krijgt toebedeeld om maatregelen te nemen ter verhoging van de kwaliteit van de statistieken.

Le vice-premier ministre ne partage pas la thèse de M. Boukili selon laquelle le projet de loi organise un contrôle permanent. Il est inexact de dire que l'autorité disposera en permanence de toutes les données. Le texte à l'examen ne va absolument pas dans ce sens. Le gouvernement a soigneusement pesé les différents intérêts en jeu.

M. Boukili a demandé quel pourcentage du territoire et de la population serait visé par la conservation des données. Le vice-premier ministre ne pourra répondre à cette question qu'après que les statistiques auront été validées par le COC. Le COC pourra également imposer des injonctions concernant ces statistiques. L'Organe de contrôle bénéficie de l'entière confiance du vice-premier ministre. Les statistiques seront publiées chaque année dans un arrêté ministériel.

Les décisions de classement sans suite pour charges insuffisantes n'ont en soi pas d'impact sur la constatation d'une infraction pénale au sens de l'article 90*ter* du Code d'instruction criminelle; elles indiquent seulement qu'une infraction à la loi pénale n'a pas pu être attribuée avec suffisamment de certitude à une personne. Dans son arrêt *La Quadrature du Net* (affaires jointes C-511/18, C-512/18 et C-520/18), la Cour de justice de l'Union européenne a considéré au paragraphe 150 que: "Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages". Le fait que de tels actes ne puissent pas être attribués à une personne déterminée n'est pas pertinent.

Selon M. Boukili, le projet de loi part du principe que la conservation des données constitue la règle, et non l'exception. Le vice-premier ministre conteste ce point de vue. Contrairement à la législation annulée sur la conservation des données, le projet de loi à l'examen règle la conservation des données sur la base de critères objectifs et conformément au principe de proportionnalité.

Le vice-premier ministre convient avec Mme Verhelst que la protection de la vie privée est cruciale. Comme il a déjà été indiqué, le projet de loi contient de nombreuses garanties en la matière. En ce qui concerne les services de renseignement, il s'agit d'un contrôle *post factum* par le Comité permanent R. La Sûreté de l'État fera quant à elle également l'objet d'un contrôle de la part de la commission BIM.

Mme Verhelst s'est interrogée sur les conséquences que l'annulation de la législation antérieure a eues sur le

De vice-eersteminister is het oneens met de stelling van de heer Boukili dat het wetsontwerp een permanent toezicht organiseert. Het is niet zo dat de overheid constant over alle gegevens zal beschikken. Dit is hoegenaamd niet de weg die met de voorliggende tekst wordt ingeslagen. De regering heeft de verschillende belangen zorgvuldig afgewogen.

De heer Boukili wilde graag weten welk percentage van het grondgebied en van de bevolking onder de gegevensbewaring zal vallen. De vice-eersteminister zal deze vraag pas kunnen beantwoorden na de validering van de statistieken door het COC. Het COC zal inzake die statistieken ook bevelen kunnen opleggen. Het Controleorgaan geniet het volle vertrouwen van de vice-eersteminister. De statistieken zullen jaarlijks in een ministerieel besluit worden gepubliceerd.

Beslissingen tot seponering wegens onvoldoende bezwaren hebben als zodanig geen impact op de vaststelling van een strafbaar feit in de zin van artikel 90*ter* van het Wetboek van Strafvordering; een en ander duidt er enkel op dat een inbreuk op de strafwet niet met voldoende zekerheid kan toegeschreven worden aan een persoon. In zijn arrest *La Quadrature du Net* (gevoegde zaken C-511/18, C-512/18 en C-520/18) overwoog het HvJ-EU in paragraaf 150: "Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.". Dat zulke daden niet kunnen worden toegeschreven aan een bepaald persoon, doet niet ter zake.

Volgens de heer Boukili is het uitgangspunt van het wetsontwerp dat gegevensbewaring de regel is, en niet de uitzondering. De vice-eersteminister betwist dit. Anders dan in de vernietigde dataretentiewetgeving, wordt de gegevensbewaring gereglementeerd op basis van objectieve criteria en in overeenstemming met het beginsel van de proportionaliteit.

De vice-eersteminister is het eens met mevrouw Verhelst dat de bescherming van het privéleven van cruciaal belang is. Zoals reeds uiteengezet, bevat het wetsontwerp talrijke waarborgen dienaangaande. Wat de inlichtingendiensten betreft, is er een controle *post factum* door het Vast Comité I. Voor de Veiligheid van de Staat is er tevens een controle door de BIM-commissie.

Mevrouw Verhelst vroeg naar de gevolgen in het veld van de vernietiging van de eerdere wetgeving.

terrain. À cet égard, le vice-premier ministre renvoie à un récent arrêt de la Cour de cassation, dans lequel la Cour a confirmé sa jurisprudence antérieure, dite Antigone.

Le vice-premier ministre remercie enfin MM. Segers et Van Hecke pour leurs interventions. Le projet de loi est le fruit d'un délicat exercice d'équilibre. De nombreuses personnes y ont travaillé âprement. Les avis sont nombreux et volumineux. Le texte à l'examen est un texte crucial, qui touche directement à la vie quotidienne des citoyens. Une véritable démocratie se reconnaît à sa capacité de trouver un bon équilibre entre la sécurité et le respect de la vie privée.

B. **Réunion du 18 mai 2022**

1. ***Commentaire des amendements du gouvernement***

Comme déjà annoncé lors de la réunion du 30 mars 2022, *le gouvernement* présente les *amendements nos 1 à 16* (DOC 55 2572), qui visent à adapter le projet de loi en fonction des enseignements de l'arrêt de la Cour constitutionnelle du 18 novembre 2021 (n° 158/2021) (voir également IV. Discussion des articles).

Mme Petra De Sutter, vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste, explique que dans cet arrêt, la Cour constitutionnelle se prononce sur le recours en annulation introduit contre la loi du 1er septembre 2016. Cette loi a été adoptée après les attentats de Paris et de Bruxelles afin de mettre fin à l'anonymat des utilisateurs de cartes prépayées permettant l'utilisation de services mobiles (appels téléphoniques, accès à Internet, envoi de SMS, etc.), et ce, en obligeant les opérateurs à identifier ces utilisateurs.

Sans remettre en cause le principe de l'identification des utilisateurs de cartes prépayées, la Cour a procédé à l'annulation partielle de la modification apportée par la loi précitée à l'article 127 de la loi télécom, tout en maintenant temporairement les effets de la disposition partiellement annulée (jusqu'au 31 décembre 2022 au plus tard). L'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle concerne uniquement l'article 127 de la loi du 13 juin 2005. Or, après analyse, il apparaît que ses enseignements s'appliquent également aux articles 126 et 126/1, en projet, de la loi du 13 juin 2005.

L'amendement n° 1 tend à déplacer les données actuellement énumérées dans l'arrêté royal du 19 septembre 2013 vers l'article 126 de la loi télécom. L'amendement précise que les opérateurs ne doivent conserver les

Dienaangaande verwijst de vice-eersteminister naar een recent arrest van het Hof van Cassatie, waarin het Hof zijn eerdere Antigoon-rechtspraak bevestigde.

De vice-eersteminister dankt ten slotte de heren Segers en Van Hecke voor hun betogen. Het wetsontwerp is het resultaat van een delicate evenwichtsoefening. Velen hebben hieraan hard gewerkt. De adviezen zijn talrijk en volumineus. De voorliggende tekst is een cruciaal stuk, dat rechtstreeks verband houdt met het dagelijks leven van de burgers. Een echte democratie komt tot uiting in het vinden van een goede balans tussen veiligheid en privacy.

B. **Vergadering van 18 mei 2022**

1. ***Toelichting bij de amendementen van de regering***

Zoals reeds aangekondigd tijdens de vergadering van 30 maart 2022, dient *de regering amendementen nrs. 1 tot 16* (DOC 55 2572) in, die tot doel hebben het wetsontwerp aan te passen aan de lering van het arrest van het Grondwettelijk Hof van 18 november 2021 (nr. 158/2021) (zie ook IV. Artikelsgewijze bespreking).

Mevrouw Petra De Sutter, vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post, legt uit dat het Grondwettelijk Hof zich in dat arrest heeft uitgesproken over een beroep tot vernietiging ingesteld tegen de wet van 1 september 2016. Die werd aangenomen na de aanslagen van Parijs en Brussel, om een einde te maken aan de anonimiteit van de gebruikers van voorafbetaalde kaarten aan de hand waarvan mobiele diensten kunnen worden gebruikt (bellen, internettoegang, sms'en versturen, enzovoort), door de operatoren te verplichten om deze laatsten te identificeren.

Zonder het principe van identificatie van de gebruikers van voorafbetaalde kaarten ter discussie te stellen, ging het Hof over tot de gedeeltelijke vernietiging van de wijziging aangebracht door voornoemde wet in artikel 127 van de telecomwet, terwijl het de gevolgen van die gedeeltelijk vernietigde bepaling voorlopig handhaafde (uiterlijk tot 31 december 2022). Het arrest nr. 158/2021 van het Grondwettelijk Hof van 18 november 2021 heeft enkel betrekking op artikel 127 van de wet van 13 juni 2005. Na analyse is evenwel gebleken dat de lessen ervan ook van toepassing zijn op de ontworpen artikelen 126 en 126/1 van de wet van 13 juni 2005.

Door amendement nr. 1 worden de gegevens die thans in het koninklijk besluit van 19 september 2013 opgesomd staan, verplaatst naar artikel 126 van de telecomwet. Het amendement bepaalt dat operatoren de gegevens enkel

données que s'ils les traitent ou les génèrent dans le cadre de la prestation de leurs services. Afin de se conformer à la jurisprudence de la Cour constitutionnelle et de la CJUE, le gouvernement prévoit une obligation de conservation générale et indifférenciée, qui se limite aux données considérées comme "moins intrusives" du point de vue de la protection de la vie privée, à savoir les données d'identification de l'utilisateur final (p. ex. le nom et le prénom), son équipement (p. ex. l'adresse IP) ainsi que la carte SIM et les données d'abonnement à un service de communications électroniques. Il s'agit donc de données d'identification à caractère essentiellement technique et commercial.

L'amendement n° 4 concerne l'article 145 de la loi du 13 juin 2005, qui impose des sanctions pénales. Il s'agit d'une modification purement formelle.

Les amendements n^{os} 5 et 7 visent à introduire de nouvelles dispositions transitoires.

L'amendement n° 6 vise à remplacer l'article 10 du projet de loi, qui lui-même remplace l'actuel article 127 de la loi télécom, partiellement annulé. En effet, depuis que la Cour constitutionnelle a indiqué, dans son arrêt n° 158/2021, que les données et documents relatifs à l'identification de l'abonné ou de l'utilisateur du service devaient être énumérés dans la loi et non dans un arrêté royal, l'article 10 du projet de loi, qui ne modifiait l'article 127 que de manière limitée, était devenu obsolète.

Il existe un lien entre les articles 126 et 127 de la loi télécom, comme le prévoient les amendements qui tendent à remplacer ces articles. L'article 126 prévoit que l'opérateur conserve les données qu'il traite ou génère (par exemple le nom de l'abonné, mais sans garantie de fiabilité), tandis que l'article 127 prévoit que l'opérateur doit collecter et conserver des informations fiables afin d'identifier l'utilisateur final.

Les amendements n^{os} 8 à 13 concernent la loi du 17 janvier 2003 concernant le statut de l'IBPT. Comme d'autres autorités, l'IBPT doit parfois pouvoir prendre connaissance de certaines données d'identification ou métadonnées pour remplir ses missions. Tel est le cas notamment pour ses missions en matière de sécurité des réseaux ou lorsqu'il contrôle le respect des articles 122 à 127 de la loi du 13 juin 2005 par les opérateurs.

M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice, commente les autres amendements, en commençant par les amendements n^{os} 2 et 3, qui sont liés.

moeten bewaren indien zij deze verwerken of generen in het kader van de verrichting van hun diensten. Om aan de rechtspraak van het Grondwettelijk Hof en van het HvJ-EU te voldoen, wordt in een algemene en ongedifferentieerde bewaarplicht voorzien die beperkt is tot de gegevens die "minder ingrijpend" worden geacht vanuit het oogpunt van de privacy, namelijk identificatiegegevens van de eindgebruiker (bijvoorbeeld naam, voornaam), zijn apparatuur (bijvoorbeeld IP-adres) alsook de SIM-kaart en abonnementsgegevens voor een elektronische-communicatiedienst. Het betreft dus identificatiegegevens die vooral technisch en commercieel zijn.

Amendement nr. 4 heeft betrekking op artikel 145 van de wet van 13 juni 2005, dat strafsancties oplegt. Het gaat over een puur formele aanpassing.

Amendementen nrs. 5 en 7 beoogt nieuwe overgangsbepalingen in te voeren.

Amendement nr. 6 strekt ertoe artikel 10 van het wetsontwerp te vervangen, dat op zijn beurt het bestaande, gedeeltelijk vernietigde artikel 127 van de telecomwet vervangt door een nieuwe versie. Vermits het Grondwettelijk Hof in zijn arrest nr. 158/2021 had gesteld dat gegevens en documenten betreffende de identificatie van de abonnee of gebruiker van de dienst in de wet opgesomd moeten worden en niet in een koninklijk besluit, was artikel 10 van het wetsontwerp, dat artikel 127 slechts beperkt wijzigde, immers achterhaald.

Er bestaat een link tussen de artikelen 126 en 127 van de telecomwet, zoals beoogd door de amendementen. Artikel 126 bepaalt dat de operator gegevens bewaart die hij verwerkt of genereert (bijvoorbeeld de naam van de abonnee, maar zonder garantie van betrouwbaarheid). Artikel 127 bepaalt dat de operator betrouwbare informatie moet verzamelen en bewaren om de eindgebruiker te identificeren.

De amendementen nrs. 8 tot 13 betreffen de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector. Net als andere autoriteiten moet het BIPT soms kennis kunnen nemen van bepaalde identificatie- of metagegevens om zijn taken te kunnen vervullen. Dat is meer bepaald het geval voor de taken betreffende de veiligheid van de netwerken of bij het toezicht op de naleving door de operatoren van de artikelen 122 tot 127 van de wet van 13 juni 2005.

De heer Vincent Van Quickenborne, vice-eersteminister en minister van Justitie, geeft toelichting bij de overige amendementen, te beginnen met de – samenhangende – amendementen nrs. 2 en 3.

Étant donné qu'elles peuvent révéler des informations sur les habitudes d'une personne (p. ex. des itinéraires ou des sites web visités), les données de localisation et de trafic ont un impact plus important sur la vie privée des individus que les données d'identification. C'est pour cette raison que le gouvernement présente les amendements n^os^ 2 et 3, qui visent à déterminer dans la loi – et non par arrêté royal – quelles données de trafic et de localisation peuvent être conservées sur la base des critères géographiques. Le premier amendement supprime, dans l'article 126/1, le renvoi à l'arrêté royal énumérant les métadonnées de communication, tandis que l'amendement n° 3 reprend l'essentiel du contenu de cet arrêté dans un article 126/2 (nouveau). Le choix d'un article distinct est dicté par le souci de favoriser la lisibilité du texte.

L'amendement n° 14 modifie l'article 46*bis* du Code d'instruction criminelle, qui décrit la possibilité pour un procureur du Roi d'identifier un utilisateur de moyens de communications électroniques. Le gouvernement propose d'insérer un nouvel alinéa entre les deuxième et troisième alinéas du paragraphe 1^er^, afin de préciser que le procureur du Roi peut demander la collaboration de certaines personnes et/ou institutions en vue de l'identification directe ou indirecte de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques.

Outre l'identification directe par l'opérateur lui-même, il est possible que l'opérateur ne dispose que des données de paiement ou des données d'un intermédiaire. Cette identification indirecte peut se faire auprès des banques et des institutions financières, des centres fermés ou d'une catégorie résiduelle, à savoir d'autres entités juridiques qui enregistrent une carte SIM au lieu de personnes physiques. Il s'agit par exemple de personnes qui, en raison de leur état de santé, ne pourraient pas se rendre dans un magasin de téléphonie.

Enfin, les amendements n^os^ 15 et 16 apportent des modifications respectivement à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers et à la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits.

2. ***Questions et observations des membres***

Mme Sophie De Wit (N-VA) indique que, malgré cette tentative, qui n'est pas sans mérite, entreprise pour répondre à la jurisprudence de la Cour constitutionnelle et de la Cour de justice de l'Union européenne, son groupe continue à se poser de nombreuses questions.

Aangezien ze informatie over de levensgewoonten van een persoon kunnen onthullen (bijvoorbeeld trajecten, bezochte websites), hebben locatie- en verkeersgegevens meer impact op de persoonlijke levenssfeer van personen dan identificatiegegevens. Om die reden dient de regering de amendementen nrs. 2 en 3 in, die ertoe strekken in de wet – en dus niet in een koninklijk besluit – te bepalen welke verkeers – en locatiegegevens mogen bewaard worden op basis van de geografische criteria. Het eerste amendement verwijdert de referentie naar het koninklijk besluit dat de metadata van communicatie opsomt, uit artikel 126/1, terwijl amendement nr. 3 het gros van de inhoud van dit besluit opneemt in een nieuw artikel 126/2. De keuze voor een apart artikel is ingegeven door de bekommering om de leesbaarheid van de tekst te bevorderen.

Amendement nr. 14 strekt tot wijziging van artikel 46*bis* van het Wetboek van strafvordering, dat bepaalt hoe een procureur des Konings een gebruiker van elektronische communicatiemiddelen kan identificeren. De regering stelt voor tussen het tweede en het derde lid van § 1 een nieuw lid in te voegen, teneinde te verduidelijken dat de procureur des Konings bepaalde personen en/of instellingen tot medewerking kan verzoeken om de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst rechtstreeks of indirect te identificeren.

De gebruiker kan rechtstreeks door de operator zelf worden geïdentificeerd of, indien die laatste slechts over de betalingsgegevens of de gegevens van een tussenpersoon beschikt, indirect via banken en financiële instellingen, via gesloten centra of via een restcategorie, namelijk de juridische entiteiten die een SIM-kaart registreren in de plaats van natuurlijke personen. Het gaat daarbij bijvoorbeeld om personen die zich vanwege hun gezondheidstoestand niet naar een telefoniewinkel kunnen begeven.

De amendementen nrs. 15 en 16, ten slotte, betreffen wijzigingen van respectievelijk de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten en van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten.

2. ***Vragen en opmerkingen van de leden***

Mevrouw Sophie De Wit (N-VA) geeft aan dat haar fractie, niettegenstaande de niet onverdienstelijke poging die wordt ondernomen om tegemoet te komen aan de rechtspraak van het Grondwettelijk Hof en het HvJ-EU, met veel vragen blijft zitten.

La protection des données à caractère personnel est une préoccupation largement partagée. La conservation de données est une chose, mais l'accès à ces données en est une autre. Si cet accès s'inscrit dans le cadre d'une enquête concernant des faits punissables d'une certaine gravité, il est clair que l'atteinte à la vie privée doit être mise en balance avec le droit à la sécurité et la lutte contre la criminalité. La hiérarchie de la magistrature debout et celle de la police judiciaire fédérale ont encore souligné récemment, au sein du parlement, l'importance capitale de pouvoir accéder aux données des communications électroniques. Un tel accès n'est pas, sur le principe, remis en cause, même si l'intervenante se demande si le système de conservation de données par niveaux que le gouvernement entend instaurer n'est pas à tel point compartimenté qu'il aboutira encore à une conservation indifférenciée.

Cependant, les textes à l'examen prévoient encore d'autres formes d'accès, par d'autres autorités, en dehors du cadre des enquêtes pénales. Cet aspect est nettement plus délicat. Dans des cas de ce type, avec quels intérêts l'ingérence dans la vie privée doit-elle être mise en balance? Cette distinction est importante pour la N-VA et se traduira également dans le vote du groupe.

En ce qui concerne à nouveau le volet justice, la Cour a proposé plusieurs lignes directrices, qui ne simplifient pas ce dispositif. L'ampleur de l'avis du Conseil d'État en la matière est éloquente. La mise en œuvre pratique du régime élaboré est particulièrement complexe. Par exemple, plusieurs zones seront délimitées au travers de statistiques, pour aboutir à un régime différencié. Cependant, si ces statistiques ne sont pas minutieusement définies ou recueillies, la conservation des données risque de porter sur l'ensemble du territoire. Autrement dit: les paramètres censés assurer la différentiation n'aboutiront-ils toutefois pas, dans la pratique, à une conservation générale et indifférenciée, de sorte que ce régime risquerait à nouveau d'être annulé? Un nouveau recours en annulation est d'ailleurs déjà en préparation.

Il est positif que le gouvernement tienne compte, dans le texte à l'examen, de la jurisprudence nationale et européenne, en particulier en ce qui concerne la conservation sur base géographique, mais le régime élaboré résistera-t-il à la mise en pratique? À lire les avis écrits, il est permis d'en douter.

Mme De Wit est également préoccupée par la longue période transitoire prévue par le projet de loi. Qu'adviendra-t-il, entre-temps, des enquêtes en cours?

De bescherming van persoonsgegevens is een breed gedeelde bekommering. Het bewaren van gegevens is één zaak, maar de toegang tot die gegevens is een andere. Als die toegang kadert in een onderzoek naar strafbare feiten van een zekere ernst, is het duidelijk dat de inbreuk op de privacy moet afgewogen worden tegen het recht op veiligheid en de strijd tegen criminaliteit. De top van de staande magistratuur en van de federale gerechtelijke politie heeft onlangs in dit parlement nog het cruciale belang onderstreept van het kunnen beschikken over gegevens van elektronische communicatie. Zulke toegang staat principieel niet ter discussie, hoewel de spreekster zich afvraagt of het gelaagde systeem van gegevensbewaring dat de regering beoogt in te voeren, niet dermate gecompartimenteerd is dat men alsnog tot een ongedifferentieerde bewaring komt.

De voorliggende teksten voorzien echter ook nog in andere vormen van toegang, door andere autoriteiten, buiten het kader van strafonderzoeken. Dat is een veel moeilijker verhaal. Tegen welke belangen moet de inmenging in het privéleven in zulke gevallen worden afgewogen? Dit onderscheid is voor de N-VA belangrijk en zal ook doorschemeren in het stemgedrag van de fractie.

Wat opnieuw het justitiële aspect betreft, heeft het Hof een aantal kapstokken aangereikt. Die maken de regeling er niet eenvoudiger op. De omvang van het advies van de Raad van State is ter zake veelzeggend. De praktische uitvoering van de ontworpen regeling wordt bijzonder complex. Zo zullen bepaalde zones worden afgebakend aan de hand van statistieken, om tot een gedifferentieerde regeling te komen. Maar als die statistieken niet zorgvuldig worden gedefinieerd of ingezameld, bestaat het risico dat de gegevensbewaring alsnog het hele grondgebied beslaat. Anders gezegd: zullen de parameters die voor differentiatie behoren te zorgen, in de praktijk toch niet leiden tot een algemene en ongedifferentieerde bewaring, waardoor de regeling opnieuw dreigt vernietigd te worden? Een nieuw beroep tot vernietiging staat overigens al in de steigers.

Het is goed dat de regering in de voorliggende tekst rekening houdt met de nationale en Europese rechtspraak, in het bijzonder wat de bewaring op geografische basis betreft, maar zal de ontworpen regeling de praktijktoets doorstaan? Als men de schriftelijke adviezen leest, kan men daaraan twijfelen.

Een andere bezorgdheid van mevrouw De Wit heeft te maken met de lange overgangsperiode waarin het wetsontwerp voorziet. Wat zal er in tussentijd gebeuren

S'il faut accorder cinq ans aux opérateurs pour pouvoir appliquer ce régime, qu'a-t-on en fait résolu?

Mme De Wit souligne que son groupe ne s'oppose nullement à ce que l'on fournisse à la police et à la justice les instruments qui leur sont nécessaires pour protéger la société. Au contraire, il s'agit d'une importante préoccupation de la N-VA. Cependant, il convient évidemment de pouvoir maintenir ces instruments. L'intervenante espère que le gouvernement pourra offrir cette garantie et donner une réponse satisfaisante aux commentaires critiques du COC, de l'APD et du Conseil d'État. Elle félicite le gouvernement d'avoir rédigé cet exposé des motifs détaillé, qu'il faudra toutefois encore compléter sur certains points.

M. Michael Freilich (N-VA) craint que ce document ne se dirige vers une nouvelle annulation par la Cour constitutionnelle.

L'intervenant souligne l'importance de la protection de la vie privée. Or, dans certaines circonstances, il peut être nécessaire de limiter ce droit. Il incombe aux politiques de réaliser cette très délicate mise en balance.

Le projet de loi à l'examen vise à rétablir un régime annulé parce qu'il contenait une atteinte injustifiée à la vie privée. C'est pourquoi l'avis de l'APD mérite une attention particulière. Dans son avis n° 66/2022 relatif aux amendements du gouvernement, l'APD renvoie à son avis n° 108/2021 concernant l'avant-projet. Elle y formule "de nombreuses remarques, certaines [] fondamentales". L'APD indique ensuite qu'"[à] défaut de revoir en profondeur le projet de loi de réparation afin de s'assurer qu'il opère le changement de perspective exigé, tant la conservation de ces données de trafic et de localisation par les opérateurs que leur communication aux autorités porteraient atteinte à la directive ePrivacy, interprétée à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Or une nouvelle annulation par la Cour constitutionnelle de la loi de réparation serait de nature à entacher gravement la confiance des citoyennes et les citoyens dans les institutions démocratiques".

Au cours de ce débat, l'utilisation de données de télécommunications afin de pouvoir localiser rapidement un enfant disparu a été mentionnée à plusieurs reprises. Il va de soi qu'il s'agit d'une préoccupation justifiée, mais le problème ne sera pas résolu en proposant des solutions générales à partir de cas particuliers. En cas d'enlèvement, les enquêteurs ont besoin de données

met de lopende onderzoeken? Als men de operatoren vijf jaar moet geven om de regeling te kunnen toepassen, wat heeft men dan eigenlijk opgelost?

Mevrouw De Wit benadrukt dat haar fractie er hoegenaamd niet op tegen is om politie en gerecht de instrumenten te geven die zij nodig hebben om de maatschappij te beschermen. Dit is integendeel een belangrijke bekommering van de N-VA. Maar die instrumenten moeten natuurlijk wel overeind kunnen blijven. De spreekster drukt de hoop uit dat de regering die garantie kan bieden en een bevredigend antwoord kan geven op de kritische commentaren van het COC, de GBA en de Raad van State. Zij prijst de regering voor de uitgebreide memorie van toelichting, die evenwel op bepaalde punten nog aanvulling zal behoeven.

De heer Michael Freilich (N-VA) vreest dat men met dit werkstuk afstevent op een nieuwe vernietiging door het Grondwettelijk Hof.

De spreker onderstreept het belang van de bescherming van het privéleven. Onder bepaalde omstandigheden kan het nodig zijn dat recht in te perken. Het is aan politici om die erg moeilijke afweging te maken.

Het voorliggende wetsontwerp sterkt ertoe een regeling te herstellen die vernietigd werd omdat zij een ongerechtvaardigde aantasting van de privacy inhield. Om die reden verdient het advies van de GBA bijzondere aandacht. In haar advies nr. 66/2022 betreffende de amendementen van de regering verwijst de GBA naar haar advies nr. 108/2021 aangaande het voorontwerp. Daarin formuleerde zij "talrijke opmerkingen [], waarvan sommige fundamenteel". De GBA geeft voorts aan dat "tenzij het ontwerp van herstelwet grondig wordt herzien om ervoor te zorgen dat het de vereiste perspectiefwijziging brengt, [] zowel het bewaren van dergelijke verkeers- en locatiegegevens door operatoren als de mededeling ervan aan autoriteiten een inbreuk zou vormen op de e-privacyrichtlijn, geïnterpreteerd in het licht van de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Een nieuwe nietigverklaring van de herstelwet door het Grondwettelijk Hof zou het vertrouwen van de burgers in de democratische instellingen ernstig kunnen ondermijnen".

In dit debat werd verscheidene keren verwezen naar het gebruik van telecomgegevens om snel een vermist kind te kunnen lokaliseren. Dit is uiteraard een terechte bekommering. Maar door brede oplossingen voor te stellen op basis van specifieke gevallen, lost men het probleem niet op. Bij een ontvoering hebben speurders live data nodig; dat is iets helemaal anders dan het

en temps réel. Cela n'a rien à voir avec la conservation des données de l'ensemble de la population pendant une longue période.

Le gouvernement se saisit de l'opportunité offerte par la réparation de la législation annulée pour aller beaucoup plus loin. C'est non seulement aux opérateurs, mais aussi aux réseaux d'entreprises privés qu'il sera demandé de conserver de nombreuses données. Les courriers électroniques et les communications de machine à machine devront être conservées au sein des entreprises. La conservation ciblée sur une base géographique prévue pour la rétention d'informations par les opérateurs ne s'applique pas à la conservation par les réseaux d'entreprises, qui est indifférenciée. Personne n'accepterait que les autorités publiques obligent une personne à noter chaque jour combien de temps elle a parlé à qui (devant l'école, au travail, etc.). Or, c'est en substance ce que le gouvernement actuel demande aux entreprises au travers du texte à l'examen.

Même les entreprises qui ne conservent pas de métadonnées, comme *Signal*, seraient concernées par cette obligation. Cela signifie-t-il que les services de cette nature seront interdits? La police interpellera-t-elle à l'avenir des citoyens en rue afin de vérifier qu'ils ont installé l'application *Signal* sur leur téléphone?

Ce raisonnement s'applique également à la navigation anonyme sur le web. Les connexions au moyen d'un VPN qui permettent aux personnes situées en Russie et en Chine de visi*ter* des sites web occidentaux seront-elles interdites?

Des critiques ont aussi été émises par les opérateurs de télécommunications. Dans son avis d'initiative, BCPA Belgium indique que l'harmonisation de la législation sur la conservation de données au sein de l'Union européenne est indispensable pour limiter la complexité des systèmes et les coûts de mise en conformité. Les initiatives prises au niveau des États membres, par exemple le projet de loi visé, ne servent pas l'idéal d'un marché interne européen uniforme. M. Freilich fait observer que, dès lors que les opérateurs seront de plus en plus tournés vers le niveau international, une initiative européenne aurait été préférable.

L'ISPA estime que l'obligation de conservation proposée, fondée sur des critères géographiques, est disproportionnée. Ses représentants soulignent que l'enregistrement géographique impose une charge informatique énorme aux exploitants. De nombreux problèmes pratiques se poseront. Il est par exemple parfaitement possible qu'une conversation mobile commence dans une zone déterminée (où la conservation est obligatoire),

bewaren van gegevens van de hele bevolking over een lange periode.

De regering grijpt de reparatie van de vernietigde wetgeving aan om veel verder te gaan. Niet enkel de operatoren worden gevraagd om vele data bij te houden, ook private bedrijfsnetwerken zullen dat moeten doen. E-mails en *machine-to-machine* communicatie binnen bedrijven zullen moeten worden bewaard. De gerichte bewaring op geografische basis, waarin wordt voorzien voor de gegevensretentie door operatoren, geldt niet voor de bewaring door bedrijfsnetwerken; die is ongedifferentieerd. Niemand zou aanvaarden dat de overheid een persoon zou verplichten elke dag bij te houden met wie hij hoe lang heeft gesproken (aan de schoolpoort, op het werk enzovoort). Toch is het in wezen dit dat de regering bedrijven middels de voorliggende tekst vraagt.

Zelfs bedrijven die geen metadata bijhouden, zoals *Signal*, zouden onder die verplichting vallen. Betekent dit dat dergelijke diensten verboden worden? Hoe gaat men dat afdwingen? Gaat de politie in de toekomst mensen op straat tegenhouden om te controleren of zij de *Signal*-app gedownload hebben op hun smartphone?

Hetzelfde geldt voor anoniem surfen. Zal de VPN-verbinding in de ban worden geslagen? Het is die technologie die mensen in Rusland en China in staat stelt om westerse websites te bezoeken.

Kritiek komt er ook vanuit de hoek van de telecomoperatoren. In zijn initiatiefadvies stelt BCPA Belgium: "Harmonisatie van dataretentiewetgeving binnen de Europese Unie is noodzakelijk om de complexiteit van systemen en processen te beperken en de nalevingskosten te drukken. Het ideaal van een eengemaakte Europese interne markt wordt niet gediend met lokale initiatieven op het niveau van de lidstaten, zoals het onderhavige wetsontwerp". Een Europees initiatief ware wenselijker geweest, aldus de heer Freilich, die erop wijst dat operatoren steeds internationaler gaan werken.

ISPA acht de voorgestelde bewaarplicht volgens geografische criteria onevenredig. Zij wijzen erop dat de geografische opslag een enorme IT-last op de exploitanten legt. Tal van praktische problemen duiken op: zo is het denkbaar dat een mobiel gesprek in een bepaalde zone (met verplichte bewaring) start, maar in een andere zone (waar geen bewaringsplicht geldt) eindigt. En wat doet men als slechts één van de partijen zich in een zone met

mais se termine dans une autre zone (où l'obligation de conservation ne s'appliquera pas). Et qu'arrivera-t-il si seulement l'une des parties se trouve dans une zone où la conservation est obligatoire? En outre, les adresses et les zones changent constamment.

Comment les prestataires de services par contournement comme *Signal* mais aussi *WhatsApp* organiseront-ils la conservation de données sur une base géographique? Peut-on attendre de ces acteurs mondiaux qu'ils réorganisent complètement leurs systèmes seulement pour la Belgique? Aucun autre État membre de l'Union européenne ne va aussi loin dans l'obligation de conservation des métadonnées.

Comme l'APD, l'intervenant craint que la mise en œuvre du critère géographique aboutisse à nouveau à une conservation de données générale et indifférenciée. Le gouvernement peut-il donner une indication du pourcentage du territoire qui sera couvert par la conservation de données sur la base des critères actuellement prévus par le projet de loi à l'examen (critère statistique, zones stratégiques, *etc.*)? La transparence s'impose à cet égard. L'APD la demande également.

La faisabilité technique de la réglementation en projet constitue un autre point sensible. Les opérateurs sont sérieusement préoccupés par cette question. Il faut être conscient que les prix des télécommunications sont directement liés à la réglementation à laquelle les opérateurs sont soumis. Si le législateur impose un temps d'attente maximal de 2,5 minutes pour les appels téléphoniques des consommateurs aux opérateurs, cette mesure aura un coût qui sera répercuté sur les consommateurs. Ce sera pareil pour la réglementation à l'examen, pour laquelle une période de transition de pas moins de cinq ans a été prévue.

Quelle certitude le gouvernement a-t-il que la règlementation en projet ne sera pas à nouveau annulée par la Cour constitutionnelle? De nombreuses institutions estiment que le risque est élevé. Dans son avis, la Ligue des droits humains indique que l'objectif ne peut pas être de résoudre le problème du sous-financement de la justice en instaurant une conservation générale des données. Une étude menée en Allemagne indique d'ailleurs que cette mesure n'est pas efficace dans la lutte contre la criminalité. L'intervenant estime que la conservation doit être ciblée, sans quoi elle risque d'être annulée pour la troisième fois.

L'intervenant souligne que l'APD n'est pas un ennemi. Au contraire, c'est l'organisme qui a l'avis le plus légitime dans cette matière. L'intervenant demande que l'on accorde à l'avis de l'APD l'importance qu'il a.

verplichte bewaring bevindt? Bovendien zijn adressen en zones aan voortdurende verandering onderhevig.

Hoe gaan aanbieders van OTT-diensten, zoals *Signal* maar ook *WhatsApp*, de dataretentie op geografische basis organiseren? Kan men van die mondiale spelers verwachten dat zij speciaal voor ons land hun systemen gaan overhoopgooien? Geen enkele andere EU-lidstaat gaat dermate ver in het verplichten van de bewaring van metadata.

Samen met de GBA is de spreker bezorgd dat de implementatie van het geografische criterium opnieuw tot een algehele en ongedifferentieerde gegevensbewaring zal leiden. Kan de regering een indicatie geven van het percentage van het grondgebied dat gedekt zal zijn door de gegevensbewaring, op basis van de criteria in de regeling zoals die nu voorligt (statistisch criterium, strategisch zones enzovoort)? Daaromtrent moet transparantie heersen, daarop hamert ook de GBA.

De technische haalbaarheid van de ontworpen regeling is een ander heikel punt. De operatoren maken zich daarover ernstige zorgen. Men moet beseffen dat er een rechtstreeks verband is tussen de telecomprijzen en de regulering waaraan de operatoren zijn onderworpen. Als de wetgever een maximale wachttijd van 2,5 minuten oplegt voor telefonische oproepen van consumenten naar operatoren, heeft dat een kostprijs die aan de consument wordt doorgerekend. Hetzelfde zal gebeuren met deze regeling, waarvoor een overgangsperiode van maar liefst vijf jaar is bepaald.

Hoe zeker is de regering dat de ontworpen regeling niet opnieuw vernietigd zal worden door het Grondwettelijk Hof? Nogal wat instanties schatten die kans hoog in. In haar advies stelt de *Ligue des droits humains* dat het niet de bedoeling mag zijn om de onderfinanciering van justitie te verhelpen door een algemene gegevensbewaring te gaan invoeren. Duits onderzoek toont overigens aan dat zo'n maatregel niet effectief is in de strijd tegen de criminaliteit. De bewaring moet gericht zijn, aldus de spreker, zo niet stevenen we af op een derde vernietiging.

De GBA is in dezen niet onze vijand, aldus de spreker. Het is integendeel de instantie die in deze materie het meest recht van spreken heeft. De spreker roept op om het GBA-advies het gewicht te geven dat het toekomt.

Ou le gouvernement n'envisage-t-il que le court terme? S'agit-il d'une forme de politique d'annonce qui remet à plus tard la question de l'annulation?

Outre la conservation, l'accès aux données est également formulé très largement dans le projet de loi. Un accès est par exemple prévu pour l'IBPT, le CCB, la Cellule personnes disparues, la FSMA et l'AFSCA afin de leur permettre de lutter contre toute utilisation malveillante du réseau. Cette notion est définie de manière très large: l'envoi d'un courrier électronique de harcèlement à un collègue est par exemple visé par cette définition. Sans vouloir minimaliser la problématique du harcèlement en ligne, l'intervenant estime qu'il est étrange que l'accès aux données soit accordé dans ce cas, sans intervention judiciaire, sachant que, selon le texte à l'examen, la criminalité grave ne peut pas être considérée comme une menace pour la sécurité nationale.

M. Albert Vicaire (Ecolo-Groen) rappelle que le respect des personnes et des choix individuels qui comprend la protection des données privées est un des trois piliers d'Ecolo-Groen. Toute brèche dans ce respect est toujours le résultat d'un compromis. Le projet de loi comble un vide juridique qui existe depuis la décision de la Cour constitutionnelle d'invalider le texte précédent. De l'autre côté, les autorités judiciaires ont besoin d'outils pour accélérer la résolution des enquêtes. Les données concernées sont celles relatives à l'identification et métadonnées. Il ne s'agit pas du contenu et il n'est pas question de demander une conversation. Avec cette loi, les services de renseignement, de police – sur accord du judiciaire – auront donc un accès plus limité que Google ou Facebook. Elles pourront connaître le lieu d'appel, les adresses IP connectées ainsi que les moments de connexion. L'intervenant estime qu'il faut donc relativiser la portée de cette loi.

Il ajoute que le texte en projet détermine des lieux et des conditions pour autoriser la collecte de données. Le niveau de criminalité par exemple ou les parlements, les aéroports, … Ceci se trouve dans l'article 126/1, en projet, de la loi du 13 juin 2005, qui décrit aussi que le NTSU, service de police mandaté va annuellement faire une carte sur la base de la criminalité des trois années précédentes. Les zones de polices seront classées par catégorie de six, neuf ou douze mois de conservation des métadonnées en fonction du niveau de criminalité.

Of heeft de regering slechts de korte termijn voor ogen? Is dit een vorm van aankondigingspolitiek, waarbij de vernietiging een zorg is voor later?

Naast de bewaring is ook de toegang tot de gegevens in het wetsontwerp zeer breed geformuleerd. Zo krijgen het BIPT, het CCB, de Cel Vermiste Personen, de FSMA en het FAVV toegang, om kwaadwillig gebruik van het netwerk te bestrijden. Dat laatste wordt zeer ruim opgevat: het sturen van een pestmail naar een collega valt daar bijvoorbeeld onder. Zonder de problematiek van cyberpesten te willen minimaliseren, vindt de spreker het opmerkelijk dat in zo'n gevallen toegang tot de gegevens kan worden verleend, zonder rechterlijke tussenkomst, zeker als men weet dat zware criminaliteit volgens de voorliggende tekst niet kan beschouwd worden als een dreiging tegen de nationale veiligheid.

De heer Albert Vicaire (Ecolo-Groen) stipt aan dat het respect voor de personen en voor de individuele keuzes, inclusief de bescherming van de privégegevens, een van de drie pijlers vormt van het gedachtegoed van Ecolo-Groen. Elke barst in dat respect is telkens het resultaat van een compromis. Het wetsontwerp moet een einde maken aan de juridische leemte die is ontstaan toen het Grondwettelijk Hof heeft beslist de vorige wettekst ongeldig te verklaren. Anderzijds hebben de gerechtelijke autoriteiten nood aan instrumenten om de onderzoeken sneller succesvol te kunnen afronden. De desbetreffende gegevens hebben betrekking op de identificatie en de metagegevens. Het gaat niet om de inhoud en het is geenszins de bedoeling een gesprek aan te vragen. Met de ontworpen wet zouden de inlichtingen- en de politiediensten – na toestemming van het gerecht – een beperktere toegang hebben dan Google of Facebook. Ze zouden de plaats van oproep kunnen achterhalen, alsook de IP-adressen waarmee een verbinding tot stand is gekomen en de tijdstippen waarop de betrokkene verbonden was. Volgens de spreker moet de strekking van deze tekst dus worden gerelativeerd.

Hij voegt eraan toe dat de ontworpen wet ook zou bepalen waar en onder welke voorwaarden die gegevensverzameling zou kunnen worden toegestaan (bijvoorbeeld de graad van criminaliteit of nog de parlementen, de luchthavens enzovoort). Zo staat het ook in het ontworpen artikel 126/1 van de wet van 13 juni 2005, dat er tevens toe strekt te bepalen dat de NTSU, een gemandateerde politiedienst, jaarlijks de criminaliteit van de drie voorgaande jaren in kaart zal brengen. De politiezones zouden naargelang van de criminaliteitsgraad worden gerangschikt per categorie van zes, negen of twaalf maanden voor het bijhouden van de metagegevens.

Il estime aussi que ce texte demande une plus grande protection des lanceurs d'alertes. Il cite l'exemple d'un employé d'un opérateur souhaitant devenir lanceur d'alerte. Il pense qu'il hésitera à le faire par voie électronique.

Il se dit curieux de lire les statistiques de l'évolution de la criminalité dans les zones calmes avec et sans collecte des données et demandera cette évolution au ministre de la Justice dans un an.

En conclusion, M. Vicaire explique que son groupe soutiendra ce texte qui est le résultat de l'équilibre entre la demande des autorités judiciaires et la nécessaire protection des concitoyens.

M. Erik Gilissen (VB) rappelle que la lutte contre la criminalité est une priorité absolue pour son groupe, comme par exemple la recherche d'indices dans le cadre d'actes terroristes ou de disparitions d'enfants: il faut doter les différentes instances des moyens nécessaires pour mener à bien leurs recherches et missions. Il comprend la difficulté de trouver un équilibre entre l'efficacité de l'action policière et judiciaire et le respect de la vie privée. Il espère qu'il pourra être recherché avec ce projet de loi. Il note que l'Autorité de protection des données (APD) et le Conseil d'État ont fait part d'une série de remarques. Il cite notamment le cas de la conservation des adresses IP, qui peuvent être contournées notamment par le truchement de connections VPN ou de réseaux publics gratuits. Ce n'est donc, à ses yeux, pas une garantie de traçabilité absolue. De même, la conservation de toutes les adresses IP revient à une conservation indifférenciée.

Sur la notion de zones stratégiques, certaines sont définies dans le projet de loi mais parfois de manière fort large. Il y a également des différences de durée de conservation des données en fonction du nombre d'infractions dans une zone définie. Il se demande si cela ne rompt pas le principe d'égalité devant la loi.

M. Nabil Boukili (PVDA-PTB) explique d'emblée que le projet n'est pas proportionné. Il relève que l'avant-projet revient à supprimer l'anonymat sur Internet. Dans son avis, l'APD donne un bon résumé du problème lorsqu'elle dit que "les nouvelles définitions d'"opérateur" et de "services de communications électroniques", couplées, notamment, à l'obligation d'identification imposée par les nouveaux articles 126 et 127 de la loi télécom (introduits par les amendements n° 1 et 6), aboutissent

De spreker is ook van mening dat dit wetsontwerp een betere bescherming van de klokkenluiders vergt. Hij geeft het voorbeeld van een werknemer van een operator die klokkenluider wil worden. Volgens hem zal die niet geneigd zijn dit via elektronische weg te doen.

Hij is benieuwd naar de statistieken over de evolutie van de criminaliteit in de kalme zones met en zonder gegevensverzameling en zal over een jaar bij de minister van Justitie informeren naar die evolutie.

Tot besluit kondigt de heer Vicaire aan dat zijn fractie haar steun zal geven aan dit wetsontwerp, dat het resultaat is van het evenwicht tussen het verzoek van de gerechtelijke overheden en de noodzakelijke bescherming van de medeburgers.

De heer Erik Gilissen (VB) stipt aan dat de criminaliteitsbestrijding, waaronder het zoeken naar sporen in het kader van terroristische daden of verdwijningen van kinderen, een absoluut speerpunt is voor zijn fractie. De verschillende instanties moeten over de nodige middelen kunnen beschikken om hun onderzoek en hun opdrachten naar behoren te kunnen uitvoeren. Hij begrijpt dat het moeilijk is een evenwicht te vinden tussen de doeltreffendheid van het werk van de politie en van het gerecht en de eerbiediging van de persoonlijke levenssfeer. Hij hoopt dat dit evenwicht met dit wetsontwerp zal kunnen worden gevonden. Hij merkt op dat de Gegevensbeschermingsautoriteit (GBA) en de Raad van State een reeks opmerkingen hebben gemaakt. Zo is er de opmerking in verband met het bijhouden van IP-adressen, waaraan evenwel kan worden ontkomen door gebruik te maken van VPN-netwerken of gratis openbare netwerken. Volgens de spreker kan de traceerbaarheid dus niet absoluut worden gewaarborgd. Bovendien komt het bijhouden van alle IP-adressen neer op een ongedifferentieerd bijhouden ervan.

Wat het begrip van de strategische zones betreft, is het zo dat sommige van die zones in het wetsontwerp worden gedefinieerd, maar dat gebeurt soms behoorlijk ruim. Ook varieert de bewaartermijn van de gegevens naargelang van het aantal inbreuken in een welbepaalde zone. De spreker vraagt zich af of dat niet in strijd is met gelijkheidsbeginsel.

De heer Nabil Boukili (PVDA-PTB) windt er geen doekjes om: het wetsontwerp is disproportioneel. Volgens hem komt de tekst erop neer dat een einde wordt gemaakt aan de anonimiteit op internet. In haar advies vat de GBA het probleem goed samen wanneer zij stelt dat de nieuwe definities van "operator" en van "elektronische communicatiediensten", meer bepaald in combinatie met de identificatieverplichting die zou worden opgelegd bij de nieuwe artikelen 126 en 127 van de telecomwet

à rendre impossible – ou en tout cas très difficile – toute correspondance anonyme sur Internet." Il se réfère à la position publique de M. Bart Preneel, professeur de cryptographie à la KU Leuven. Avec ce projet de loi, des opérateurs comme *Signal*, qui offrent des services de communication sécurisés et anonymes, ne pourront plus opérer en Belgique.

Il estime que l'anonymat sur Internet, ce n'est pas juste une sorte de "caprice" d'intellectuel. Lorsque *WhatsApp* a annoncé qu'il partage ses données avec tout le reste du groupe Meta (comme *Facebook*), des personnalités comme Edward Snowden (qui a dénoncé la surveillance de masse par la *National Security Agency*) se sont prononcées en faveur de *Signal*. Les mots du lanceur d'alerte sont assez clairs: "Une raison pour utiliser *Signal* est que je l'utilise tous les jours et que je ne suis pas encore mort".

Selon le rapport spécial de l'ONU sur la liberté d'expression, "le chiffrement et l'anonymat offrent la confidentialité et la sécurité nécessaires à l'exercice du droit à la liberté d'opinion et d'expression à l'ère du numérique. Une telle sécurité peut s'avérer indispensable pour l'exercice d'autres droits". Il formule la recommandation suivante: "en ce qui concerne l'anonymat, les États devraient adopter des politiques de non-restriction ou de protection globale (…) Les États devraient tendre à renforcer le chiffrement et l'anonymat. Les lois nationales devraient reconnaître la liberté de protéger la confidentialité de ses communications électroniques à l'aide de technologies et d'outils de chiffrement permettant d'être anonyme en ligne. (…) Les États ne devraient pas imposer de restriction au chiffrement et à l'anonymat qui facilitent et, souvent, rendent possible l'exercice des droits à la liberté d'opinion et d'expression."

M. Boukili affirme que le gouvernement fait exactement le contraire. *Signal* est utilisé de par le monde par les militants, la société civile, les lanceurs d'alerte ou encore les journalistes qui ont besoin de ce caractère anonyme. Notamment pour éviter des représailles ou de la censure. Même la Commission européenne impose à son personnel d'utiliser *Signal*. Selon lui, c'est totalement hors de proportion par rapport à l'objectif poursuivi.

Il se demande dès lors ce que répond le gouvernement aux inquiétudes de la société civile et des citoyens par rapport à l'anonymat sur Internet. Est-ce que l'impact de ce projet de loi sur les messageries cryptées, comme *Signal*, a été examiné? Il demande au vice-premier

(waarvan de amendementen nrs. 1 en 6 de invoeging beogen), ertoe leiden dat elke anonieme correspondentie op internet "onmogelijk – of op zijn minst zeer moeilijk –" wordt. Hij verwijst naar het publieke standpunt van professor Bart Preneel, hoogleraar cryptografie aan de KU Leuven. Met dit wetsontwerp zullen operatoren als *Signal*, die beveiligde en anonieme communicatiediensten aanbieden, niet langer in België actief kunnen zijn.

Volgens de spreker is anonimiteit op internet niet gewoon een soort van intellectuele "gril". Toen *WhatsApp* aangaf dat het data zou delen met andere onderdelen van de Meta-groep (zoals *Facebook*), hebben vooraanstaande figuren als Edward Snowden (die de massascreening door het *National Security Agency* aan de kaak gesteld heeft) zich voor *Signal* uitgesproken. De woorden van de klokkenluider spreken voor zich: "*Une raison pour utiliser Signal est que je l'utilise tous les jours et que je ne suis pas encore mort.*"

De speciaal VN-rapporteur voor de vrijheid van meningsuiting verwoordde het zo: "*le chiffrement et l'anonymat offrent la confidentialité et la sécurité nécessaires à l'exercice du droit à la liberté d'opinion et d'expression à l'ère du numérique. Une telle sécurité peut s'avérer indispensable pour l'exercice d'autres droits.*" Hij verstrekt de volgende aanbeveling: "*en ce qui concerne l'anonymat, les États devraient adopter des politiques de non-restriction ou de protection globale (…). Les États devraient tendre à renforcer le chiffrement et l'anonymat. Les lois nationales devraient reconnaître la liberté de protéger la confidentialité de ses communications électroniques à l'aide de technologies et d'outils de chiffrement permettant d'être anonyme en ligne. (…) Les États ne devraient pas imposer de restriction au chiffrement et à l'anonymat qui facilitent et, souvent, rendent possible l'exercice des droits à la liberté d'opinion et d'expression*."

Volgens de heer Boukili doet de regering precies het tegenovergestelde. Wereldwijd wordt *Signal* gebruikt door militanten, middenveldorganisaties, klokkenluiders en ook journalisten die deze anonimiteit nodig hebben. Al was het maar om zich te beschermen voor represailles of censuur. Zelfs de Europese Commissie legt het gebruik van *Signal* aan haar personeelsleden op. De spreker is van mening dat het wetsontwerp volstrekt buiten proportie is ten opzichte van het streefdoel.

Hij wil dan ook weten hoe de regering antwoordt op de bekommeringen van het middenveld en van de burgers in verband met anonimiteit op internet. Werd de impact van dit wetsontwerp op versleutelingsdiensten zoals *Signal* onderzocht? Hij vraagt of de vice-eersteminister

ministre de confirmer que ce type de messagerie ne pourra plus être utilisée si le projet est voté.

L'intervenant relève ensuite que l'étendue géographique de la conservation des données ne peut pas être évaluée à ce stade: les critères de choix des "zones" qui seront surveillées ne sont pas transparents. Il rappelle avoir demandé quel pourcentage du territoire serait concerné. Il a reçu comme réponse que "ce n'est pas au ministre de le déterminer". Il prend acte qu'il est demandé aux membres de la commission de voter en validant un projet de loi qui instaure une surveillance aux contours flous.

Il observe qu'on va garder les données des zones où un certain taux de criminalité est constaté (ports, gares, aéroports, prisons, communes où sont présentes des infrastructures critiques, zones où il y a une menace grave potentielle pour les intérêts vitaux du pays, comme les autoroutes et les parkings attenants, les domaines royaux,…). Il comprend dès lors que les zones faisant l'objet de la conservation des données vont être très larges et que cela pourrait très bien être proche de 100 % du territoire. Il observe qu'il suffit de passer par une autoroute, une gare, un aéroport pour être l'objet de cette conservation des données: selon lui, tout le monde ou presque passe par ces endroits, souvent quotidiennement. Il souligne à ce propos la formulation utilisée dans les développements: "il n'est pas impossible que l'entièreté du territoire national soit visé par une conservation des données. Autrement formulé, […] si cette hypothèse est rencontrée, il s'agira alors d'une conservation ciblée dans son approche mais généralisée dans ses conséquences."

En conclusion, il prend acte que c'est un ciblage qui est "ciblé" sur l'entièreté de la Belgique et l'entièreté de sa population.

Or, la CJUE admet la conservation des données "ciblée". Mais elle interdit aussi et surtout la conservation généralisée et indifférenciée. On ne doit pas, sous couvert de "ciblage", réintroduire une conservation généralisée sur tout le territoire. Il cite à ce sujet la Cour dans son arrêt *The Commissioner of the Garda Síochána e.a.* du 5 avril 2022 (C-140/20): "[…] il importe, dans une société démocratique, que [la conservation des données] soit […] l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur

kan bevestigen dat, mocht het wetsontwerp worden aangenomen, dergelijke berichtendiensten niet langer gebruikt zullen mogen worden.

Vervolgens merkt de spreker op dat de geografische reikwijdte van de databewaring in dit stadium niet kan worden nagegaan: de keuzecriteria voor de "gebieden" waarop toezicht van toepassing zal zijn, zijn niet transparant. Eerder vroeg de spreker al om welk percentage van het grondgebied het ging. "*Ce n'est pas au ministre de le déterminer*", luidde het antwoord. Hij neemt er akte van dat de commissieleden gevraagd wordt in te stemmen met een wetsontwerp dat een toezicht invoert waarvan de krijtlijnen wazig zijn.

De spreker wijst erop dat de gegevens zullen worden bewaard van locaties met een zekere criminaliteitsgraad (havens, stations, luchthavens, gevangenissen, gemeenten met kritieke voorzieningen, gebieden waar 's lands vitale belangen ernstig kunnen worden bedreigd, zoals autosnelwegen en bijbehorende parkings, de koninklijke domeinen enzovoort). Voor de spreker is het dan ook duidelijk dat de gebieden waarvoor de gegevens zullen worden bewaard, bijzonder ruim opgevat zijn en dat het weleens om bijna 100 % van het grondgebied zou kunnen gaan. Hij merkt op dat je je nog maar op een autosnelweg, in een station of op een luchthaven hoeft te bevinden opdat je gegevens bewaard zullen worden; stuk voor stuk plaatsen waar iedereen of toch bijna iedereen weleens komt, vaak dagelijks. Hij benadrukt in dit verband de formulering die in de toelichting is gebruikt: "het [is] niet onmogelijk (…) dat het gehele nationale grondgebied onder de gegevensbewaring valt. Met andere woorden, […]. (i)ndien aan deze hypothese wordt voldaan, dan is er sprake van bewaring die doelgericht is in haar aanpak maar veralgemeend in haar gevolgen."

Tot besluit neemt de spreker er nota van dat de beoogde gegevensbewaring "gericht" is op heel België en de hele Belgische bevolking.

Het Hof van Justitie van de Europese Unie staat evenwel "doelgerichte" gegevensbewaring toe. Maar ook en vooral verbiedt het veralgemeende en ongedifferentieerde databewaring. Onder het mom van een "doelgerichte" maatregel mag geen veralgemeende databewaring over het hele grondgebied mogelijk worden gemaakt. De spreker verwijst naar een arrest van het Hof van Justitie (arrest C-140/20, *Commissioner of the Garda Síochána and Others*, van 5 april 2022): "[…] in een democratische samenleving [is het] dan ook van belang dat [de bewaring van gegevens] […], de uitzondering en niet de regel vormt en dat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Deze conclusie geldt zelfs met betrekking tot de doelstellingen

reconnaître." (paragraphe 65). "[…] [C]'est [aux États membres] et non à la Cour qu'il incombe d'identifier de tels critères [pour mettre en œuvre une conservation ciblée], étant entendu qu'il ne saurait être question de réinstaurer, par ce biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation." (paragraphe 83).

M. Boukili explique qu'il faut donc savoir, avant de voter ce projet de loi, si l'application de ces critères va mener à cette conservation généralisée et indifférenciée. Or, il constate que le gouvernement ne sait pas préciser ni le pourcentage du territoire concerné, ni le pourcentage de la population. Il se demande comment on peut vérifier dans ces conditions qu'on reste dans les "clous" du droit européen. Il observe néanmoins que les spécialistes de la question ont cependant déjà des éléments de réponse, même si le gouvernement n'en n'a pas. Selon M. Vilenas Vadapalas, ancien juge à la CJUE, "le ciblage simultané dans plusieurs zones est à exclure, parce qu'il acquiert là un caractère général et perd son caractère ciblé". Selon lui, ce projet de loi "revient à autoriser des mesures de ciblage dans tellement de zones que cela transformerait la conservation "ciblée" en une "conservation de données générale et indiscriminée sans établir les garanties juridiques nécessaires". Il considère dès lors que le gouvernement réintroduit bien une conservation généralisée des données interdite par le droit européen.

L'intervenant se pose la question de savoir si avant de voter ce projet de loi, une vraie évaluation du territoire national et de la population qui seront ciblés ne serait pas utile. Pour répondre au principe de légalité, il se demande si cette évaluation ne devrait-elle pas figurer dans les travaux législatifs, voire dans le projet de loi lui-même.

Pour la conservation de données de certaines zones, comme par exemple les autoroutes et certains lieux précis comme les prisons ou des lieux stratégiques, l'intervenant se demande comment le gouvernement va strictement limiter la conservation à ces lieux, d'un point de vue technique. Il se demande si les quartiers entourant les établissements pénitentiaires ne seront pas ciblés de façon "collatérale".

M. Boukili estime ensuite que la notion "d'infractions graves" est trop large. Il relève que le gouvernement a indiqué que la Cour autorise une conservation des

van bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen voor de openbare veiligheid en het belang dat aan deze doelstellingen moet worden toegekend" (paragraaf 65). En verder: "[H]et [is] aan [de lidstaten] en niet aan het Hof (…) om die criteria [om een gerichte bewaring te organiseren] te bepalen, met dien verstande dat niet opnieuw een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens mag worden ingevoerd" (paragraaf 83).

Volgens de heer Boukili dient, voordat over dit wetsontwerp wordt gestemd, de vraag te worden beantwoord of de toepassing van die criteria zal leiden tot een veralgemeende, ongedifferentieerde bewaring van gegevens. Hij stelt echter vast dat de regering niet exact kan aangeven om welk percentage van het grondgebied of van de bevolking het gaat. Hij vraagt zich af hoe in die omstandigheden kan worden nagegaan dat het Europees recht wel degelijk in acht genomen wordt. De spreker wijst erop dat de regering hierop het antwoord schuldig blijft, maar dat deskundigen ter zake alvast wel een aanzet tot antwoord hebben. De heer Vilenas Vadapalas, gewezen rechter bij het Hof van Justitie van de Europese Unie, stelt dat "*le ciblage simultané dans plusieurs zones est à exclure, parce qu'il acquiert là un caractère général et perd son caractère ciblé*". Volgens hem komt het wetsontwerp neer op "*autoriser des mesures de ciblage dans tellement de zones que cela transformerait la conservation "ciblée" en une "conservation de données générale et indiscriminée sans établir les garanties juridiques nécessaires".*" Hij is dus van oordeel dat de regering wel degelijk een veralgemeende – door het Europees recht verboden – databewaring opnieuw invoert.

De spreker acht het raadzaam, alvorens over dit wetsontwerp te stemmen, duidelijk te onderzoeken op welk gedeelte van 's lands grondgebied en bevolking deze doelgerichte gegevensbewaring van toepassing zou zijn. In het licht van het legaliteitsbeginsel vraagt hij zich af of die beoordeling niet vervat moet zijn in de documenten met betrekking tot de parlementaire voorbereiding of zelfs in het wetsontwerp zelf.

Aangaande de bewaring van gegevens in welbepaalde gebieden, zoals autosnelwegen en strikt afgebakende locaties zoals gevangenissen of strategische plaatsen, wil de spreker weten hoe de regering er technisch in zal slagen de databewaring strikt te beperken tot die plaatsen. Hij vraagt zich af of de omwonenden van strafinrichtingen niet het voorwerp van "collaterale" databewaring zullen zijn.

Vervolgens vindt de heer Boukili het begrip "ernstig misdrijf" te ruim. Hij wijst erop dat de regering heeft aangegeven dat het HvJ-EU een "gerichte" gegevensbewaring

données “ciblée” notamment sur la base du taux “d’infractions graves”. Encore faut-il savoir ce qu’on considère comme de la “criminalité grave”. La notion reprise dans le projet de loi renvoie à l’article 90*ter* du Code d’instruction criminelle qui prévoit les cas dans lesquels un juge d’instruction peut ordonner des mises sur écoutes. C’est une notion particulièrement large qui comprend, par exemple, le faux informatique, la fraude informatique, la détention de stupéfiants, entre autres.

L’intervenant croit comprendre que le gouvernement a voulu faire une sorte d’analogie en se basant sur l’article 90*ter* C.I.cr. Il estime que cette analogie est fausse: on ne peut pas simplement transposer les infractions permettant qu’un juge ordonne des écoutes téléphoniques à la conservation de données en amont sur des zones géographiques parce que, dans le cas des écoutes, elles doivent être ordonnées par un juge d’instruction, ce qui constitue une garantie supplémentaire. Il rappelle que les écoutes sont réellement ciblées sur un individu ou un groupe d’individus, et ne concernent pas des populations entières.

À ce stade, il relève que la CJUE ne donne pas de définition “de criminalité grave”. Mais, selon lui, il n’est pas du tout certain que le renvoi à l’article 90*ter* passe la rampe des critères qu’elle pourrait être amenée à définir. Là aussi, il estime que cela pose une vraie question au niveau de la proportionnalité du projet de loi. Il se demande dès lors pourquoi avoir choisi de procéder par renvoi à l’article 90*ter* C.i.cr. pour définir la notion de “criminalité grave”. Est-ce que cela répond aux critères de la CJUE?

M. Boukili relève également que le gouvernement instaure une obligation de conservation généralisée des données pour lutter contre la fraude. Il rappelle à la vice-première ministre De Sutter qu’il l’a interrogé sur la conservation des données pour la lutte contre la fraude sur les réseaux, en insistant sur l’avis de l’APD qui indiquait qu’on réintroduit “par la fenêtre” une conservation généralisée et indifférenciée. La vice-première ministre avait répondu que “cette obligation de conservation généralisée concerne seulement la lutte contre la fraude”.

L’intervenant en retient deux choses: la vice-première ministre reconnaît bien qu’il s’agit d’une obligation de conservation généralisée et la CJUE n’admet pas de telles obligations généralisées de conservation. Elle ne le permet même pas pour lutter contre la “criminalité grave”. Or, la fraude n’est pas forcément de la “criminalité grave”. La CJUE a confirmé que le droit de l’Union s’oppose à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques aux fins de la lutte

toestaat, met name op basis van het percentage “ernstige misdrijven”. Dan blijft de vraag wat moet worden beschouwd als “zware criminaliteit”. Het desbetreffende begrip in het wetsontwerp verwijst naar artikel 90*ter* van het Wetboek van strafvordering, dat de gevallen opsomt waarin een onderzoeksrechter de opdracht kan geven tot telefoontaps. Wat daaronder valt is erg ruim, met onder andere computervervalsing, computerfraude, bezit van verdovende middelen enzovoort.

De spreker meent te hebben begrepen dat de regering een soort van parallel wilde trekken met artikel 90*ter* van het Wetboek van strafvordering. Hij is echter van oordeel dat die analogie onjuist is: men kan de strafbare feiten waarvoor een rechter telefoontaps kan gelasten, niet zonder meer overnemen wanneer het erom gaat anticipatief gegevens te bewaren op basis van een geografisch criterium. Telefoontaps kunnen namelijk enkel op bevel van een onderzoeksrechter, wat een extra waarborg biedt. De spreker herinnert eraan dat telefoontaps echt gericht zijn op een individu of op een groep van individuen, en niet op hele populaties.

In dit stadium wijst de spreker erop dat het HvJ-EU geen definitie geeft van “zware criminaliteit”. Maar volgens hem is het helemaal niet zeker dat de verwijzing naar artikel 90*ter* zou volstaan, mocht het Hof dienaangaande criteria formuleren. Ook op dit punt is de spreker van oordeel dat het wetsontwerp onevenredig is. Derhalve vraagt hij waarom ervoor werd gekozen te verwijzen naar artikel 90*ter* van het Wetboek van strafvordering om het begrip “zware criminaliteit” te definiëren. Voldoet dit aan de criteria van het HvJ-EU?

De heer Boukili stelt ook vast dat de regering een algemene bewaarplicht van gegevens invoert om fraude tegen te gaan. Hij attendeert vice-eersteminister De Sutter erop dat hij haar vragen heeft gesteld over de bewaring van gegevens inzake fraudebestrijding op de netwerken, waarbij met nadruk werd gewezen op het advies van de GBA die stelde dat via een achterdeurtje opnieuw een algemene en ongedifferentieerde bewaring werd ingevoerd. De vice-eersteminister had toen geantwoord dat die algemene bewaarplicht alleen de fraudebestrijding betreft.

Daaruit onthoudt de spreker twee zaken: de vice-eersteminister erkent dat het een algemene bewaarplicht betreft en het HvJ-EU aanvaardt een dergelijke algemene bewaarplicht niet – zelfs niet om de “zware criminaliteit” tegen te gaan. Fraude is echter niet noodzakelijkerwijs “zware criminaliteit”. Het HvJ-EU heeft bevestigd dat het EU-recht zich verzet tegen een algemene en ongedifferentieerde bewaring van gegevens met betrekking tot het elektronische dataverkeer en de locatie van elektronische communicatie, met het oog op de bestrijding van

contre les infractions graves. Si même la criminalité grave ne le justifie pas, *a fortiori* la fraude, qui ne rentre pas nécessairement dans la définition de “criminalité grave”, ne le peut pas non plus. Il observe que la Ligue des droits humains (LDH) ne dit pas autre chose et juge d’ailleurs ce système “manifestement disproportionné”.

Il aimerait réentendre la vice-première ministre par rapport à cette obligation de conservation généralisée pour la fraude, alors que ce n’est pas permis par le droit européen. Quels sont les arguments pour aller contre la jurisprudence de la CJUE? Est-il proportionné de conserver des données pour lutter contre la fraude, alors que cela ne l’est pas pour la criminalité grave?

Plus globalement, M. Boukili estime que le projet manque sa cible. Il invite à examiner un autre critère, celui de la nécessité: est-il utile et nécessaire de conserver les données pour lutter contre la criminalité grave? À lire l’avis de l’APD, il estime qu’on peut au minimum réfléchir à cette question: “les criminels qui souhaitent échapper à la surveillance trouveront d’autres moyens de communication qui leur permettront de préserver leur anonymat”. En clair, il constate que l’APD dit que ça ne va pas marcher pour donner les moyens à la justice de poursuivre des infractions. La LDH ne dit pas autre chose quand elle indique dans son avis qu’“en matière de lutte contre la criminalité grave, le projet de loi à l’examen consiste avant tout en un choix politique désastreux.”

Il souligne encore qu’une étude du service de recherches du Parlement européen démontre que les lois sur la conservation des données n’ont pas d’effet mesurable sur la criminalité dans les pays de l’UE où elles ont été mises en place. L’étude révèle:

— qu’en Autriche, où la loi sur la conservation des données n’existe plus depuis 2015, le taux d’élucidation des crimes a augmenté massivement: de 44 % en 2015 à 52,5 % en 2018. Le nombre de crimes constatés a diminué;

— qu’aux Pays-Bas, où la loi n’est plus en vigueur depuis 2016, le taux d’élucidation des crimes a augmenté de 25,5 % en 2016 à 28,5 % en 2018;

— qu’en Allemagne, où la loi n’est plus en vigueur depuis 2011, le taux d’élucidation des crimes a augmenté de 55 % en 2011 à 58 % en 2018;

— qu’en Italie, en Suède et en Espagne, où des lois similaires sont en vigueur, on n’observe pas d’évolution positive mais une stabilité du taux d’élucidation, voire une diminution.

ernstige misdrijven. Als zelfs de zware criminaliteit zulks niet rechtvaardigt, dan kan fraude, die niet noodzakelijkerwijs onder de definitie van “zware criminaliteit” valt, dat *a fortiori* evenmin. De spreker stipt aan dat de *Ligue des droits humains* (LDH) hetzelfde zegt en voorts van oordeel is dat de regeling “kennelijk onevenredig” is.

De spreker zou de vice-eersteminister nogmaals willen horen over die algemene bewaarplicht met betrekking tot fraude, terwijl het Europees recht zulks niet toestaat. Wat zijn de argumenten om tegen de rechtspraak van het HvJ-EU in te gaan? Is het evenredig om gegevens te bewaren om fraude te bestrijden, terwijl zulks niet het geval is met betrekking tot zware criminaliteit?

Meer in het algemeen is de heer Boukili van oordeel dat het wetsontwerp zijn doel voorbijschiet. Hij roept op ook het criterium van de noodzaak te onderzoeken: is de gegevensbewaring nuttig en noodzakelijk om de zware criminaliteit tegen te gaan? Op basis van het advies van de GBA is de spreker van oordeel dat het vraagstuk minstens uitdieping vereist: de criminelen die aan toezicht willen ontsnappen, zullen andere communicatiemiddelen vinden waarmee ze anoniem kunnen blijven. In klare taal: de spreker wijst erop dat de GBA stelt dat zulks niet zal volstaan in het streven om het gerecht de middelen te verschaffen om misdrijven te vervolgen. Het advies van de LDH is van een soortgelijke strekking: inzake de bestrijding van de zware criminaliteit getuigt het ter bespreking voorliggende wetsontwerp vooral van een rampzalige beleidskeuze.

De spreker benadrukt nog dat uit een studie van de onderzoeksdienst van het Europees Parlement is gebleken dat de wetten inzake gegevensbewaring geen meetbare gevolgen hebben voor de misdaad in de EU-landen waar ze werden ingevoerd. Zo blijkt onder meer:

— dat in Oostenrijk, sinds de wet inzake de gegevensbewaring er in 2015 werd opgeheven, aanzienlijk méér misdrijven werden opgehelderd: van 44 % in 2015 steeg de ophelderingsgraad naar 52,5 % in 2018. Voorts is het aantal geregistreerde misdrijven gedaald;

— dat in Nederland, waar de wet sinds 2016 niet meer van kracht is, de ophelderingscijfers zijn gestegen van 25,5 % in 2016 naar 28,5 % in 2018;

— dat in Duitsland, waar de wet sinds 2011 niet meer van kracht is, de ophelderingscijfers zijn gestegen van 55 % in 2011 naar 58 % in 2018;

— dat in Italië, Zweden en Spanje, waar soortgelijke wetten van kracht zijn, geen positieve evolutie maar een status quo of zelfs een daling van de ophelderingscijfers wordt vastgesteld.

L'orateur cite ensuite une étude de 2011, réalisée en Allemagne, avancée par la LDH, qui démontre qu'après deux années d'entrée en vigueur de la loi, la conservation des données n'avait pas rendu plus efficace la poursuite des infractions graves. En effet, si la conservation des données a permis à la police d'enregistrer plus d'actes criminels graves (2009: 1 422 968) qu'avant (2007: 1 359 102), les infractions graves ont cependant moins souvent été élucidées (2009: 76,3 %) qu'avant la conservation de toutes les données de communication (2007: 77,6 %). Selon la LDH, les effets contreproductifs de la conservation des données sur les enquêtes criminelles peuvent s'expliquer par "le comportement d'évitement des utilisateurs": "afin d'éviter l'enregistrement d'informations sensibles, les utilisateurs ayant l'intention de protéger leurs communications ont recours à d'autres moyens: utilisés des cybercafés, des points d'accès sans fil, des services d'anonymisation, des téléphone publics, etc."

M. Boukili affirme que si on veut prendre une mesure qui porte atteinte aux droits et libertés, il faut d'abord établir quel sera son impact réel, si elle permet d'atteindre l'objectif qu'on se donne, *in casu* lutter contre la criminalité. Et dans cette matière, la charge de la preuve incombe au gouvernement afin de démontrer l'efficacité de ce type de mesures. Il se demande dès lors si le gouvernement a procédé à une étude de l'efficacité de ces législations existant à l'étranger pour lutter contre la criminalité grave.

Il estime que ce projet de loi s'attaque à des droits fondamentaux qu'il faut préserver. Il invite le gouvernement à argumenter sur la base d'études qui iraient dans le sens des choix posés pour mettre en place ce projet de loi.

M. Koen Geens (CD&V) souligne qu'en 2020, la Sûreté de l'État a demandé 5 123 fois à un opérateur de fournir les données d'identification d'un utilisateur de télécommunications, et 524 fois les données de trafic et de localisation. Pour la police fédérale, les chiffres sont encore plus élevés, et atteignent respectivement 1 749 000 et 49 000 demandes (données de trafic). Ces chiffres illustrent l'importance de ce débat. Il importe que le gouvernement puisse apporter des réponses aux questions qui se posent, car une fois la loi adoptée, ce ne sera qu'une question de temps avant qu'elle ne fasse l'objet d'un recours en annulation devant la Cour constitutionnelle.

Un point important de la réglementation en projet est l'utilisation du cryptage. L'intervenant est très préoccupé par la possibilité pour les services de décrypter. Bien que l'article 107/5 proposé de la loi télécom (article 3 du projet

Vervolgens verwijst de spreker naar een in Duitsland uitgevoerde studie uit 2011, aangehaald door de LDH, waaruit blijkt dat – twee jaar na de inwerkingtreding van de wet – de gegevensbewaring er niet toe had geleid dat ernstige misdrijven doeltreffender werden vervolgd. Hoewel de gegevensbewaring de politie in de mogelijkheid heeft gesteld om meer zware criminele feiten te registreren (2009: 1 422 968) dan voorheen (2007: 1 359 102), werden de ernstige misdrijven minder vaak opgehelderd (2009: 76,3 %) dan vóór de bewaring van alle communicatiegegevens (2007: 77,6 %). Volgens de LDH kunnen de contraproductieve gevolgen van de gegevensbewaring voor de strafonderzoeken worden verklaard door het "vermijdingsgedrag" van de gebruikers: om de registratie van gevoelige informatie te voorkomen, nemen de gebruikers die hun communicatie willen beschermen hun toevlucht tot andere middelen: cybercafés, draadloze toegangspunten, anonimiseringsdiensten, openbare telefoons enzovoort.

De heer Boukili stelt dat indien wordt beoogd een maatregel te nemen die afbreuk doet aan de rechten en vrijheden, eerst moet worden vastgesteld wat de werkelijke impact ervan zal zijn en of de beoogde doelstelling ermee kan worden bereikt, *in casu* de criminaliteit bestrijden. Aldus ligt de bewijslast bij de regering; zij moet aantonen dat dergelijke maatregelen doeltreffend zijn. In het licht daarvan vraagt de spreker of de regering de doeltreffendheid van een dergelijke wetgeving in het buitenland bij de bestrijding van zware criminaliteit al heeft onderzocht.

De spreker is van oordeel dat dit wetsontwerp grondrechten aantast die moeten worden gehandhaafd. Hij roept de regering op om op grond van onderzoek argumenten aan te reiken ter ondersteuning van de in dit wetsontwerp gemaakte keuzes.

De heer Koen Geens (CD&V) wijst erop dat de Staatsveiligheid in 2020 5 123 keer een operator heeft gevorderd om de identificatiegegevens van een telecomgebruiker mee te delen, en 524 keer verkeers- en locatiegegevens. Voor de Federale Politie liggen deze cijfers nog een pak hoger, respectievelijk op 1 749 000 en 49 000 (verkeersgegevens). Deze cijfers illustreren het belang van dit debat. Het is belangrijk dat de regering antwoorden kan geven op de vragen die zich stellen, want eens aangenomen is het slechts een kwestie van tijd vooraleer de wet het voorwerp zal uitmaken van een beroep tot vernietiging bij het Grondwettelijk Hof.

Een belangrijk aandachtspunt in de ontworpen regeling is het gebruik van versleuteling. De spreker is heel bekommerd om de mogelijkheid voor de diensten om te decrypteren. Hoewel het ontworpen artikel 107/5 van

de loi) vise à instaurer certaines restrictions au principe de la liberté de cryptage, la Sûreté de l'État indique dans son avis écrit que le projet de loi est insuffisant à cet égard. Les vice-premiers ministres peuvent-ils confirmer que, nonobstant cet avis, le texte à l'examen offre des possibilités suffisantes en matière de décryptage?

L'article 122, § 4, proposé, de la loi télécom, tel que prévu à l'article 5 du projet de loi, dispose que l'obligation de conserver certaines données d'identification et de trafic peut être générale, en cas de fraude présumée ou d'utilisation malveillante du réseau. Cette disposition est-elle conforme à la jurisprudence de la CJUE, qui interdit la conservation indifférenciée et généralisée à d'autres fins que la sauvegarde de la sécurité nationale?

Dans son avis écrit, Me Catherine Forget examine l'arrêt *Ministerio Fiscal* (C-207/16) de la CJUE. Elle écrit que, si la Cour a déclaré dans cet arrêt que la conservation du numéro d'identification des téléphones mobiles (*International Mobile Equipment Identity* ou IMEI) est autorisée, on ne sait pas clairement si cette conservation peut être imposée aux opérateurs. Dans cette optique, Me Forget estime qu'il est souhaitable de limiter l'obligation de collecter certaines données de manière systématique et indifférenciée aux adresses IP. Quels arguments le gouvernement tire-t-il de l'arrêt précité pour imposer une obligation de conservation qui va au-delà de ce que recommande Me Forget?

3. ***Réponses des vice-premiers ministres***

Mme Petra De Sutter, vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste, apporte les précisions suivantes:

— sur l'équilibre à trouver entre la sécurité et le respect de la vie privée, elle estime que c'est le cœur du dilemme qui peut opposer différentes visions. Elle rappelle que l'arrêt de la Cour n'impliquait pas des changements cosmétiques mais un véritable changement de perspective. A ses yeux, cet objectif est rencontré dans le projet de loi;

— sur l'accès des autorités aux métadonnées, il était nécessaire d'y apporter des adaptations, ce qui a été fait;

— sur les demandes de différentes autorités, la loi organique prévoit la nécessité pour avoir accès aux différentes catégories de données que la demande soit

de telecomwet (artikel 3 van het wetsontwerp) enkele beperkingen beoogt in te voeren op de principiële vrijheid van versleuteling, stelt de Veiligheid van de Staat in zijn schriftelijk advies dat het wetsontwerp op dit punt ontoereikend is. Kunnen de vice-eersteministers bevestigen dat, niettegenstaande dit advies, de voorliggende tekst toch voldoende mogelijkheden biedt op het stuk van de ontsleuteling?

In het ontworpen artikel 122, § 4, van de telecomwet, zoals beoogd door artikel 5 van het wetsontwerp, wordt bepaald dat de verplichting tot het bewaren van bepaalde identificatie- en verkeersgegevens algemeen kan zijn, in geval van vermeende fraude of van vermeend kwaadwillig gebruik van het netwerk. Is zulks in overeenstemming met de rechtspraak van het HvJ-EU, die een algemene en ongedifferentieerde bewaring voor andere redenen dan de vrijwaring van de nationale veiligheid, verbiedt?

In haar schriftelijk advies bespreekt meester Catherine Forget het arrest *Ministerio Fiscal (*C-207/16) van het HvJ-EU. Zij schrijft dat het Hof in dat arrest weliswaar heeft gesteld dat het bewaren van het identificatienummer van gsm-toestellen (*International Mobile Equipment Identity* of IMEI) toegelaten is, maar dat het niet duidelijk is of die bewaring mag worden opgelegd aan de operatoren. In die optiek acht meester Forget het raadzaam om de verplichting om bepaalde gegevens op systematische en ongedifferentieerde wijze te verzamelen, te beperken tot IP-adressen. Welke argumenten haalt de regering uit genoemd arrest om een bewaarplicht voor te schrijven die verdergaat dan wat meester Forget aanbeveelt?

3. ***Antwoorden van de vice-eersteministers***

Mevrouw Petra De Sutter, vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post, verstrekt de volgende verduidelijkingen:

— het evenwicht tussen veiligheid en de inachtneming van de persoonlijke levenssfeer is volgens de minister de kern van het dilemma waarover uiteenlopende zienswijzen kunnen bestaan. Zij wijst erop dat het arrest van het Grondwettelijk Hof een heuse ommezwaai noodzakelijk maakt, dus méér dan enkele oppervlakkige wijzigingen. Volgens de minister maakt het wetsontwerp die doelstelling waar;

— de overheidstoegang tot de metagegevens moest worden bijgestuurd en dat is gebeurd;

— wat de verzoeken vanwege de diverse overheden betreft, vereist de organieke wet dat het verzoek om toegang tot de diverse gegevenscategorieën met

justifiée. Le cadre a été strictement défini pour rencontrer ces conditions;

— sur la question de savoir si la loi ne va pas à nouveau être annulée, elle espère avoir rencontré au mieux les critiques et arguments soulevés par la Cour;

— sur les critiques de l'APD relayées par M. Freilich, l'intervenante estime qu'elles ont été en partie rencontrées et, si non, qu'elles ont fait l'objet d'une argumentation détaillée. Il s'agit pas uniquement d'une question d'utilisation des données au seul regard du respect de la vie privée mais aussi de devoir tenir compte des impératifs de sécurité et de technicité pour les opérateurs;

— sur les réseaux privés et d'entreprises, elle précise qu'ils relèvent de l'article 9, § 7, de la loi du 13 juin 2005, qui n'a pas été modifié. Ils ne sont pas couverts par le projet de loi;

— sur les réseaux privés virtuels (VPN) qui sont une connexion sécurisée et chiffrée entre deux réseaux ou entre un utilisateur individuel et un réseau et qui permettent de se cacher lorsqu'on surfe sur le Web, ils ne tombent pas non plus sous le coup du projet de loi;

— sur le fait que chaque État membre a sa propre réglementation, elle constate que cela ne facilite pas les choses. Une réglementation européenne unique serait préférable mais la loi de réparation ne pouvait attendre puisque la loi avait été annulée;

— sur la faisabilité technique, elle explique que de nombreuses remarques ont été faites par les opérateurs eux-mêmes. Ces adaptations représentent un coût et prennent du temps, ce qui explique le délai prévu et la période transitoire, notamment pour l'article 126/1 en projet;

— sur la question de savoir qui reçoit l'accès et de quelle manière, en matière de sécurité des réseaux, la loi relative au statut de l'IBPT précise ces points. Le secrétaire d'État Michel pourra répondre plus avant;

— la vice-première ministre prend bonne note de la suggestion de M. Vicaire sur les lanceurs d'alerte, un sujet qui mérite une réflexion plus large;

— sur la conservation indifférenciée des adresses IP, la CJUE a autorisé cette pratique si c'est pour lutter contre les pratiques criminelles graves;

redenen wordt omkleed. De regels voor het voldoen aan die voorwaarden werden strikt omschreven;

— op de vraag of de wet niet opnieuw zal worden vernietigd, antwoordt de minister dat zij hoopt zo goed mogelijk tegemoet te zijn gekomen aan de kritiek en de argumenten van het Grondwettelijk Hof;

— wat de door de heer Freilich aangehaalde kritiek vanwege de GBA betreft, meent de minister dat er gedeeltelijk tegemoet aan werd gekomen en dat voor de overige aspecten uitvoerige argumenten werden verstrekt. Het is niet louter zaak de gegevens te gebruiken met inachtneming van de persoonlijke levenssfeer, maar ook moet rekening worden gehouden met de vereisten qua veiligheid en techniek waarmee de operatoren worden geconfronteerd;

— de minister verduidelijkt dat private en bedrijfsnetwerken onder de toepassing van artikel 9, § 7, van de wet van 13 juni 2005 vallen, dat niet werd gewijzigd. Deze netwerken vallen niet onder het wetsontwerp;

— het wetsontwerp is evenmin van toepassing op de virtuele privénetwerken (VPN) die een beveiligde en gecodeerde verbinding tot stand brengen tussen twee netwerken of tussen een individuele gebruiker en een netwerk, waardoor men anoniem op het internet kan surfen;

— de minister stelt vast dat het feit dat elke lidstaat zijn eigen regelgeving heeft, de zaken niet vergemakkelijkt. Eengemaakte Europese regelgeving zou de voorkeur verdienen, maar de herstelwet duldde geen uitstel, aangezien de wet vernietigd was;

— de operatoren zelf hebben talrijke opmerkingen aangaande de technische haalbaarheid geformuleerd. Die aanpassingen kosten geld en tijd. Dat verklaart de geplande termijn en de overgangsperiode, in het bijzonder voor het ontworpen artikel 126/1;

— inzake netwerkbeveiliging wordt de vraag wie toegang krijgt en hoe nader geregeld door de wet betreffende het statuut van het BIPT. Staatssecretaris Michel kan ter zake meer details verstrekken;

— de vice-eersteminister neemt nota van de door de heer Vicaire geformuleerde suggestie aangaande de klokkenluiders en stelt dat dit thema een bredere denkoefening verdient;

— het HvJ-EU heeft de ongedifferentieerde bewaring van IP-adressen toegelaten, indien het doel ervan de bestrijding van zware criminaliteit is;

— dans le cadre de la lutte contre la fraude, elle prend acte que M. Boukili conteste l'interprétation avancée que la Cour européenne n'aurait pas admis la conservation et l'utilisation des données indifférenciées. Elle précise que la CJUE ne s'est pas prononcée sur le sujet de la lutte contre la fraude. La CJUE ne s'est prononcée qu'en matière pénale. Cependant, elle rappelle que la Cour tient compte des gradations entre l'importance des finalités poursuivies. Dans ce cas, les données dont la conservation est rendue obligatoire par l'article 122, § 4, en projet, à des fins de lutte contre la fraude et des utilisations malveillantes de réseaux, sont déjà conservées par les opérateurs pour d'autres finalités (facturation, marketing, sécurité). La Cour précise que si elles sont déjà conservées, elle peuvent être utilisées pour d'autres finalités plus importantes. La CJUE ne s'est pas prononcée de manière explicite, mais le cadre légal proposé est conforme à la jurisprudence en vigueur, notamment dans les cas de lutte contre la fraude et d'abus de réseaux. La vice-première ministre rappelle que la loi de réparation vise surtout à garantir une durée de conservation uniforme pour l'ensemble des opérateurs;

— sur la question de Me Forget relative aux adresses IP (conservation des adresses IP plutôt que des vraies données d'identification), elle précise que la Cour ne s'est pas prononcée de manière spécifique sur ce sujet. Elle relève que les adresses IP peuvent être utilisées pour le profilage par les opérateurs. Il y a donc une différence qui semble justifiée à ses yeux.

M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice, fait remarquer que, dans ce débat, plusieurs intérêts doivent être mis en balance. Pour M. Freilich, qui insiste pour que l'avis de l'APD soit suivi sans réserve, seule la protection de la vie privée compte visiblement. D'autres intérêts doivent cependant être pris en compte. Le vice-premier ministre cite à cet égard l'avis écrit de l'Association des juges d'instruction:

"Les juges d'instruction sont des juges qui, en ce qui concerne les droits fondamentaux garantis par la constitution et par les conventions internationales, doivent toujours examiner la question de savoir si la violation d'un droit est proportionnelle à l'application d'un autre droit. On parle de droits fondamentaux à raison (avec un "s" à la fin) et on parle de *fundamental rights* (avec un "s" à la fin). Cela signifie que dans chaque cas, il doit être possible de mettre en balance l'atteinte à la vie privée d'une personne avec d'autres intérêts protégés. Ces autres intérêts sont le droit à un procès équitable (à charge et à décharge, […] le droit à la sécurité, le droit à la vie… On oublie trop souvent que pour protéger la vie privée (pensons au *hacking* de plus en plus fréquent,

— wat de fraudebestrijding betreft, neemt de minister nota van het feit dat de heer Boukili de interpretatie betwist dat het HvJ-EU de bewaring en het gebruik van ongedifferentieerde gegevens niet heeft toegelaten. Zij verduidelijkt dat het HvJ-EU zich niet heeft uitgesproken over fraudebestrijding, maar louter over strafrechtelijke materie. Zij wijst er echter op dat het HvJ-EU rekening houdt met de mate waarin de nagestreefde doelen van belang zijn. *In casu* bewaren de operatoren nu al de gegevens die op grond van het ontworpen artikel 122, § 4, verplicht zouden moeten worden bewaard met het oog op de bestrijding van fraude en van het misbruik van netwerken, maar dan om andere doeleinden (facturatie, marketing, veiligheid). Het HvJ-EU geeft aan dat indien die gegevens hoe dan ook worden bewaard, zij mogen worden gebruikt voor belangrijkere doeleinden. Het HvJ-EU heeft geen expliciete uitspraak gedaan, maar de ontworpen wettelijke regeling strookt met de gebruikelijke rechtspraak, in het bijzonder met betrekking tot de bestrijding van fraude en van misbruik van netwerken. De minister herinnert eraan dat de herstelwet vooral bedoeld is om te waarborgen dat voor alle operatoren een eenvormige bewaarduur zou gelden;

— op de vraag van mr. Forget inzake de IP-adressen (bewaring van de IP-adressen, veeleer dan van echte identificatiegegevens), antwoordt de minister dat de gerechtelijke uitspraak ter zake niet specifiek daarop sloeg. Mevrouw De Sutter wijst erop dat de operatoren de IP-adressen kunnen gebruiken voor profilering. Er is dus sprake van een verschil dat haar gerechtvaardigd lijkt.

De heer Vincent Van Quickenborne, vice-eersteminister en minister van Justitie, wijst erop dat in dit debat meerdere belangen tegen elkaar moeten worden afgewogen. Voor de heer Freilich, die erop aandringt dat het advies van de GBA onverkort zou worden gevolgd, is blijkbaar enkel de privacy van tel. Er zijn evenwel andere belangen die in rekening moeten worden gebracht. De vice-eersteminister citeert dienaangaande uit het schriftelijk advies van de Vereniging van Onderzoeksrechters:

"Onderzoeksrechters zijn rechters die ten aanzien van de grondwettelijk en internationaal gewaarborgde grondrechten steeds de afweging moeten maken of de schending van het ene recht in proportie staat tot de bewaking van het andere recht. Men spreekt met een reden over fundamentele rechten (met een "en" op het einde) en men spreekt over *fundamental rights* (met een "s" op het eind). Dat wil zeggen dat in elk dossier de afweging moet kunnen worden gemaakt om heel concreet iemands privacy te schenden ten aanzien van andere beschermde belangen. Die andere belangen zijn het recht op een eerlijk proces (à charge en à décharge […]), het recht op veiligheid, het recht op leven… Men vergeet al te vaak dat ook voor de bescherming van

au *doxing*, […] aux *deep nudes*…) une atteinte à la vie privée est nécessaire pour pouvoir identifier les suspects et mettre fin aux infractions. Cette évaluation devient impossible s'il n'y a plus rien à évaluer".

Le projet de loi à l'examen est le fruit d'une pesée minutieuse des intérêts en présence. Beaucoup de travail y a été consacré. Pour le vice-premier ministre, la longueur de l'avis du Conseil d'État est révélatrice. Il ajoute que le Conseil n'a formulé aucune objection fondamentale au texte en termes de contenu.

L'intervenant précise par ailleurs que le Comité de concertation a approuvé le projet de loi et les amendements respectivement le 22 février et le 13 mai 2022. Il serait incohérent que les partis – qui sont presque tous membres du Comité de concertation – s'opposent soudain aux textes en cette commission.

Aucune alternative n'est non plus proposée. Comment dès lors concilier vie privée et sécurité? Les détracteurs du projet n'apportent aucune réponse.

Le projet de loi à l'examen est basé sur une philosophie fondamentalement différente des lois précédentes. Au lieu d'une conservation générale et indifférenciée des données, la conservation est organisée de manière transparente, selon des critères objectifs, à contrôler annuellement.

D'aucuns prétendent qu'il suffirait de réglementer strictement l'accès aux données et qu'il n'est pas nécessaire d'établir un cadre strict pour la conservation. Ils ont tort; la CJUE exige que l'obligation de conservation soit conforme au principe de proportionnalité.

Mme De Wit a exprimé ses inquiétudes au sujet de l'application du critère statistique. Les critères géographiques ont été proposés par la Cour de justice de l'Union européenne. Leur application à un pays comme la Suède ne permettrait pas de couvrir l'ensemble de son territoire. Cela prouve qu'une approche différenciée est effectivement suivie. Par ailleurs, la Belgique est un petit pays densément peuplé qui comporte de nombreux lieux stratégiques. Le COC a validé cette approche et contrôlera le décompte des chiffres. De plus, des règles ont été convenues pour éviter tout double comptage. Dans son arrêt du 5 avril 2022 (C-140/20), la Cour de justice de l'Union européenne a confirmé que les chiffres moyens de la criminalité pouvaient être utilisés comme critères pour organiser de la conservation de données sur une base géographique. Il se pourrait effectivement que

de privacy zelf (denk aan steeds meer voorkomende hacking, *doxing*, […] deep nudes…) een inbreuk op de privacy nodig is om de verdachten te kunnen identificeren en de misdrijven te laten stoppen. Deze afweging wordt onmogelijk als er niets meer af te wegen zou vallen".

Het voorliggende wetsontwerp is de vrucht van een zorgvuldige belangenafweging. Er is lang en veel aan gewerkt. De lengte van het advies van de Raad van State spreekt boekdelen, aldus de vice-eersteminister, die eraan toevoegt dat de Raad inhoudelijk geen fundamentele bezwaren had bij de tekst.

De spreker wijst er voorts op dat het Overlegcomité op 22 februari en 13 mei 2022 ingestemd heeft met respectievelijk het wetsontwerp en de amendementen. Het zou van weinig consequentie getuigen mochten partijen – ze schuiven nagenoeg allemaal mee aan bij het Overlegcomité – zich in deze commissie plots gaan verzetten tegen de teksten.

Er worden ook geen alternatieven aangedragen. Hoe zouden privacy en veiligheid dan wel met elkaar moeten worden verzoend? De criticasters blijven het antwoord schuldig.

Het voorliggende wetsontwerp is gebaseerd op een fundamenteel andere filosofie dan de voorgaande wetten. In de plaats van een algemene en ongedifferentieerde gegevensbewaring wordt de bewaring georganiseerd op een transparante wijze, volgens objectieve, jaarlijks te controleren criteria.

Sommigen beweren dat het voldoende zou zijn om de toegang tot de gegevens strikt te reguleren en dat er geen nood is aan een strikt kader voor de bewaring. Zij dwalen; het HvJ-EU eist dat de bewaarplicht in overeenstemming is met het evenredigheidsbeginsel.

Mevrouw De Wit uitte haar bezorgdheid over de toepassing van het statistisch criterium. De geografische criteria werden aangereikt door het HvJ-EU. Toegepast op een land als Zweden zou niet het hele grondgebied gedekt zijn. Dit bewijst dat er wel degelijk gedifferentieerd wordt. België is nu eenmaal een klein, dichtbevolkt land met veel strategische plekken. Het COC heeft die aanpak gevalideerd. Dat controleorgaan zal de telling van de cijfers controleren. Er werden regels afgesproken om dubbeltelling te vermijden. In zijn arrest van 5 april 2022 (C-140/20) heeft het HvJ-EU het gebruik van gemiddelde criminaliteitscijfers bevestigd als criterium om op geografische basis retentie te organiseren. Het is inderdaad mogelijk dat op basis van een statistisch criterium het hele grondgebied wordt gedekt door dataretentie. De bewaring is dan wel algemeen, maar niet ongedifferentieerd; er

l'ensemble du territoire soit couvert par de la conservation de données effectuée sur la base d'un critère statistique. S'il est vrai que cette conservation est générale, elle n'est néanmoins pas indifférenciée. En effet, des délais de conservation différents sont applicables selon les différentes zones et données.

La période transitoire de cinq ans, que Mme De Wit et M. Freilich ont évoquée, ne porte que sur la conservation de données effectuée à proximité de lieux stratégiques. Les opérateurs doivent disposer de suffisamment de temps pour l'organiser. Cela prouve que le gouvernement prend au sérieux la concertation avec les opérateurs. D'autres formes de conservation de données, y compris celle effectuée sur une base géographique, seront applicables immédiatement.

Contrairement à ce que semble laisser entendre M. Freilich, une disparition n'est pas toujours remarquée immédiatement, la probabilité qu'elle ne soit remarquée qu'après plusieurs jours étant élevée. Dans ce cas, les données historiques sont importantes et un gel des données en temps réel (*future freeze)* ne suffit pas.

Le vice-premier ministre réfute catégoriquement l'affirmation selon laquelle le projet de loi à l'examen nous ferait entrer dans une société de surveillance orwellienne. Il n'est en effet nullement question de surveillance généralisée, les données ne pouvant être demandées que dans le cadre d'une enquête pénale concrète. Ce ne sera d'ailleurs pas l'État qui conservera les données, mais les opérateurs.

M. Freilich a évoqué en détail les problèmes que rencontreraient, selon lui, les services OTT tels que *Signal* après l'adoption du projet de loi l'examen. Le vice-premier ministre donne lecture de l'avis du Collège des procureurs généraux:

"Le cryptage ne peut pas justifier qu'un opérateur ne puisse pas satisfaire à ses obligations en matière de rétention de données. Cependant, le Collège des procureurs généraux souhaite également rappeler l'arrêt de la Cour de cassation relatif à SKYPE (Cour de cassation, 19 février 2019, P.17 1229.N), dans lequel cette dernière a expressément stipulé qu'un opérateur doit s'organiser d'un point de vue technique pour pouvoir fournir, par voie numérique, conformément aux articles 88*bis* et 90*ter* du Code d'instruction criminelle, des données demandées. […] Le danger pour la vie privée ne découle pas du simple fait que davantage d'opérateurs sont maintenant soudainement tenus d'appliquer la rétention de données, mais bien du fait qu'ils le font déjà d'une façon totalement non contrôlée, généralement sans travailler avec des réquisitoires légitimes des services de recherche. Le projet de loi actuel veut reconnaître – ce qui est d'ailleurs en

gelden immers verschillende bewaringstermijnen voor verschillende zones en gegevens.

De overgangsperiode van vijf jaar, waarnaar werd verwezen door mevrouw De Wit en de heer Freilich, betreft enkel de dataretentie rond strategische plaatsen. De operatoren moeten voldoende tijd krijgen om die te organiseren. Dit bewijst dat de regering het overleg met de operatoren ernstig neemt. Andere vormen van dataretentie, inclusief die op geografische basis, zullen onmiddellijk van toepassing worden.

Anders dan de heer Freilich lijkt te suggereren, is een verdwijningszaak niet steeds een "*live action*". Het is zeer wel mogelijk dat een verdwijning pas na enkele dagen wordt opgemerkt. In dat geval zijn historische data van belang. Een *future freeze* volstaat dan niet.

Dat we met dit wetsontwerp zouden afglijden naar een bigbrotheriaanse maatschappij ontkent de vice-eersteminister ten stelligste. Er is geen sprake van een algemeen toezicht. De data kunnen slechts worden opgevraagd in het kader van een concreet strafrechtelijk onderzoek. Het is overigens niet de overheid die de data bijhoudt, dat doen de operatoren.

De heer Freilich ging uitgebreid in op de problemen die OTT-diensten zoals *Signal* volgens hem zouden ondervinden door het voorliggende wetsontwerp. De vice-eersteminister haalt het advies van het College van procureurs-generaal aan:

"Encryptie mag er niet toe leiden dat een operator niet zou kunnen voldoen aan diens verplichtingen inzake dataretentie. Het College van procureurs-generaal wil echter ook het SKYPE-cassatiearrest (Cass. 19 februari 2019, P.17 1229.N) in herinnering brengen, waarbij het Hof van Cassatie uitdrukkelijk gestipuleerd heeft dat een operator zich technisch moet organiseren dat het de overeenkomstig artikel 88*bis* Sv. en 90*ter* Sv. gevraagde gegevens kan aanleveren via digitale weg. […] Het gevaar voor de privacy komt niet voort uit het luttele feit dat er nu plots meer operatoren verplicht zouden zijn tot het bijhouden van gegevens, maar wel dat zij dit nu reeds doen op een geheel ongecontroleerde wijze, veelal zonder mee te werken met rechtmatige vorderingen van de opsporingsdiensten. Huidig wetsontwerp wil – overigens geheel in lijn met de cassatierechtspraak in de zaken YAHOO en SKYPE – deze maatschappelijke realiteit

conformité complète avec la jurisprudence de la Cour de cassation dans les affaires YAHOO et SKYPE – cette réalité sociale et, par conséquent, mettre en place, en toute transparence, une concurrence équitable entre les opérateurs classiques et les nombreux acteurs numériques actifs d'un nouveau type."

À l'heure actuelle, les fournisseurs de services OTT décident de coopérer ou non avec la justice et, dans l'affirmative, de la forme que prendra cette coopération. Par exemple, l'entreprise Apple ne coopère qu'en cas de risque de suicide. L'entreprise transmet alors des données qu'elle conserve durant quarante jours. Mais elle choisit de ne pas coopérer dans les affaires liées au crime organisé. Les entreprises Meta et Twitter coopèrent quant à elles dans les dossiers de terrorisme, mais pas dans les dossiers d'espionnage.

Il n'est nullement question d'interdire les services OTT ou leurs fournisseurs. Seules les données générées ou traitées par les opérateurs devront être conservées dans le cadre de la lutte contre la criminalité grave. Le projet de loi l'examen, ainsi que la modification de la notion d' "opérateur" au travers de la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électronique, rappellent que des règles similaires sont applicables à tous les opérateurs, qu'ils fournissent des services classiques ou OTT, gratuits ou payants.

Le vice-premier ministre donne lecture d'un extrait de la politique de respect de la vie privée de Signal: "Les seules données collectées sont les données "Infos Contact", qui correspondent au numéro de téléphone. […] L'entreprise a été développée de telle sorte qu'elle ne collecte ou ne conserve jamais la moindre information sensible. Tous les messages et les appels transitant par l'application sont totalement cryptés, ce qui signifie qu'aucun tiers, pas même l'entreprise elle-même, ne peut y accéder. […] Toute autre information ajoutée au compte, comme les noms et photos de profil, est totalement cryptée. L'entreprise n'enregistre pas vos messages ou toute autre information au sujet de vos appels sur ses serveurs. Toutefois, elle met en file d'attente, sur ses serveurs, les messages totalement cryptés qui doivent être délivrés à des appareils qui sont temporairement hors ligne.". (traduction)

Si cela implique que l'entreprise Signal ne traite ou ne génère aucune métadonnée, aucune modification ne devra être apportée à ses systèmes.

Le gouvernement entend instaurer des règles communes à l'ensemble des opérateurs qui proposent des services en Belgique. La définition utilisée de la notion

erkennen en derhalve in alle transparantie een gelijk speelveld creëren tussen de conventionele operatoren en de talloze nieuwsoortige digitale spelers die actief zijn".

Vandaag beslissen aanbieders van OTT-diensten of ze zullen meewerken met het gerecht en zo ja op welke manier. Zo werkt *Apple* enkel mee als er zelfmoordrisico bestaat. Het maakt dan gegevens over die het gedurende 40 dagen bewaart. Het kiest ervoor niet mee te werken in gevallen van georganiseerde misdaad. *Meta* en *Twitter* werken mee in zaken van terrorisme maar niet bij spionage.

Er is geen sprake van om OTT-diensten of de aanbieders daarvan te verbieden. Enkel de gegevens die door de operator gegenereerd of verwerkt worden, moeten bewaard worden in het kader van de strijd tegen de zware criminaliteit. Dit wetsontwerp, alsook de wijziging van het begrip "operator" door de wet van 21 december 2021 "houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie", herinneren aan het feit dat soortgelijke spelregels gelden voor alle operatoren, conventioneel of OTT, gratis of betalend.

De vice-eersteminister citeert uit het privacybeleid van *Signal*: "*the only data that is collected is "Contact Info", which is the phone number. (…) The company is designed to never collect or store any sensitive information. All messages and calls on the app are end-to-end encrypted, meaning no third-party, nor the company itself can access them. (…) Other information added to the account such as profile name and picture is end-to-end encrypted. The company does not store your messages or any information about your calls on its servers. However, it does queue "end-to-end encrypted messages on its servers for delivery to devices that are temporarily offline.*"

Als dat impliceert dat *Signal* geen metadata verwerkt of genereert, dient het niets te wijzigen aan zijn systemen.

De regering beoogt een *level playing field* voor alle operatoren die diensten aanbieden in België. De gehanteerde definitie van "operator" is volledig in overeenstemming

d'"opérateur" est totalement conforme au droit européen. L'IBPT se concertera avec les fournisseurs de services OTT pour évaluer s'ils respectent la législation qui leur est applicable.

Une connexion VPN permet à l'utilisateur de cacher son adresse IP, ce qui est toutefois différent de la navigation privée. Les connexions VPN ne sont pas interdites. Il peut être nécessaire de conserver l'adresse IP source. Si cette adresse mène à un fournisseur de connexion VPN, les autorités judiciaires pourront lui adresser leur réquisition.

La loi belge sur la conservation des données ayant été annulée, notre pays ne peut se permettre d'attendre une initiative législative européenne. Il est clair que les autorités européennes suivent de près l'évolution de la situation en Belgique.

L'article concernant la conservation ciblée sur une base géographique (article 9 du projet de loi) offre une solution pour le cas où des durées de conservation différentes s'appliqueraient aux mêmes données. La règle générale est que, dans ce cas, les opérateurs conservent les données pendant la durée la plus courte (cf. l'article 126/1, § 4, alinéa 8, en projet de la loi télécom).

Il a été demandé comment des fournisseurs tels que Facebook et WhatsApp doivent, en pratique, appliquer la réglementation à l'examen. Le vice-premier ministre souligne qu'ils disposent des données nécessaires; ils en tirent de l'argent. Comme il a été mentionné, le projet de loi vise des données qui existent déjà, c'est-à-dire les données générées ou traitées par les opérateurs. Le projet de loi ne leur demande pas de créer des données supplémentaires. Néanmoins, les fournisseurs de services OTT conservent beaucoup plus de données que celles demandées par la justice. Tant l'Association des juges d'instruction que le Collège des procureurs généraux estiment qu'il est nécessaire que tous les opérateurs, y compris les fournisseurs de services OTT, coopèrent avec la justice.

M. Vicaire s'est interrogé quant au fait que l'ensemble du territoire puisse être couvert par la conservation des données visée par l'article 126/1 en projet de la loi télécom. Le vice-premier ministre souligne que, conformément au paragraphe 6, le gouvernement soumettra un rapport d'évaluation annuel sur l'application de cet article à la Chambre des représentants. Ce rapport comprendra, entre autres, le pourcentage du territoire national soumis à l'obligation de conservation des données en vertu de l'article. La transparence est également assurée par la publication annuelle d'un arrêté ministériel établissant la liste des zones géographiques soumises à l'obligation

met het Europese recht. Het BIPT zal in gesprek gaan met de aanbieders van OTT-diensten om te evalueren of ze de relevante wetgeving naleven.

Een VPN-verbinding stelt de gebruiker in staat zijn IP-adres te verhullen. Dit is evenwel niet hetzelfde als anoniem surfen. VPN-verbindingen zijn niet verboden. Het kan nodig zijn om het bron-IP-adres te bewaren; als dat leidt naar een VPN-provider, zal het gerecht zijn vordering aan die laatste kunnen richten.

Aangezien de Belgische dataretentiewet vernietigd werd, kan ons land het zich niet veroorloven te wachten op een Europees wetgevend initiatief. Het is duidelijk dat de Europese autoriteiten de ontwikkelingen in België op de voet volgen.

In het artikel over de gerichte bewaring op geografische basis (artikel 9 van het wetsontwerp) wordt een oplossing aangereikt voor het geval dat verschillende bewaartermijnen zouden gelden voor dezelfde gegevens. De algemene regel is dat de operatoren in dergelijk geval de gegevens gedurende de kortste termijn bewaren (cf. het ontworpen artikel 126/1, § 4, achtste lid, van de telecomwet).

De vraag werd gesteld hoe aanbieders als *Facebook* en *WhatsApp* de voorliggende regeling praktisch moeten aanpakken. De vice-eersteminister wijst erop dat zij over de nodige data beschikken; ze verdienen er geld mee. Zoals gezegd viseert het wetsontwerp data die reeds bestaan, dat wil zeggen gegevens die door de operatoren gegenereerd of verwerkt worden. Het wetsontwerp verlangt niet dat zij bijkomende data zouden aanmaken. Niettemin houden de aanbieders van OTT-diensten veel meer gegevens bij dan gevraagd door justitie. Zowel de Vereniging van Onderzoeksrechters als het College van procureurs-generaal achten het nodig dat alle operatoren, inclusief de aanbieders van OTT-diensten, met het gerecht meewerken.

De heer Vicaire plaatste kanttekeningen bij het feit dat het ganse grondgebied gedekt kan zijn door gegevensbewaring bedoeld in het ontworpen artikel 126/1 van de telecomwet. De vice-eersteminister wijst erop dat de regering krachtens paragraaf 6 jaarlijks een evaluatieverslag omtrent de toepassing van dit artikel zal bezorgen aan de Kamer van volksvertegenwoordigers. Dat verslag bevat onder meer het percentage van het nationale grondgebied waarvoor de verplichting tot gegevensbewaring op basis van dat artikel van toepassing is. De transparantie wordt ook verzekerd door de jaarlijkse publicatie van een ministerieel besluit waarin

de conservation des données, ainsi que leur durée de conservation.

En ce qui concerne la protection des lanceurs d'alerte, le vice-premier ministre souligne qu'il n'existe aucune base juridique pour demander des données aux opérateurs afin de retrouver un lanceur d'alerte. Une distinction doit être opérée entre la conservation des données et l'utilisation des données conservées. Il en va de même pour les journalistes, les avocats et les médecins.

M. Gilissen a commenté la définition, à son avis très large, des zones stratégiques. Le vice-premier ministre répond qu'il sera fait appel à l'expertise de l'Institut géographique national (IGN), qui délimitera les périmètres. L'IGN transmettra ensuite ses données à la NTSU de la police fédérale, qui établira la carte. Elle sera ensuite contrôlée par le COC.

Il n'y a pas de violation du principe d'égalité, comme le suggère M. Gilissen. Les citoyens vivant dans une zone similaire seront traités de la même manière. L'égalité de traitement est assurée par l'utilisation de critères objectifs et statistiques.

À l'attention de M. Boukili, le vice-premier ministre répète que le projet de loi à l'examen n'apporte aucune modification à la notion d"opérateur". La définition de cette notion a été modifiée par la loi du 21 décembre 2021 précitée, qui a également modifié la notion de "service de communications électroniques" pour y inclure les services OTT. Le vice-premier ministre souligne que l'anonymat n'est pas un droit garanti par le RGPD ni par la Charte des droits fondamentaux de l'Union européenne. La liberté d'expression est bien sûr garantie, mais celui qui l'utilise doit en assumer la responsabilité. L'anonymat va à l'encontre du principe essentiel selon lequel il appartient à chacun de répondre de ses actes, tant sur le plan civil que pénal.

En ce qui concerne la protection des données à caractère personnel, la directive police-justice[1] prévoit déjà une limitation du droit de certaines personnes à

[1] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, wordt vastgesteld.

Wat de bescherming van klokkenluiders betreft, geeft de vice-eersteminister aan dat er geen enkele juridische basis is om gegevens op te vragen bij operatoren om een klokkenluider op te sporen. Er dient een onderscheid te worden gemaakt tussen de bewaring van de gegevens en het gebruik van de bewaarde gegevens. Hetzelfde geldt voor journalisten, advocaten en artsen.

De heer Gilissen maakte een opmerking omtrent de, naar zijn mening erg brede, omschrijving van de strategische zones. De vice-eersteminister antwoordt dat er een beroep zal worden gedaan op de expertise van het Nationaal Geografisch Instituut (NGI), dat de perimeters zal afbakenen. Het NGI zal zijn input vervolgens bezorgen aan de NTSU van de Federale Politie, die de kaart zal opstellen. Die wordt dan vervolgens gecontroleerd door het COC.

Er is geen sprake van een schending van het gelijkheidsbeginsel, zoals geopperd door de heer Gilissen. Burgers die in een gelijkaardige zone wonen, zullen op eenzelfde manier worden behandeld. Die gelijke behandeling wordt verzekerd door het gebruik van objectieve, statistische criteria.

Ter attentie van de heer Boukili herhaalt de vice-eersteminister dat het voorliggende wetsontwerp geen wijzigingen aanbrengt aan het begrip "operator". De definitie van dat begrip werd hervormd door de reeds aangehaalde wet van 21 december 2021, die eveneens het begrip "elektronische-communicatiedienst" aanpaste zodat daar ook OTT-diensten onder vallen. De spreker wijst erop dat anonimiteit geen recht is dat gewaarborgd wordt door de AVG noch door het Handvest van de Grondrechten van de Europese Unie. De vrijheid van meningsuiting is vanzelfsprekend gewaarborgd, maar wie zich daarvan bedient moet er de verantwoordelijkheid voor dragen. De anonimiteit druist in tegen het essentiële principe dat een persoon steeds verantwoording moet afleggen voor zijn daden, zowel op burgerrechtelijk als op strafrechtelijk vlak.

Wat de bescherming van persoonsgegevens betreft, voorziet de zogenaamde richtlijn politie-justitie[1] reeds in een beperking van het recht van bepaalde personen voor

[1] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

quelques fins clairement définies. La Cour constitutionnelle a confirmé ce point de vue dans son arrêt n° 158/2021 du 18 novembre 2021: “La simple collecte de données d’identification de tous les utilisateurs finaux d’un réseau de communications électroniques ne saurait justifier la crainte, dans un État de droit démocratique, que toutes les communications menées sur ce réseau seront supervisées par les pouvoirs publics. La loi attaquée ne saurait dès lors avoir pour effet, par elle-même, de dissuader des personnes d’exprimer leur opinion ou de partager des informations avec des journalistes ou avec des personnalités politiques.”

M. Boukili se disait préoccupé par le fait que le critère statistique pourrait entraîner une conservation générale des données et estimait par ailleurs que le système tel qu’il est conçu manque de transparence. Le vice-premier ministre n’est pas de cet avis. Le critère choisi est objectif et le système est proportionné. Ces éléments sont indépendants du taux de couverture, qui est évolutif. Le droit européen n’exige pas d’atteindre un taux de couverture prédéterminé. La CJUE exige en revanche de l’objectivité et de la proportionnalité. Appliqué à d’autres États membres, le critère statistique donnerait des résultats différents. La Belgique est un petit pays densément peuplé, avec de nombreuses frontières et un trafic de transit important.

Le vice-premier ministre donne lecture du paragraphe 80 de l’arrêt du 5 avril 2022 de la CJUE (C-140/20):

“Il convient de souligner que, selon cette jurisprudence, les autorités nationales compétentes peuvent prendre, pour les zones visées au point précédent, une mesure de conservation ciblée fondée sur un critère géographique, tel que notamment le taux moyen de criminalité dans une zone géographique, sans qu’elles disposent nécessairement d’indices concrets portant sur la préparation ou la commission, dans les zones concernées, d’actes de criminalité grave. Dans la mesure où une conservation ciblée fondée sur un tel critère est susceptible de toucher, en fonction des infractions pénales graves visées et de la situation propre aux États membres respectifs, à la fois des lieux caractérisés par un nombre élevé d’actes de criminalité grave et des lieux particulièrement exposés à la commission de tels actes, elle n’est, en principe, pas davantage de nature à donner lieu à des discriminations, le critère tiré du taux moyen de criminalité grave ne présentant, en soi, aucun lien avec des éléments potentiellement discriminatoires.”

La CJUE ne définit pas la notion de “criminalité grave”. Pour les mesures d’investigation les plus intrusives, la proportionnalité est garantie par l’utilisation de la liste des infractions contenue à l’article 90*ter* du Code d’instruction criminelle. Dans son avis sur l’avant-projet de

enkele welomschreven doeleinden. Het Grondwettelijk Hof bevestigt deze zienswijze in zijn arrest nr. 158/2021 van 18 november 2021: “[d]e loutere verzameling van identificatiegegevens van alle eindgebruikers van een elektronische-communicatienetwerk kan in een democratische rechtsstaat niet de vrees rechtvaardigen dat alle communicatie over dat netwerk door de overheid zal worden gemonitord. De bestreden wet kan er bijgevolg op zich niet toe leiden dat personen worden ontmoedigd om hun mening te uiten of om informatie te delen met journalisten of politici”.

De heer Boukili sprak de bezorgdheid uit dat het statistisch criterium zou uitmonden in een algemene gegevensbewaring en achtte het ontworpen systeem onvoldoende transparant. De vice-eersteminister is het daarmee niet eens. Het gekozen criterium is objectief en de regeling proportioneel. Een en ander staat los van het percentage van de dekking, dat evolutief is. Het Europees recht verlangt niet dat men een voorafgaandelijk vastgesteld dekkingspercentage bereikt. Het HvJ-EU verlangt objectiviteit en proportionaliteit. Toegepast op andere lidstaten zou het statistisch criterium andere resultaten geven. België is een klein, dichtbevolkt land met veel grenzen en dito transitverkeer.

De vice-eersteminister geeft lezing van paragraaf 80 van het arrest van 5 april 2022 van het HvJ-EU (C-140/20):

“Benadrukt moet worden dat de bevoegde nationale autoriteiten volgens deze rechtspraak voor de in het vorige punt genoemde plekken een gerichte bewaringsmaatregel kunnen nemen op basis van een geografisch criterium, zoals met name het gemiddelde criminaliteitscijfer in een geografische zone, zonder noodzakelijkerwijs concrete aanwijzingen te hebben dat er in die zones zware misdaden worden voorbereid of gepleegd. Voor zover met een op een geografisch criterium gebaseerde gerichte bewaringsmaatregel, afhankelijk van de zware strafbare feiten in kwestie en de situatie in de respectieve lidstaten, kan worden gemikt op zowel plekken waar veel zware strafbare feiten worden gepleegd als plekken waar daar een verhoogd risico op bestaat, kan een dergelijke maatregel in beginsel evenmin aanleiding geven tot discriminatie. Als criterium is het gemiddelde zwarecriminaliteitscijfer op zich immers niet discriminerend.”

Het HvJ-EU definieert het begrip “zware criminaliteit” niet. Voor de meest indringende onderzoeksmaatregelen wordt de proportionaliteit gewaarborgd door het gebruik van de lijst van misdrijven in artikel 90*ter* Sv. In zijn advies omtrent het voorontwerp van wet oordeelde het COC

loi, le COC avait indiqué que "[l]adite "liste des écoutes" de l'art. 90*ter* C.i.cr. est, *de lege lata*, en droit belge, le seul véritable critère utilisable pour pouvoir différencier lesdits "délits graves" de la "criminalité ordinaire"."

M. Boukili a évoqué l'exemple des Pays-Bas. Le vice-premier ministre répond que la loi néerlandaise a été annulée et qu'elle doit être réparée.

En attendant la réparation de la loi belge, les opérateurs continuent de coopérer avec l'appareil judiciaire. Les conclusions auxquelles aboutit M. Boukili sur ce point sont donc inexactes.

Selon le vice-premier ministre, l'étude allemande citée par le même intervenant est dépassée. Elle date de 2011 et porte sur des données de 2007 à 2009, une époque où les médias sociaux n'existaient pas encore ou à peine. Comme l'indique l'Association des juges d'instruction dans son avis écrit, il est impossible, dans une société de plus en plus numérique, de passer à côté de la conservation des données. Il ressort des avis de la police locale et fédérale que leurs services ont recours à l'exploitation de métadonnées dans plus de 90 % des enquêtes. Si l'utilisation de ces données n'était plus autorisée, ces affaires risqueraient d'être classées sans suite.

M. Geens a abordé la question du cryptage. Il est vrai que la recommandation de la Commission d'enquête parlementaire Attentats visant à rendre possible l'accès au contenu des communications cryptées n'a pas encore été mise en œuvre. De nombreux pays sont confrontés à ce problème. La Belgique veut jouer un rôle de pionnier dans ce domaine et s'efforce de trouver une solution technique permettant d'établir cet accès sans compromettre l'essence des applications concernées. Dans ce contexte, le vice-premier ministre renvoie également à la proposition de règlement en matière de protection des enfants contre les abus commis en ligne, publiée par la Commission européenne le 11 mai 2022 (COM(2022) 209 final). Cette proposition vise à inciter les opérateurs à lutter contre la maltraitance des enfants qui se fait par le biais de *chats* cryptés.

L'arrêt *Ministerio Fiscal* (C-207/16) de la CJUE se limite aux circonstances de l'affaire, qui concernait des adresses IP. Le gouvernement estime que d'autres données d'identification peuvent également être conservées, non seulement à des fins judiciaires mais aussi pour lutter contre la fraude et les utilisations malveillantes du réseau. Les données qui devraient être rendues accessibles aux autorités judiciaires sont les mêmes que celles qui sont conservées à d'autres fins. Le projet de loi désigne ces données, ce qui est nécessaire pour des raisons de transparence. Dès que des données devront

dat "[d]e zgn. "taplijst" van art. 90*ter* Sv. [] *de lege lata* naar Belgische recht het enige echt bruikbare criterium [is] om zgn. "zware misdrijven" te kunnen onderscheiden van "gewone criminaliteit"."

De heer Boukili verwees naar het Nederlandse voorbeeld. De vice-eersteminister repliceert dat de Nederlandse wet vernietigd is en dient hersteld te worden.

In afwachting van de reparatie van de Belgische wet blijven de operatoren samenwerken met het gerechtelijk apparaat. De conclusies waartoe de heer Boukili op dit punt komt, zijn dus inaccuraat.

Volgens de vice-eersteminister is de door hetzelfde lid aangehaalde Duitse studie achterhaald. Ze dateert uit 2011 en heeft betrekking op gegevens uit de periode van 2007 tot 2009, toen er nog geen of amper sociale media bestonden. Zoals aangegeven door de Vereniging van Onderzoeksrechters in haar schriftelijk advies, kan men in een steeds digitalere maatschappij niet voorbij aan gegevensbewaring. De adviezen van de Lokale en Federale Politie laten zien dat in meer dan 90 % van de onderzoeken een beroep wordt gedaan op metadata. Als die data niet meer zouden mogen gebruikt worden, dreigen die zaken geseponeerd te worden.

De heer Geens sneed het thema van de encryptie aan. Het klopt dat de aanbeveling van de parlementaire onderzoekscommissie Aanslagen, om toegang mogelijk te maken tot de inhoud van geëncrypteerde communicatie, nog niet werd uitgevoerd. Vele landen lopen aan tegen deze problematiek. België wil ter zake een voortrekkersrol opnemen en trachten een technische oplossing aan te dragen die toegang mogelijk maakt zonder het wezen van deze applicaties op de helling te zetten. In dit verband verwijst de vice-eersteminister nog naar het voorstel van verordening inzake het voorkomen van kindermisbruik, dat de Europese Commissie op 11 mei 2022 heeft gepubliceerd (COM (2022) 229 final). Het voorstel beoogt operatoren aan te sporen om kindermisbruik via geëncrypteerde chats tegen te gaan.

Het arrest *Ministerio Fiscal* (C-207/16) van het HvJ-EU is beperkt tot de omstandigheden van het geval, dat betrekking had op IP-adressen. De regering is van oordeel dat ook andere identificatiegegevens kunnen worden bewaard, niet enkel voor justitiële doeleinden maar ook ter bestrijding van fraude en kwaadwillig gebruik van het netwerk. De gegevens die voor het gerecht moeten beschikbaar worden gemaakt zijn dezelfde als degene die voor andere finaliteiten worden bewaard. Het wetsontwerp benoemt die gegevens. Dit is nodig ter wille van de transparantie. Zodra gegevens moeten

être conservées sur la base de critères énumérés dans la loi télécom et dans les différentes lois organiques, le législateur indiquera quelles sont ces données. Étant donné que les données seront conservées par les autorités sur la base de critères géographiques, il ne pourra être question de conservation générale et indifférenciée de données.

4. ***Répliques***

Selon *Mme Sophie De Wit (N-VA),* tout le monde comprend que la conservation de données puisse être très utile dans certaines affaires, mais nous ne pouvons pas fermer les yeux sur les risques inhérents à cet instrument. Elle estime qu'il relève de sa mission de députée d'exprimer ses préoccupations à ce sujet.

Elle ne conteste pas que des intérêts autres que la protection de la vie privée soient en jeu. C'est là que réside précisément cet exercice extrêmement difficile de mise en balance. La protection de la vie privée n'en est pas moins essentielle. Son rôle de parlementaire est également d'assurer la défense de ce principe.

Mme De Wit est frappée de constater que la discussion se concentre sur la conservation de données à des fins judiciaires. Les données sont cependant bel et bien conservées et la question se pose de savoir à quelles autres fins ces données pourront être utilisées. Les préoccupations exprimées sont d'autant plus légitimes et logiques que c'est la troisième fois que ce débat est mené.

Dans ce débat, l'accent est mis sur plusieurs exemples concrets à propos desquels rares sont ceux qui contesteront que la protection de la vie privée doit pouvoir céder le pas à la sécurité et à la découverte de la vérité: terrorisme, enfant disparu, etc. Le projet de loi contient toutefois également un autre volet qui confie une très grande responsabilité aux opérateurs. Ces derniers seront par exemple censés prendre des mesures appropriées, proportionnées, préventives et curatives de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services, sans prendre connaissance du contenu de la communication. Le Roi pourra préciser les mesures à prendre (*cf.* article 121/8, § 1er, en projet, de la loi télécom; article 4 du projet de loi). En outre, aux termes de l'article 5 du projet de loi, les opérateurs pourront également conserver d'autres données. Le projet de loi délimite à peine la marge d'appréciation des opérateurs dans son exposé des motifs, qui est pourtant détaillé. Quelles seront les mesures justifiées? Sur quelle base et avec quels instruments les opérateurs devront-ils exercer ces pouvoirs? Ces points ne sont pas suffisamment abordés dans ce débat, ce qui inquiète beaucoup Mme De Wit. Il ne faudrait pas que

worden bewaard op basis van criteria die zijn opgesomd in de telecomwet en de diverse organieke wetten, geeft de wetgever aan welke die gegevens zijn. Doordat er voor de autoriteiten bewaard wordt op grond van geografische criteria, is er geen sprake van een algemene en ongedifferentieerde dataretentie.

4. ***Replieken***

Volgens *mevrouw Sophie De Wit (N-VA)* beseft eenieder dat dataretentie in bepaalde zaken erg nuttig kan zijn, maar mogen we niet blind zijn voor de inherente risico's van dit instrument. Ze acht het haar taak als volksvertegenwoordiger om haar bezorgdheden daarover te uiten.

Zij betwist niet dat er andere belangen dan privacy op het spel staan. Dat is precies de uiterst moeilijke afweging die moet worden gemaakt. Maar dat belet niet dat privacy essentieel is; de verdediging van dat beginsel opnemen beschouwt de spreekster evenzeer als haar rol als parlementslid.

Het valt mevrouw De Wit op dat de discussie zich toespitst op de gegevensbewaring voor justitiële doeleinden. Ondertussen worden de data wel bewaard en stelt zich de vraag voor welke andere doeleinden die allemaal kunnen worden aangewend. De bezorgdheden daarover zijn legitiem en logisch, niet het minst in het licht van het feit dat het reeds de derde keer is dat deze oefening wordt gemaakt.

Er wordt in dit debat gefocust op een aantal concrete voorbeelden waarbij weinigen zullen betwisten dat privacy het moet kunnen afleggen tegen veiligheid en waarheidsvinding: terrorisme, een verdwenen kind enzovoort. Maar het wetsontwerp bevat ook een ander onderdeel, één waarbij een zeer grote verantwoordelijkheid bij de operatoren wordt gelegd. Zo wordt er van hen verwacht dat zij, zonder kennis te nemen van de inhoud van de communicatie, de gepaste, evenredige, preventieve en curatieve maatregelen nemen om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen. De Koning kan de te treffen maatregelen preciseren (cf. het ontworpen artikel 121/8, § 1, van de telecomwet; artikel 4 van het wetsontwerp). Daarnaast mogen zij, volgens artikel 5 van het wetsontwerp, ook nog andere gegevens bewaren. Ondanks de uitgebreide toelichting wordt de beoordelingsbevoegdheid van de operatoren op voornoemde punten amper omkaderd in het wetsontwerp. Welke maatregelen zijn gerechtvaardigd? Op welke basis en met welke instrumenten moeten de operatoren deze bevoegdheden uitoefenen? Deze aspecten komen onvoldoende aan bod in dit debat. Een en ander stemt mevrouw De Wit tot grote ongerustheid.

cet autre volet du projet de loi soit oblitéré par le souhait largement partagé – certainement aussi par la N-VA – de doter le pouvoir judiciaire des instruments nécessaires pour mener ses enquêtes à bien.

En ce qui concerne les zones géographiques, Mme De Wit ne conteste nullement que le gouvernement s'appuie en l'espèce sur les lignes directrices fournies par la Cour de justice de l'Union européenne. Le régime en projet est particulièrement complexe sur ce point. Le fait que cela pourrait avoir pour effet de couvrir l'ensemble du pays n'est pas le problème principal. Selon l'intervenante, il importe surtout de savoir si ces éléments pourront être déterminés correctement au moyen de données correctes. Sinon, nous risquons de nous trouver dans une situation de conservation données non différenciée qui nous ramènera à la case départ. Nous devons être sûrs des critères, des statistiques et des interprétations qui seront utilisés.

M. Nabil Boukili (PVDA-PTB) regrette que les réponses apportées amènent encore plus de questions. Il souligne que la vice-première ministre a avancé qu'il n'y a pas de preuve de l'efficacité du système. Si c'est le cas, il estime que le texte est contraire à l'article 8 de la Convention européenne des droits de l'homme. Celui-ci précise le droit au respect de la vie privée et familiale, interdisant l'ingérence de l'autorité publique dans l'exercice de ce droit, sauf si elle est prévue par la loi et si elle répond à des conditions strictes. Il estime que si la preuve ne peut être apportée, il se demande en quoi le projet de loi est proportionné et si les règles de protection de la vie privée sont respectées.

L'intervenant revient ensuite sur l'article 127, en projet, et la mise à disposition des données aux autorités de police. Selon lui, la CJUE conteste ce principe et l'exclut en matière de criminalité grave: le risque que cela soit refusé pour la fraude est élevé.

Sur la question de la proportion du territoire concerné, le ministre indique que ce sera ciblé et jugé ultérieurement. M. Boukili souhaiterait savoir ce que cela représente afin d'en vérifier la proportionnalité.

Sur la question de l'anonymat, il rappelle qu'il s'agit d'une condition indispensable qui permet d'exercer des droits fondamentaux (respect de la vie privée et liberté d'expression). Il s'inquiète pour le cas des lanceurs

Het mag niet zo zijn dat dit andere onderdeel van het wetsontwerp ondergesneeuwd geraakt door de breed gedragen bekommering – zeker ook door de N-VA – om justitie de nodige instrumenten te geven om onderzoeken tot een goed einde te kunnen brengen.

Wat de geografische zones betreft, betwist mevrouw De Wit geenszins dat de regering dienaangaande gebruikmaakt van de door het HvJ-EU aangereikte kapstokken. De ontworpen regeling is op dit punt bijzonder complex. Dat hierdoor mogelijk het hele land gedekt kan zijn, is als zodanig niet het probleem. Voor de spreekster is het vooral belangrijk te weten of dit op een correcte wijze zal vastgesteld kunnen worden, aan de hand van de juiste gegevens. Zo niet bestaat het risico dat we opnieuw in een situatie van ongedifferentieerde gegevensbewaring verzeild geraken, waardoor we dus terug bij af zullen zijn. We moeten zeker kunnen zijn van de gebruikte criteria, statistieken en interpretaties.

De heer Nabil Boukili (PVDA-PTB) betreurt dat de verstrekte antwoorden nog meer vragen oproepen. Hij benadrukt dat de vice-eersteminister heeft gesteld dat de doeltreffendheid van de regeling niet is bewezen. In dat geval is het wetsontwerp volgens de spreker in strijd met artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Daarin wordt het recht op de eerbiediging van het privéleven gewaarborgd via een verbod voor de overheid om zich te mengen met de uitoefening van dat recht, behalve wanneer zulks is toegelaten op grond van een wet en onder strikte voorwaarden. De heer Boukili vraagt zich af in hoeverre het wetsontwerp het evenredigheidsbeginsel en de regels inzake bescherming van de persoonlijke levenssfeer in acht neemt, als het bewijs ter zake niet kan worden geleverd.

De spreker komt vervolgens terug op het ontworpen artikel 127 en op de terbeschikkingstelling van de gegevens aan de politie. Volgens hem wordt dat beginsel door het HvJ-EU betwist en uitgesloten met betrekking tot zware misdaad; er bestaat dus een grote kans op een weigering met betrekking tot fraude.

De omvang van het betrokken gebied is volgens de minister een aspect dat later zal worden aangepakt en beoordeeld. De heer Boukili zou willen weten wat dat betekent, teneinde de evenredigheid ervan te kunnen nagaan.

Anonimiteit is volgens de heer Boukili een onontbeerlijke voorwaarde voor de uitoefening van de grondrechten (inachtneming van de persoonlijke levenssfeer en vrijheid van meningsuiting). De spreker maakt zich

d'alerte ou des journalistes. Pour l'intervenant, cet anonymat est remis en question par le projet de loi.

Sur la conservation ciblée, il estime que le projet de loi ne cible pas suffisamment, amenant à une surveillance généralisée.

Sur l'article 90*ter* C.i.cr., il rappelle que c'est le juge d'instruction qui prend l'initiative. Or, dans le projet de loi, le juge n'est pas présent. Il ne s'agit de surcroît jamais de mesures non ciblées.

Sur le classement sans suite, il rappelle que le Collège des procureurs généraux a affirmé avoir les informations mais ne dispose pas de suffisamment de moyens. M. Boukili suggère que c'est dû à l'arriéré judiciaire.

M. Denis Ducarme (MR) rappelle qu'il s'agit d'une loi réparatrice: c'est une nécessité pour protéger la société de menaces, comme récemment avec les attentats islamistes. Ce texte est sur la table pour adapter la loi en tenant compte des menaces qui pèsent aujourd'hui sur la société. Il invite à relire les conclusions de la commission d'enquête parlementaire *Attentats* qui a permis d'identifier les faiblesses de l'État.

Mme Sophie De Wit (N-VA) indique que les articles 4 à 6 du projet de loi énumèrent les données que les opérateurs doivent conserver. Ces derniers peuvent y ajouter certaines données. La liste des autorités qui pourront avoir recours à ces données figure à l'article 127/1, § 2, en projet. Il s'agit d'une longue liste qui pourra toutefois encore être allongée. Si certaines des autorités énumérées semblent évidentes (par exemple celles visées aux 1° à 3° et 6°), la mention d'autres autorités fait froncer les sourcils. Le 7° renvoie par exemple aux "autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale". Presque toutes les administrations en dehors de la justice peuvent être visées. On peut également s'interroger sur l'inclusion dans cette liste des "autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques" (10°). La liste concrète figure dans une circulaire. Or, cet instrument n'offre que de très peu de garanties.

zorgen om de klokkenluiders en de journalisten, want hun anonimiteit komt volgens hem door dit wetsontwerp op de helling te staan.

Wat de gerichte bewaring betreft, meent hij dat de in het wetsontwerp opgenomen gerichtheid ontoereikend is en tot veralgemeend toezicht zal leiden.

Wat artikel 90*ter* van het Wetboek van strafvordering betreft, wijst hij erop dat het initiatief wordt genomen door de onderzoeksrechter. De rechter wordt echter niet vermeld in het wetsontwerp. Bovendien gaat het nooit om niet-gerichte maatregelen.

Wat de seponering betreft, wijst de spreker erop dat het College van procureurs-generaal heeft verklaard wel te beschikken over de informatie, maar niet over toereikende middelen. Zulks is volgens de heer Boukili te wijten aan de gerechtelijke achterstand.

De heer Denis Ducarme (MR) brengt in herinnering dat het de bedoeling is een herstelwet aan te nemen. Dat is nodig om de samenleving te beschermen tegen bedreigingen, zoals de recente aanslagen door islamisten. Het voorliggende wetsontwerp strekt ertoe de wet aan te passen, rekening houdend met de bedreigingen waarmee de samenleving thans te maken heeft. De spreker spoort aan de conclusies van de parlementaire onderzoekscommissie "Aanslagen" te herlezen, want daarin worden de zwakke punten van het bestel beschreven.

Mevrouw Sophie De Wit (N-VA) stel dat het wetsontwerp in zijn artikelen 4 tot 6 de gegevens oplijst die operatoren moeten bewaren. Daar mogen ze zelf een aantal gegevens aan toevoegen. De lijst van de instanties die op die gegevens een beroep kunnen doen, is opgenomen in het ontworpen artikel 127/1, § 2. Het betreft een lange lijst, die echter nog kan uitgebreid worden. Sommige opgelijste autoriteiten lijken evident (bijvoorbeeld de autoriteiten bedoeld in de bepalingen onder 1° tot 3° en 6°), maar andere doen de wenkbrauwen fronsen. Zo wordt in de bepaling onder 7° gewag gemaakt van "de administratieve autoriteiten belast met het behoud van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid". Nagenoeg alle administraties buiten justitie kunnen daaronder vallen. Ook bij de opname in de lijst van "de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden" (10°), kan men vraagtekens plaatsen. De concrete lijst wordt vervat in een omzendbrief, toch een instrument dat met zeer weinig waarborgen is omgeven.

L'intervenante exprime l'espoir que les vice-premiers ministres pourront dissiper ses craintes à cet égard au cours de la discussion des articles. Elle s'étonne que ces préoccupations ne soient apparemment pas partagées par les partis de la majorité. Mme De Wit estime qu'il est crucial que le gouvernement puisse répondre à cette question, y compris dans l'intérêt des personnes qui devront utiliser ce cadre juridique à l'avenir.

M. Erik Gilissen (VB) remercie les vice-premiers ministres pour leurs réponses et renvoie à ses interventions précédentes.

La législation doit être solide et tournée vers l'avenir. On peut se demander si c'est le cas du régime à l'examen. On peut en effet se demander s'il pourra résister au contrôle de la Constitution et du droit européen. L'APD a été acerbe dans son avis. Quelques partis ont déjà fait savoir qu'ils attaqueraient la nouvelle loi devant la Cour constitutionnelle. Il appartient aux parlementaires de se montrer critiques.

IV. — **DISCUSSION DES ARTICLES**

CHAPITRE 1ER

Disposition générale

Article 1er

Cet article ne donne lieu à aucune observation.

CHAPITRE 2

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

Art. 2

Cet article complète l'article 2 de la loi du 13 juin 2005 en définissant les notions de "fraude", d'"utilisation malveillante du réseau ou du service", de "données de communications électroniques", de "contenu de communications électroniques" et de "métadonnées de communications électroniques". En outre, la définition des "appels infructueux", que la Cour constitutionnelle avait annulée dans son arrêt du 22 avril 2021 (arrêt n° 57/2021), est réintroduite.

Mme Sophie De Wit (N-VA) observe que la notion de "métadonnées de communications électroniques" énoncée

De spreekster drukt de hoop uit dat de vice-eersteministers haar bezorgdheden hieromtrent zullen kunnen wegnemen tijdens de artikelsgewijze bespreking. Ze verwondert zich erover dat deze bekommeringen blijkbaar niet leven bij de meerderheidspartijen. Mevrouw De Wit acht het cruciaal dat de regering hierop een antwoord kan bieden, ook ten behoeve van degenen die in de toekomst met dit wettelijk kader aan de slag zullen moeten.

De heer Erik Gilissen (VB) dankt de vice-eersteministers voor hun antwoorden en verwijst naar zijn eerdere betogen.

Wetgeving moet toekomstgericht en robuust zijn. Het is zeer de vraag of dat het geval is voor de voorliggende regeling. Het is met name twijfelachtig of zij de toetsing aan de Grondwet en het Europees recht kan doorstaan. De GBA was scherp in haar advies. Enkele partijen hebben reeds aangegeven de nieuwe wet te zullen aanvechten voor het Grondwettelijk Hof. Het is de taak van parlementsleden om zich kritisch op te stellen.

IV. — **ARTIKELSGEWIJZE BESPREKING**

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Over dit artikel worden geen opmerkingen gemaakt.

HOOFDSTUK 2

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

Art. 2

Dit artikel vult artikel 2 van de wet van 13 juni 2005 aan met definities van de begrippen "fraude", "kwaadwillig gebruik van het netwerk of de dienst", "elektronische-communicatiegegevens", "inhoud van elektronische communicatie" en "elektronische-communicatiemetagegevens". Voorts wordt de definitie van "oproeppoging zonder resultaat", die het Grondwettelijk Hof had vernietigd in zijn arrest van 22 april 2021 (arrest nr. 57/2021), opnieuw ingevoegd.

Mevrouw Sophie De Wit (N-VA) merkt op dat het begrip "elektronische-communicatiemetagegevens",

au 3° fait référence à la fois au contenu des communications électroniques et à leurs métadonnées. Plus loin dans le projet de loi à l'examen, il est fait référence, à divers endroits, aux "données". Ce mot désigne-t-il le contenu, les métadonnées ou les deux? La réponse à cette question revêt une grande importance pour l'application du régime en projet. L'intervenante invite les services de la Chambre à s'assurer de l'utilisation uniforme de cette terminologie lorsqu'ils procéderont à une vérification du texte.

Se référant également à cette définition, *M. Michael Freilich (N-VA)* demande pourquoi elle mentionne le contenu des communications électroniques. Le membre pensait que le projet de loi à l'examen ne prévoyait pas la conservation du contenu des données. Le contenu sera-t-il finalement conservé et, dans l'affirmative, dans quels cas et pour quelles communications (*quid*, par exemple, des courriers électroniques)?

Mme Petra De Sutter, vice-première ministre et ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste (ci-après: la ministre des Télécommunications), attache une grande importance à l'utilisation cohérente d'une terminologie claire et préconise un contrôle légistique du texte sur le point soulevé par Mme De Wit.

Art. 3

Cet article vise à remplacer l'article 107/5 de la loi du 13 juin 2005, qui traite de l'utilisation de la cryptographie.

M. Nabil Boukili (PVDA-PTB) indique que le projet d'article 107/5 établit le principe de la liberté d'utiliser le cryptage, mais lui fixe également des limites. Ainsi, selon le paragraphe 3 en projet, l'utilisation du cryptage "ne peut pas empêcher l'exécution d'une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et localiser des communications non accessibles au public". Dans son avis écrit, la Ligue des droits humains (LDH) relève à cet égard ce qui suit: "*[l]a suppression des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public […] constitue une ingérence disproportionnée dans le droit au respect de la vie privée des personnes concernées et qui excède dès lors ce qui est nécessaire dans une société démocratique*".

luidens de bepaling onder 3°, zowel slaat op de inhoud van elektronische communicatie als op de metagegevens ervan. Verderop in het wetsontwerp wordt op verschillende plaatsen gewag gemaakt van "gegevens". Wordt hiermee dan de inhoud of de metagegevens bedoeld, of allebei? Het antwoord op die vraag is van groot belang voor de toepassing van de ontworpen regeling. De spreekster oppert dat de diensten van de Kamer bij een controle van de tekst zouden toezien op een eenvormig gebruik van deze terminologie.

Verwijzend naar diezelfde definitie vraagt *de heer Michael Freilich (N-VA)* zich af waarom daarin überhaupt melding wordt gemaakt van de inhoud van elektronische communicatie. Het lid had begrepen dat dit wetsontwerp niet voorzag in de bewaring van de inhoud van de gegevens. Zal er dan toch inhoud worden bijgehouden, en zo ja in welke gevallen en voor welke communicatie (vb. e-mails)?

Mevrouw Petra De Sutter, vice-eersteminister en minister van Ambtenarenzaken, Overheidsbedrijven, Telecommunicatie en Post (hierna: de minister van Telecommunicatie), hecht veel belang aan een consequent gebruik van heldere terminologie en pleit voor een wetgevingstechnische controle van de tekst op het door mevrouw De Wit aangehaalde punt.

Art. 3

Dit artikel beoogt artikel 107/5 van de wet van 13 juni 2005, dat handelt over het gebruik van versleuteling, te vervangen.

De heer Nabil Boukili (PVDA-PTB) stelt vast dat het ontworpen artikel 107/5 het beginsel van de vrijheid van het gebruik van versleuteling vastlegt, maar daaraan meteen limieten verbindt. Zo mag, luidens de ontworpen paragraaf 3, het gebruik van versleuteling "geen beletsel vormen voor de uitvoering van een gericht verzoek van een bevoegde autoriteit, onder de bij wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie". In haar schriftelijk advies merkt de *Ligue des droits humains* (LDH) daaromtrent het volgende op: "*[l]a suppression des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public […] constitue une ingérence disproportionnée dans le droit au respect de la vie privée des personnes concernées et qui excède dès lors ce qui est nécessaire dans une société démocratique*".

L'APD, pour sa part, plaide sans équivoque en faveur de la levée de cette restriction à l'utilisation de la cryptographie. Dans son avis n° 108/2021, cette autorité constate l'opposition de la communauté scientifique à l'utilisation de "portes dérobées" ("*backdoors*") dans les systèmes cryptés. L'APD conclut en indiquant que le projet de loi à l'examen "doit dès lors être revu afin de supprimer l'obligation pour les opérateurs qui mettent en place un système d'encryptage de rendre possible les mesures d'interception légale "(paragraphe 163).

Le ministre Van Quickenborne peut-il confirmer que des portes dérobées seront effectivement utilisées pour l'application de cet article? Dans le cas contraire, peut-il indiquer comment cet article sera mis en œuvre? Les opérateurs devront-ils s'abstenir de toute utilisation de la cryptographie? Et que pense-t-il des avis de la LDH et de l'APD à propos de cet article?

M. Vincent Van Quickenborne, vice-premier ministre et ministre de la Justice et de la Mer du Nord (ci-après: le ministre de la Justice), réplique en indiquant que le gouvernement ne partage pas l'avis de l'APD sur ce point. Le gouvernement reconnaît l'atteinte considérable à la vie privée que représente l'interception du contenu des communications. En ce qui concerne les données d'identification des utilisateurs, dont la Cour de justice de l'Union européenne indique elle-même qu'elles peuvent être considérées comme non sensibles dans certains cas, et les données de trafic et de localisation, qui sont effectivement sensibles mais moins sensibles que leur contenu, le législateur estime approprié et proportionné d'imposer cette obligation, dans les conditions prévues aux articles 126 et 126/1 du présent projet.

Le ministre de la Justice souligne que l'élément "porte dérobée" ne fait pas partie du projet de loi à l'examen, mais que notre pays fait des efforts pour aboutir à une solution européenne coordonnée de ce problème. Le ministre s'oppose à l'installation de portes dérobées à l'insu des opérateurs. Il préconise au contraire une coopération saine et directe entre les services judiciaires et de sécurité et les opérateurs, coopération d'ailleurs prévue à l'article 90*ter* du Code pénal. C'est aussi le meilleur moyen de tracer les demandes faites aux opérateurs et de réduire les coûts. Comme indiqué antérieurement, au cours de la discussion générale, le gouvernement a estimé qu'il était préférable de ne pas prendre de mesures légales à ce stade en ce qui concerne la coopération éventuelle des opérateurs en cas de cryptage de bout en bout.

M. Nabil Boukili (PVDA-PTB) se demande si l'APD se trompe lorsqu'elle indique dans son avis qu'il faudra

De GBA, van haar kant, pleit onomwonden voor een opheffing van deze begrenzing van het gebruik van versleuteling. In haar advies nr. 108/2021 constateert deze autoriteit dat de wetenschappelijke gemeenschap zich afzet tegen het gebruik van "achterdeurtjes" ("*backdoors*") in versleutelde systemen. De GBA besluit dat het wetsontwerp "derhalve [moet] worden herzien in die zin dat operatoren die een versleutelingssysteem opzetten, niet langer verplicht zijn om wettelijk toegestane interceptiemaatregelen mogelijk te maken" (paragraaf 163).

Kan de minister Van Quickenborne bevestigen dat er inderdaad gebruik zal worden gemaakt van *backdoors* voor de toepassing van dit artikel? Als dat niet het geval is, kan hij dan aangeven hoe uitvoering zal worden gegeven aan dit artikel? Zullen de operatoren elk gebruik van de cryptografie achterwege moeten laten? En wat vindt hij van de adviezen van de LDH en de GBA omtrent dit artikel?

De heer Vincent Van Quickenborne, vice-eersteminister en minister van Justitie en Noordzee (hierna: de minister van Justitie), repliceert dat de regering de GBA op dit punt niet is gevolgd. De regering erkent de grote inbreuk op het privéleven wat betreft het onderscheppen van de inhoud van de communicatie. Wat betreft de identificatiegegevens van een gebruiker, waarvan de rechtspraak van het Europees Hof van Justitie zelf aangeeft dat ze in bepaalde gevallen als niet-gevoelig kunnen worden beschouwd, en de verkeers- en lokalisatiegegevens, die wel degelijk gevoelig zijn maar dan weer minder gevoelig dan de inhoud, oordeelt de regering dat het redelijk en proportioneel is om, binnen de voorwaarden bepaald in de ontworpen artikelen 126 en 126/1, deze verplichting op te leggen.

De minister van Justitie benadrukt dat het element van de *backdoor* geen deel uitmaakt van het voorliggend wetsontwerp, maar dat ons land inspanningen doet om tot een Europees gecoördineerde oplossing voor deze problematiek te komen. De minister verzet zich tegen de installatie van *backdoors* zonder medeweten van de operatoren; hij is daarentegen pleitbezorger van een gezonde en directe samenwerking tussen de gerechtelijke en veiligheidsdiensten en de operatoren, samenwerking waarin overigens wordt voorzien door artikel 90*ter* Sv. Dat is ook de beste manier om de aan de operatoren gerichte verzoeken te kunnen traceren en om de kosten te drukken. De regering heeft, zoals reeds gezegd tijdens de algemene bespreking, geoordeeld dat het beter is vooralsnog geen wettelijke maatregelen te treffen omtrent de mogelijke samenwerking van operatoren bij *end-to-end* encryptie.

De heer Nabil Boukili (PVDA-PTB) vraagt zich af of de GBA dan dwaalt wanneer zij in haar advies stelt dat

disposer d'une porte dérobée pour pouvoir appliquer le régime proposé.

Si, comme l'affirme le ministre, il ne faut effectivement pas disposer d'une porte dérobée, comment cela se passera-t-il techniquement?

M. Michael Freilich (N-VA) se rallie à cette dernière question. L'utilisation de la cryptographie est en principe libre dans certaines limites. Si un opérateur crypte des métadonnées et n'est pas en mesure d'accéder lui-même aux données, doit-il adapter ses programmes pour que ces informations puissent être décryptées? L'applicabilité de cette mesure a-t-elle été discutée avec les opérateurs?

Un acteur comme *Signal* ne conserve pas de métadonnées. Devra-t-il changer de systèmes?

Le paragraphe 4 en projet dispose que l'utilisation de la cryptographie par un opérateur étranger ne peut pas empêcher les opérateurs de respecter, du fait de ce cryptage, les dispositions légales en matière de conservation des données et d'interception du contenu des communications à l'égard des personnes utilisant une carte SIM étrangère dans leur appareil sur le territoire belge. M. Freilich doute que le gouvernement soit en mesure de faire appliquer cette disposition en pratique. Dans quelle mesure est-il réaliste d'attendre des opérateurs étrangers qu'ils adaptent leurs systèmes? Cela ne posera-t-il pas des problèmes à de nombreux expatriés qui travaillent dans notre pays? Selon le membre, il serait préférable de convenir de telles mesures au niveau européen.

Le ministre de la Justice répète à l'intention de M. Boukili que le gouvernement ne vise pas une "porte dérobée", mais une collaboration entre la justice et les opérateurs. Parallèlement, la Belgique veut peser sur le débat mené au niveau européen, où des techniciens réfléchissent aujourd'hui à comment avoir accès aux données cryptées sans mettre en péril le système du cryptage de bout en bout.

Concernant la question de M. Freilich sur les opérateurs étrangers, le ministre de la Justice épingle des précédents dans la jurisprudence de la Cour de cassation, où Yahoo et Skype ont été condamnés pour non-respect de l'obligation de concours qui leur incombe (resp. Cass. 1er décembre 2015, P.13 2082.N et Cass. 19 février 2019, P.17 1229.N), ainsi que la proposition récente de règlement de la Commission européenne, qui vise à instaurer un décryptage obligatoire des messages électroniques en lien avec des abus sexuels commis sur des enfants (COM(2022) 209 final).

de toepasselijkheid van de voorgenomen regeling een *backdoor* vereist.

Als, zoals de minister beweert, er inderdaad geen nood is aan een *backdoor*, hoe zal dit dan technisch in zijn werk gaan?

De heer Michael Freilich (N-VA) sluit zich aan bij deze laatste vraag. Het gebruik van versleuteling is principieel vrij, mits bepaalde limieten. Als een operator metagegevens versleutelt en zelf niet in staat is aan de gegevens te raken, moet hij dan zijn programma's aanpassen opdat die informatie kan ontsleuteld worden? Werd de haalbaarheid daarvan bekeken met de operatoren?

Een speler zoals *Signal* houdt geen metagegevens bij. Zal die zijn systemen moeten omgooien?

In de ontworpen paragraaf 4 wordt bepaald dat het gebruik van versleuteling door een buitenlandse operator niet tot gevolg mag hebben dat de operatoren, bij personen die een buitenlandse SIM-kaart in hun toestel gebruiken op Belgisch grondgebied, als gevolg van deze versleuteling, niet meer kunnen voldoen aan de wettelijke bepalingen rond dataretentie en het onderscheppen van de inhoud van de communicatie. De heer Freilich acht het twijfelachtig dat de regering deze bepaling zal kunnen hardmaken in de praktijk. Hoe realistisch is het om van buitenlandse operatoren te verwachten dat zij hun systemen aanpassen? Gaat dit geen problemen opleveren voor talrijke expats die in ons land werken? Volgens het lid ware het beter om dergelijke maatregelen op Europees niveau af te spreken.

Ter attentie van de heer Boukili herhaalt *de minister van Justitie* dat de regering geen *backdoor* maar wel een samenwerking tussen justitie en de operatoren op het oog heeft. Daarnaast wil ons land wegen op het debat op Europees vlak, waar technici thans nadenken over manieren om toegang te krijgen tot geëncrypteerde gegevens zonder het systeem van de *end-to-end* encryptie op de helling te zetten.

Wat de vraag van de heer Freilich betreffende buitenlandse operatoren betreft, wijst de minister van Justitie op precedenten in de rechtspraak van het Hof van Cassatie, waarbij Yahoo en Skype werden veroordeeld wegens het niet-naleven van de op hen rustende medewerkingsplicht (resp. Cass. 1 december 2015, P.13 2082.N en Cass. 19 februari 2019, P.17 1229.N), alsook op het recente voorstel van verordening van de Europese Commissie, dat een verplichte ontsleuteling wil invoeren van onlineberichten die verband houden met kindermisbruik (COM(2022) 209 final).

S'agissant de l'élaboration pratique du paragraphe 3 en projet, le ministre fait observer que cette disposition vise à instaurer des conditions de concurrence équitables pour tous les opérateurs. Ces applications doivent définir elles-mêmes comment se conformer aux règles. Dans l'arrêt Skype précité, la Cour de cassation a balayé l'argument de cet opérateur selon lequel le cryptage rendrait techniquement impossible le respect de l'obligation de concours.

Selon *M. Nabil Boukili (PVDA-PTB),* l'explication du ministre de la Justice suscite plus de questions qu'elle n'apporte de réponses. Il estime qu'il n'y a que deux possibilités: soit il s'agit de données cryptées et alors il faut une "porte dérobée" pour pouvoir les décrypter, soit il s'agit de données non cryptées. Or, le ministre de la Justice indique qu'il n'y aura pas de porte dérobée ET que l'on ne touchera pas au cryptage. Il promet que ce problème sera résolu à l'aide d'une technique qui n'est pas encore disponible pour l'instant et dont il ne peut définir la forme exacte. Quelles garanties aurons-nous que cette technique en cours de développement ne constituera pas une "porte dérobée"?

L'observation de l'APD est très pertinente. Voter cet article revient à sauter dans l'inconnu, un choix que l'intervenant juge très problématique.

Le ministre de la Justice réplique que le cryptage de bout en bout n'exclut pas la disponibilité des métadonnées. Des opérateurs comme *Whatsapp* et *Telegram* conservent les données à des fins commerciales. Actuellement, une collaboration existe déjà avec les opérateurs qui cryptent les données: ceux-ci parviennent à transmettre des données à la justice à la demande d'un juge d'instruction. Ce n'est donc pas tout ou rien, comme M. Boukili tente de nous le faire croire.

Le débat actuel porte sur les métadonnées et leur éventuel cryptage, pas sur leur contenu. Ce dernier aspect sort du cadre du texte à l'examen; le débat y relatif sera mené au niveau européen. Tous ces éléments ne doivent en aucun cas nous empêcher de voter le texte à l'examen.

M. Nabil Boukili (PVDA-PTB) estime que ce qui pose problème, c'est que les membres sont invités à voter sur un article dont on ignore toujours quelle technique sera utilisée pour le mettre en œuvre. Même si le gouvernement considère qu'une "porte dérobée" peut être exclue, il ne peut indiquer comment les données cryptées seront décryptées dans ce cas.

Met betrekking tot de praktische uitwerking van de ontworpen paragraaf 3, merkt de minister op dat de ontworpen regeling een *level playing field* beoogt in te voeren voor alle operatoren. Dergelijke applicaties moeten zelf uitmaken hoe ze voldoen aan de regels. In het aangehaalde Skype-arrest veegde het Hof van Cassatie het argument van die operator als zou de encryptie het technisch onmogelijk maken te voldoen aan de medewerkingsplicht, van tafel.

Volgens *de heer Nabil Boukili (PVDA-PTB)* roept het antwoord van de minister van Justitie meer vragen op dan het beantwoordt. Volgens het lid zijn er slechts twee mogelijkheden: ofwel betreft het versleutelde gegevens, en heeft men een *backdoor* nodig om te kunnen ontsleutelen, ofwel betreft het niet-versleutelde gegevens. Niettemin stelt de minister van Justitie dat er geen *backdoor* zal zijn én dat er niet geraakt wordt aan de versleuteling. Hij belooft dat dit probleem zal opgelost worden door een techniek die op dit moment nog niet voorhanden is en waarvan hij niet kan zeggen hoe die eruit zal zien. Welke garanties zijn er dat die nog uit te dokteren techniek niet alsnog een *backdoor* zal uitmaken?

De opmerking van de GBA is zeer pertinent. Dit artikel stemmen komt neer op een sprong in het duister. Dit is zeer problematisch, aldus de spreker.

De minister van Justitie repliceert dat *end-to-end* encryptie de beschikbaarheid van metagegevens niet uitsluit. Spelers als *Whatsapp* en *Telegram* houden gegevens bij voor commerciële doeleinden. Op dit moment bestaat er reeds een samenwerking met operatoren die gegevens versleutelen; zij slagen erin om, op verzoek van een onderzoeksrechter, gegevens te bezorgen aan het gerecht. Het is dus niet alles of niets, zoals de heer Boukili wil doen geloven.

Het huidige debat gaat over metagegevens en de mogelijke encryptie ervan, niet over de inhoud van de gegevens. Dat laatste valt buiten het bestek van de voorliggende tekst; het debat daarover zal gevoerd worden op Europees niveau. Een en ander vormt geenszins een beletsel om deze tekst te stemmen.

Volgens *de heer Nabil Boukili (PVDA-PTB)* is de crux dat de leden gevraagd wordt te stemmen over een artikel waarvan men nog niet weet welke techniek zal worden gebruikt om het uit te voeren. Een *backdoor* mag dan volgens de regering uitgesloten zijn, zij kan niet aangeven hoe versleutelde gegevens dan wel zullen worden ontsleuteld.

Art. 4

Cet article vise à insérer un article 121/8 dans la loi du 13 juin 2005. L'article en projet vise à pouvoir garantir une réaction rapide et efficace de la part des opérateurs et du régulateur en cas de fraude commise par le biais des services de communications électroniques et d'utilisation malveillante des réseaux et services de communications électroniques.

Mme Sophie De Wit (N-VA) rappelle que l'article 121/8 de la loi télécom dispose que "les opérateurs prennent les mesures appropriées, proportionnées, préventives et curatives [.] de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services". Dans la première phrase du paragraphe 1er en projet, il est toutefois indiqué que ces mêmes opérateurs ne peuvent prendre connaissance du contenu des communications. Comment peuvent-ils dans ce cas juger s'il est question de fraude et d'utilisation malveillante des réseaux et services de communications électroniques et prendre ainsi certaines mesures? En effet, ces mesures sont plutôt lourdes de conséquences, comme en atteste l'énumération non exhaustive donnée au paragraphe 2 en projet.

Dans ce paragraphe 2, il est également prévu que des mesures peuvent être prises "lorsque cela se justifie au regard de la gravité des circonstances". Sur ce point également, l'intervenante demande comment les opérateurs pourraient être appelés à se prononcer sans connaître le contenu de la communication.

La ministre des Télécommunications indique qu'il appartient avant tout aux opérateurs eux-mêmes de juger dans quels cas des mesures doivent être prises contre la fraude et l'utilisation malveillante. L'article a dès lors été rédigé en concertation avec eux.

Les opérateurs ont en effet l'expérience des situations dans lesquelles, par exemple, des messages sont envoyés en masse à partir d'une seule adresse. Sans connaître le contenu de la communication, ils savent quand il s'agit de messages frauduleux ou de spam. Ils peuvent prendre certaines mesures contre ce phénomène, comme le blocage de numéros ou la désactivation de certains services. Ils effectuent une surveillance continue dans ce domaine et sont en concertation avec l'IBPT.

Mme Sophie De Wit (N-VA) souligne que certains messages, comme les messages push, peuvent également être innocents. Les opérateurs doivent alors encore déterminer eux-mêmes s'il est question de fraude ou d'utilisation malveillante. L'alinéa 3 du paragraphe 1er

Art. 4

Dit artikel strekt ertoe een artikel 121/8 in te voegen in de wet van 13 juni 2005. Het ontworpen artikel beoogt een snelle en doeltreffende reactie vanwege de operatoren en de regulator te kunnen garanderen in gevallen van fraude gepleegd aan de hand van elektronischecommunicatiediensten en kwaadwillig gebruik van de elektronische-communicatienetwerken en –diensten.

Mevrouw Sophie De Wit (N-VA) haalt aan dat het ontworpen artikel 121/8 van de telecomwet operatoren de mogelijkheid biedt om "gepaste, evenredige, preventieve en curatieve maatregelen [te treffen] om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen". In de eerste zin van de ontworpen paragraaf 1 wordt vermeld dat operatoren daarbij evenwel geen kennis mogen nemen van de inhoud van de communicatie. Hoe kunnen ze dan beoordelen of er sprake is van fraude en kwaadwillig gebruik van hun diensten om aldus te beslissen bepaalde maatregelen te nemen? Die maatregelen zijn immers eerder verstrekkend, zo getuige de niet-limitatieve opsomming in de ontworpen paragraaf 2.

In laatstgenoemde paragraaf wordt voorts bepaald dat maatregelen genomen kunnen worden "wanneer dat gerechtvaardigd is ten aanzien van de ernst van de omstandigheden". Ook op dit punt vraagt de spreekster zich af hoe operatoren een dergelijke beoordeling moeten maken zonder de inhoud van de communicatie te kennen.

De minister van Telecommunicatie geeft aan dat het in de eerste plaats aan de operatoren zelf is om te beoordelen in welke gevallen er maatregelen getroffen moeten worden tegen fraude en kwaadwillig gebruik. Het artikel werd dan ook in overleg met hen opgesteld.

De operatoren hebben immers ervaring met dergelijke situaties, waarbij bijvoorbeeld massaal berichten vanuit één bepaald adres verstuurd worden. Zonder de inhoud van de communicatie te kennen, weten ze wanneer het over frauduleuze berichten of spamberichten gaat. Ze kunnen daartegen bepaalde maatregelen nemen, zoals de blokkering van nummers of het deactiveren van bepaalde diensten. Op dit stuk voeren ze een continue monitoring uit en staan ze in overleg met het BIPT.

Mevrouw Sophie De Wit (N-VA) wijst erop dat bepaalde berichten, zoals pushberichten, ook onschuldig kunnen zijn. Operatoren moeten dan alsnog zelf vaststellen of er sprake is van fraude of kwaadwillig gebruik. Het derde lid van de ontworpen paragraaf 1 stipuleert dat het BIPT

proposé prévoit que l'IBPT a le pouvoir de donner des instructions contraignantes en la matière. En quoi consistent exactement ces instructions?

La ministre des Télécommunications explique que l'IBPT ne donne des instructions contraignantes que s'il constate qu'un opérateur ne respecte pas l'obligation énoncée dans l'article 121/8 proposé dans une situation qui affecte l'utilisateur final. Les instructions données ne concernent donc pas le mécanisme utilisé par l'opérateur pour lutter contre l'utilisation malveillante, mais visent simplement à garantir que l'opérateur empêche les messages frauduleux d'atteindre l'utilisateur final.

Mme Sophie De Wit (N-VA) demande encore quelques précisions. Ces instructions sont-elles données à la demande de l'utilisateur final lorsqu'il signale une situation frauduleuse? L'IBPT peut-il également agir sans signalement de l'utilisateur final?

La ministre des Télécommunications explique que l'IBPT ne contrôle pas quelles communications sur les réseaux parviennent ou non aux opérateurs et aux utilisateurs finaux. Toutefois, si des préjudices sont observés, l'IBPT peut vérifier si l'opérateur a pris les mesures nécessaires pour empêcher la communication frauduleuse.

Mme Sophie De Wit (N-VA) demande un complément d'explication concernant le rôle de l'opérateur. Est-il tributaire du signalement d'un préjudice par un utilisateur final? Ou l'opérateur peut-il également intervenir s'il identifie lui-même une utilisation malveillante sur le réseau?

La ministre des Télécommunications indique que deux scénarios sont possibles. D'une part, les utilisateurs finaux peuvent signaler des messages frauduleux, à la suite de quoi l'IBPT vérifie auprès de l'opérateur ce qu'il a fait ou non pour mettre fin à ces messages. D'autre part, des messages frauduleux peuvent également être évoqués dans la communication entre les opérateurs et l'IBPT. Dans ce cas, l'opérateur peut discuter avec l'IBPT de la meilleure façon de bloquer ces messages.

Mme Sophie De Wit (N-VA) souligne que les instructions de l'IBPT constituent pour elle une deuxième étape. Dans un premier temps, l'opérateur doit évaluer lui-même s'il y a une utilisation malveillante et si des mesures doivent être prises. Dans ce cas, l'opérateur dépend-il du signalement d'un utilisateur final ou peut-il également agir de son propre chef?

bevoegd is om ter zake bindende instructies te geven. Wat houden die juist in?

De minister van Telecommunicatie licht toe dat het BIPT enkel bindende instructies uitvaardigt wanneer het vaststelt dat een operator de in het ontworpen artikel 121/8 vervatte verplichting niet naleeft in een situatie waarbij de eindgebruiker getroffen wordt. De gegeven instructies hebben dus geen betrekking op het mechanisme dat de operator hanteert om kwaadwillig gebruik aan te pakken, maar strekken er enkel toe te verzekeren dat de operator verhindert dat frauduleuze berichten de eindgebruiker bereiken.

Mevrouw Sophie De Wit (N-VA) wenst nog enige verduidelijking. Worden dergelijke instructies uitgevaardigd op aangeven van de eindgebruiker wanneer die een frauduleuze situatie meldt? Kan het BIPT ook optreden zonder melding door een eindgebruiker?

De minister van Telecommunicatie verduidelijkt dat het BIPT niet monitort welke communicatie op de netwerken de operatoren en eindgebruikers al dan niet bereikt. Als er evenwel schade vastgesteld wordt, kan het BIPT nagaan of de operator het nodige heeft gedaan om de frauduleuze communicatie te verhinderen.

Mevrouw Sophie De Wit (N-VA) vraagt verdere toelichting over de rol van de operator. Is die afhankelijk van de melding van schade door een eindgebruiker? Of kan hij ook optreden als hij uit zichzelf kwaadwillig gebruik op het netwerk vaststelt?

De minister van Telecommunicatie geeft aan dat er twee scenario's mogelijk zijn. Enerzijds kunnen eindgebruikers frauduleuze berichten melden, waarop het BIPT bij de operator nagaat wat die al dan niet heeft gedaan om dergelijke berichten tegen te houden. Anderzijds kunnen frauduleuze berichten ook ter sprake komen in de communicatie tussen de operatoren en het BIPT. In dat geval kan de operator met het BIPT in discussie treden over de beste manier om dergelijke berichten tegen te houden.

Mevrouw Sophie De Wit (N-VA) stipt aan dat de instructies van het BIPT voor haar een tweede stap vormen. In een eerste fase moet de operator zelf beoordelen of er sprake is van kwaadwillig gebruik en of er maatregelen getroffen moeten worden. Is de operator in dat geval afhankelijk van een melding door een eindgebruiker of kan hij ook op eigen houtje optreden?

La ministre des Télécommunications confirme que l'opérateur peut également agir de sa propre initiative et ajoute que les signalements de tiers peuvent aussi donner lieu à une intervention. Par exemple, une institution financière peut signaler un volume inhabituel de messages. L'opérateur est alors obligé de bloquer la communication en question.

Art. 5

Cet article vise à apporter diverses modifications à l'article 122 de la loi du 13 juin 2005 en ce qui concerne la conservation et le traitement des données de trafic, notamment, par les opérateurs.

Mme Sophie De Wit (N-VA) revient sur l'article 5, 4°, qui tend à remplacer le paragraphe 4 de l'article 122 de la loi du 13 juin 2005, et particulièrement sur l'alinéa 2 du paragraphe 4, en projet, qui dispose: "[p]ar dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service, d'identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées nécessaires à ces fins". Elle se demande si cela signifie que les opérateurs téléphoniques peuvent décider eux-mêmes quelles sont les données qu'ils vont conserver ou non, voire d'ajouter une série de données. Elle souhaite savoir sur base de quels critères cela se produira: leur expérience, leurs connaissances, … Cela sera-t-il objectivé? Elle souligne que cela se passerait en dehors des critères stricts d'une procédure pénale (où un juge d'instruction est désigné, des délais sont prévus et des conditions déterminées sont à respecter). Elle estime que le champ d'application est large et aimerait se voir préciser comment ces champs et leur utilisation seront fixés.

M. Nabil Boukili (PVDA-PTB) réagit sur l'alinéa 1, 1°, du paragraphe 4, en projet. Il rappelle que l'APD précise que même dans le cas d'une criminalité grave, une conservation générale des données est interdite. Il souligne qu'en cas de fraudes ou de malveillances, qui sont d'un degré moindre, c'est d'autant moins autorisé. L'avis de la Ligue des droits humains va dans le même sens. La ministre des Télécommunications avait répondu que la Cour n'excluait pas cette pratique. Cependant, l'intervenant observe qu'elle s'est prononcée de manière plus générale dans l'arrêt du 5 avril 2022 (C-140/20, *The Commissioner of the Garda Síochána e.a.*) décidant que "[l]'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002,

De minister van Telecommunicatie bevestigt dat de operator ook op eigen initiatief kan optreden en voegt daaraan toe dat ook meldingen van derden aanleiding kunnen geven tot het ondernemen van actie. Zo kan een financiële instelling een ongebruikelijk volume berichten melden. De operator is in dat geval verplicht de communicatie in kwestie een halt toe te roepen.

Art. 5

Dit artikel beoogt diverse wijzigingen aan te brengen in artikel 122 van de wet van 13 juni 2005, wat de bewaring en verwerking van met name verkeersgegevens door operatoren betreft.

Mevrouw Sophie De Wit (N-VA) gaat opnieuw in op artikel 5, 4°, dat artikel 122, § 4, van de wet van 13 juni 2005 beoogt te vervangen, en met name op het tweede lid van de ontworpen § 4, dat luidt: "In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en verwerken, die voor deze doeleinden nodig worden geacht.". Het lid vraagt zich af of zulks betekent dat de telecomoperatoren zelf mogen bepalen welke gegevens zij al dan niet zullen bijhouden, en of ze daar zelfs bepaalde gegevens aan mogen toevoegen. Zij peilt naar de criteria die daarbij zullen worden gehanteerd: hun ervaring, hun kennis, of andere criteria? Zal een en ander worden geobjectiveerd? Zij benadrukt dat buiten de strenge criteria van een strafrechtprocedure om zou worden gegaan; bij die laatste wordt een onderzoeksrechter aangesteld, gelden er termijnen en moeten bepaalde voorwaarden in acht worden genomen. Zij is van oordeel dat het toepassingsgebied heel ruim is en verneemt graag hoe de beoogde werkingsgebieden en het gebruik ervan zullen worden vastgelegd.

De heer Nabil Boukili (PVDA-PTB) reageert op het eerste lid, 1°, van de ontworpen § 4. Hij herinnert eraan dat de GBA erop wijst dat een veralgemeende gegevensbewaring verboden is, zelfs bij zware criminaliteit. Hij onderstreept dat zulks bij fraude of kwaadwillig gebruik – wat toch van een minder ernstige orde is – des te minder toegestaan is. Het advies van de *Ligue des droits humains* gaat in dezelfde richting. De minister van Telecommunicatie had geantwoord dat het Hof van Justitie die praktijk niet uitsloot. De spreker wijst er evenwel op dat het Hof zich ter zake op een meer algemene manier uitgesproken heeft in zijn arrest van 5 april 2022 (C-140/20, *The Commissioner of the Garda Síochána and Others*). In dat arrest oordeelt het

concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation" (dispositif). Cette conservation de données n'est donc pas justifiée à ses yeux. Il se demande dès lors comment le dispositif prévu dans le projet de loi passera la rampe de la CJUE ou de la Cour constitutionnelle.

M. Michael Freilich (N-VA) s'attarde également au même dispositif, en se demandant s'il s'agissait d'une obligation de conservation des données dans le chef des opérateurs, de manière systématique pour tous les utilisateurs, quel que soit l'endroit où ils se trouvent. Si c'est le cas, il aimerait savoir si le ministre de la Justice n'y voit pas une immixtion dans la vie privée ou, à tout le moins, une infraction aux règles de protection de la vie privée. Il s'interroge sur le cas de la société *Signal* qui propose un procédé de communication où il n'y a pas de métadonnées conservées. Devra-t-elle se conformer à l'obligation?

Sur la criminalité grave, il souligne l'importance de lutter sans relâche contre ces actes mais se demande si ce n'est pas disproportionné d'englober tout le territoire national. Sur les 3° et 4° du paragraphe 4, alinéa 1er, en projet, il souhaiterait savoir pourquoi il n'y a pas de délai maximum de conservation et jusque quand ils peuvent courir.

La ministre des Télécommunications apporte les précisions suivantes:

— les données qui sont conservées doivent l'être de manière proportionnée et nécessaire. Cela n'empêche pas les différents opérateurs de garder les données en leur possession pour d'autres raisons qui leur sont propres (lutte contre la fraude, …);

— la CJUE ne s'est pas prononcée sur la rétention des données avec le but de lutte contre la fraude mais Hof dat "Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, (…) aldus [moet] worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die met het oog op de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens" (dispositief). De beoogde gegevensbewaring is volgens hem dan ook niet gerechtvaardigd. Hij vraagt zich dan ook af hoe de ontworpen regeling de toetsing van het Hof van Justitie van de Europese Unie of van het Grondwettelijk Hof zou kunnen doorstaan.

Ook *de heer Michael Freilich (N-VA)* staat stil bij diezelfde beoogde regeling. Hij wil weten of de operatoren verplicht zullen zijn de gegevens te bewaren, en zulks stelselmatig te doen voor álle gebruikers, waar zij zich ook bevinden. Mocht dat zo zijn, dan wil hij van de minister van Justitie vernemen of die daar geen inmenging in de privacy in ziet, of minstens een inbreuk op de regels inzake de bescherming van de persoonlijke levenssfeer. Hij gaat ook nader in op het geval van het bedrijf *Signal*, dat met een communicatieproces werkt waarbij geen metagegevens bewaard worden. Zal ook die onderneming zich naar de verplichting moeten schikken?

Wat zware criminaliteit betreft, benadrukt de spreker dat tegen dergelijke daden een onophoudelijke strijd moet worden gevoerd, maar hij vraagt zich af of het niet disproportioneel is de regeling over het hele grondgebied te doen toepassen. Wat de bepalingen onder 3° en 4° van de ontworpen § 4, eerste lid, betreft, wil hij weten waarom niet in een maximumtermijn voor de gegevensbewaring voorzien is, en tot wanneer die termijnen zouden kunnen lopen.

De minister van Telecommunicatie verduidelijkt de volgende zaken:

— het bijhouden van gegevens moet noodzakelijk zijn voor en evenredig met de doelstellingen. Dat neemt niet weg dat de verschillende operatoren de gegevens nog om andere en voor hen geldende redenen (fraudebestrijding enzovoort) in hun bezit kunnen houden;

— het HvJ-EU heeft zich niet uitgesproken over de bewaring van gegevens met het oog op fraudebestrijding,

uniquement dans des cas du ressort pénal. En suivant le raisonnement de la CJUE, la jurisprudence européenne se prononce plutôt pour la conservation généralisée à des fins de poursuite pénale; dire que toute conservation généralisée serait impossible n'est pas correct: l'exemple des données de facturation est éclairant à ce titre;

— la CJUE a indiqué que ces données, conservées pour une certaine finalité, peuvent être utilisées pour des finalités plus importantes, comme la lutte contre la fraude;

— l'APD a fait une distinction dans son avis n° 66/2022, considérant qu'une décision coercitive pouvait être prise à l'égard de la personne dont les données sont traitées et qu'il s'agissait en effet d'un critère pertinent;

— sur la conservation des données par les opérateurs, il ne s'agit pas d'un non-respect de la vie privée mais d'une décision qui peut se justifier au regard de la protection des intérêts des opérateurs et des utilisateurs finaux;

— sur le cas de *Signal*, ils ont toujours les métadonnées à disposition;

— sur la question des délais maximaux, au paragraphe 4, en projet, ils sont précisés et varient de quatre mois (*Call detail record*) à douze mois (lutte contre fraude ou l'utilisation malveillante des réseaux).

M. Michael Freilich (N-VA) revient sur le cas de *Signal* en lien avec le projet de loi qui prévoit bien une obligation de conservation dans le chef des opérateurs télécoms. Au vu de la réponse de la ministre des Télécommunications, il se demande dès lors si le texte ne doit pas être adapté pour les opérateurs aux technologies OTT (*over-the-top*).

Sur l'aspect protection de la vie privée, concernant la conservation des métadonnées téléphoniques sur l'ensemble du territoire, il rappelle que c'est interdit et qu'il a été décidé de procéder par zones géographiques. Sur les fraudes sur les réseaux, la ministre des Télécommunications a précisé qu'elle ne procéderait pas par zones géographiques et que les données seraient bien conservées pour tous.

M. Nabil Boukili (PVDA-PTB) revient sur l'exemple donné par la ministre des Télécommunications des opérateurs téléphoniques qui ont besoin des données

maar alleen over de gevallen die onder het strafrecht vallen. Volgens de redenering van het HvJ-EU is de Europese rechtspraak veeleer voorstander van algemene bewaring met het oog op strafvervolging; het is niet correct te beweren dat algemene bewaring onmogelijk zou zijn: het voorbeeld van de factureringsgegevens is in dit verband verhelderend;

— het HvJ-EU heeft verklaard dat die gegevens, die voor een bepaald oogmerk worden bewaard, ook voor belangrijkere doeleinden kunnen worden aangewend, zoals fraudebestrijding;

— de GBA heeft in haar advies nr. 66/2022 een onderscheid gemaakt vanuit de overweging dat een dwingende beslissing kon worden genomen ten aanzien van iemand wiens gegevens worden verwerkt en dat het wel degelijk om een relevant criterium gaat;

— de gegevensbewaring door de operatoren is geen kwestie van het niet-respecteren van de persoonlijke levenssfeer, maar een beslissing die kan worden verantwoord op grond van het feit dat de belangen van de operatoren en de eindgebruikers moeten worden beschermd;

— wat het geval van *Signal* betreft, is het zo dat zij steeds over metagegevens beschikken;

— de in de ontworpen § 4 bedoelde maximale termijnen zouden variëren van vier maanden (*Call detail record*) tot twaalf maanden (fraudebestrijding of kwaadwillig gebruik van netwerken).

De heer Michael Freilich (N-VA) gaat nader in op het geval van Signal, dat verband houdt met dit wetsontwerp dat er wel degelijk toe strekt de telecomoperatoren te verplichten de gegevens te bewaren. Gelet op het antwoord van de minister van Telecommunicatie vraagt hij zich af of het wetsontwerp niet moet worden aangepast voor de operatoren die gebruik maken van de OTT-technologieën (*over-the-top*).

In verband met de bescherming van de persoonlijke levenssfeer en de bewaring van telefonische metagegevens over het hele grondgebied, wijst de spreker erop dat zulks verboden is en dat er werd beslist om met geografische zones te werken. Wat de gevallen van fraude op de netwerken betreft, heeft de minister van Telecommunicatie aangegeven dat ze niet met geografische zones zou werken en dat de gegevens wel degelijk voor iedereen zou worden bewaard.

De heer Nabil Boukili (PVDA-PTB) gaat nader in op het door de minister van Telecommunicatie aangehaalde voorbeeld van de telefoonoperatoren die de gegevens

pour la facturation. Il rappelle qu'il y a dans ce cas un contrat et donc un consentement du client, ce qui n'est pas le même cas de figure. Ici, il s'agit de l'État qui oblige à garder les métadonnées, sans le consentement des utilisateurs. Il estime que ce sont deux situations incomparables. Il rappelle que la CJUE a précisé que seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique peuvent justifier des ingérences graves dans les droits fondamentaux. Si on applique ce raisonnement au projet de loi, on est ici dans la lutte contre la fraude, et donc on n'est ni dans la lutte contre la criminalité grave ni dans la prévention des menaces graves contre la sécurité publique. L'intervenant estime donc que la ministre des Télécommunications ne peut donc pas justifier cette conservation généralisée dans le cadre fixé par la CJUE (délits qui ne sont pas de la criminalité grave).

Mme Sophie De Wit (N-VA) revient sur les délais de conservation des données (de quatre à douze mois selon les cas). Au paragraphe 4, alinéa 1er, 3°, en projet, il est précisé que ces délais peuvent être prolongés aux fins d'analyse, à la résolution ou au traitement de l'utilisation des cas. Elle note qu'il faudra déterminer ce délai de prolongation. Elle le met en parallèle avec l'article 126/1, en projet, où c'est limité à douze mois alors qu'il s'agit de cas qui mettent en jeu la sécurité du pays. Elle déplore que les opérateurs téléphoniques aient plus de latitude en pouvant conserver plus longtemps les données dans des cas qui s'avèrent au final moins graves. Il s'agit pour elle d'une rupture d'équilibre.

La ministre des Télécommunications précise que *Signal* devra en effet garder (et éventuellement transmettre) les données s'il les conserve dans son système.

Le ministre de la Justice ajoute que la CJUE s'est uniquement exprimée sur la conservation des métadonnées dans le cadre de la lutte contre la criminalité. La conservation des données de facturation par exemple, pendant une durée de quatre mois, poursuit un autre objectif: celui de la protection des consommateurs.

Sur les autres questions, *la ministre des Télécommunications* apporte les réponses suivantes:

— concernant la deuxième question de M. Boukili, elle précise qu'on n'est pas dans le cadre du RGPD;

nodig hebben voor de facturering. Hij wijst erop dat er in dat geval sprake is van een contract en dat de klant dus toestemming heeft gegeven, wat niet dezelfde situatie is. Hier gaat het erom dat men door de Staat wordt verplicht de metagegevens bij te houden, zonder dat de gebruikers daarvoor toestemming hebben gegeven. Dat zijn volgens de spreker twee situaties die niet met elkaar kunnen worden te vergeleken. Hij wijst erop dat het HvJ-EU heeft verduidelijkt dat ernstige vormen van inmenging in de grondrechten enkele kunnen worden verantwoord indien dit gebeurt in het raam van de strijd tegen de zware misdaad en om ernstige bedreigingen voor de openbare veiligheid te voorkomen. Dit wetsontwerp volgt die redenering echter niet, want hier gaat over fraudebestrijding en dus niet over de strijd tegen zware misdaad of over het voorkomen van ernstige bedreigingen voor de openbare veiligheid. De spreker is dus van oordeel dat de minister van Telecommunicatie deze algemene bewaring niet kan rechtvaardigen op grond van het kader dat door het HvJ-EU werd vastgelegd (misdrijven die niet onder zware misdaad vallen).

Mevrouw Sophie De Wit (N-VA) komt terug op de gegevensbewaringstermijnen (die naargelang van het geval van vier tot twaalf maanden kan variëren). In de ontworpen § 4, eerste lid, 3°, wordt verduidelijkt dat die termijnen kunnen worden verlengd voor analysedoeleinden, of voor het verhelpen van fraude of kwaadwillig gebruik van het netwerk of voor de behandeling van het gebruik van de gevallen. Ze merkt op dat die verlengingstermijn zal moeten worden vastgelegd. Ze vergelijkt die termijn met die uit het ontworpen artikel 126/1, die tot twaalf maanden beperkt is, hoewel het om gevallen gaat waarin de veiligheid van het land op het spel staat. Ze betreurt dat de telefoonoperatoren over een ruimere marge beschikken en gegevens met betrekking tot gevallen die uiteindelijk minder erg zijn, langer mogen bewaren in. Volgens haar zorgt dat verschil voor een onevenwichtigheid.

De minister van Telecommunicatie verduidelijkt dat als *Signal* de gegevens in zijn systeem bewaart, het die inderdaad zal moeten bijhouden (en eventueel doorsturen).

De minister van Justitie voegt daaraan toe dat het HvJ-EU zich enkel over de bewaring van metadata in het kader van misdaadbestrijding heeft uitgesproken. Met het bewaren van facturatiegegevens gedurende vier maanden bijvoorbeeld, wordt een ander doel, namelijk consumentenbescherming, nagestreefd.

Op de overige vragen antwoordt *de minister van Telecommunicatie* het volgende:

— wat de tweede vraag van de heer Boukili betreft, verduidelijkt ze dat een en ander niet in het kader van de

elle fait une autre interprétation de l'arrêt: la CJUE a répondu à des questions préjudicielles qui concernent des cas spécifiques, en complétant sa jurisprudence.

— concernant la question de Mme De Wit, elle précise qu'il s'agit de cas de fraudes spécifiques permettant de garder les données plus longtemps, le temps de bien comprendre de quoi il en retourne et de voir comment lutter contre le procédé. Il y a donc bien une différence dans l'application entre les articles 5 et 9 du projet de loi.

M. Nabil Boukili (PVDA-PTB) rappelle que la discussion est utile pour veiller à ce que le projet de loi ne soit pas recalé une troisième fois par la Cour constitutionnelle. Si la CJUE juge que même pour la criminalité grave, la conservation généralisée n'est pas opportune, il se demande comment elle va l'autoriser pour des actes moins graves de type fraude ou utilisation malveillante du réseau.

La ministre des Télécommunications répète que dans ces cas-ci, il s'agit de fraudes sur le réseau qui touchent tout le territoire. Il ne s'agit pas du même cas de figure. Elle précise qu'elle pense que la CJUE suivra ce raisonnement.

M. Michael Freilich (N-VA) revient encore sur le cas de *Signal*. Il relève que le paragraphe 4, en projet, parle bien d'une obligation pour l'opérateur de conserver les données qui y sont mentionnées. Si *Signal* n'est pas affecté, le texte ne devrait-il pas être modifié?

Sur les justifications au regard du respect de la vie privée et des exceptions prévues dans le projet de loi quant à la conservation des données, notamment pour la facturation, il observe que de nouvelles technologies de type OTT ne facturent pas leurs services, comme *WhatsApp*. Il souligne que l'APD partage plutôt ces inquiétudes. Il estime que les métadonnées seront conservées de manière indifférenciée et que toute une série d'organes publics auront accès à ces données, comme l'administration fiscale. Raison pour laquelle son groupe votera contre le texte proposé.

La ministre des Télécommunications complète sa réponse à M. Freilich: seules les données en mémoire seront conservées (cf. l'article 126, en projet). De nouvelles données ne seront pas demandées à de nouveaux

AVG past; zij interpreteert het arrest anders: het HvJ-EU heeft in dat arrest een antwoord gegeven op prejudiciële vragen die over specifieke gevallen gaan en heeft op die manier zijn rechtspraak vervolledigd.

— wat de vraag van mevrouw De Wit betreft, legt ze uit dat het om specifieke fraudegevallen gaat, waarbij de gegevens langer mogen worden bewaard totdat men terdege weet wat er aan de hand is en hoe men dat soort van fraude kan tegengaan. De artikelen 5 en 9 van het wetsontwerp worden dus wel degelijk op een verschillende manier toegepast.

De heer Nabil Boukili (PVDA-PTB) wijst erop dat het nuttig is deze besprekingen te voeren om te voorkomen dat de wet, mocht het wetsontwerp worden aangenomen, voor de derde keer een onvoldoende zou krijgen van het Grondwettelijk Hof. Als het HvJ-EU van oordeel is dat een veralgemeende bewaring zelfs voor zware criminaliteit niet aan de orde is, hoe zal het Hof die bewaring dan kunnen toestaan voor minder ernstige handelingen zoals fraude of een kwaadwillig gebruik van het netwerk, vraagt de spreker zich af.

De minister van Telecommunicatie herhaalt dat het in deze gevallen gaat om fraude op het netwerk, die een impact heeft op het hele grondgebied. De twee situaties kunnen volgens haar niet met elkaar worden vergeleken. Ze denkt dat het HvJ-EU die redenering zal volgen.

De heer Michael Freilich (N-VA) komt nogmaals terug op *Signal*. Hij merkt op dat het in de ontworpen § 4 wel degelijk gaat over de verplichting van de operatoren om de gegevens die erin zijn vermeld, te bewaren. Indien die verplichting niet op *Signal* van toepassing is, dient de tekst dan niet te worden gewijzigd?

Inzake de verantwoordingen met betrekking tot de inachtneming van de persoonlijke levenssfeer en inzake de in het wetsontwerp bepaalde uitzonderingen voor gegevensbewaring, met name in het kader van de facturatie, merkt hij op dat toepassingen die gebruik maken van nieuwe technologieën, zoals de OTT-technologie, hun diensten niet factureren. Dat is bijvoorbeeld bij *WhatsApp* het geval. Hij beklemtoont dat de GBA die bekommeringen veeleer te delen. Volgens hem zullen alle metadata zonder onderscheid worden bewaard en zullen tal van overheidsinstanties, waaronder de belastingadministratie, toegang hebben tot die gegevens. Dat is dan ook de reden waarom zijn fractie tegen de ontworpen tekst zal stemmen.

De minister van Telecommunicatie vervolledigt haar antwoord aan de heer Freilich: enkel de gegevens in het geheugen zullen worden bewaard (zie het ontworpen artikel 126). Er zullen geen nieuwe gegevens worden

opérateurs de type *Signal,* comme précisé dans l'exposé des motifs.

Art. 6

Cet article vise à apporter diverses modifications à l'article 123 de la loi du 13 juin 2005, en particulier pour tenir compte des évolutions techniques et légales.

M. Nabil Boukili (PVDA-PTB) relève que l'article 6 sert notamment à remplacer le paragraphe 1er de l'article 123 de la loi du 13 juin 2005. Il autorise les opérateurs de réseaux mobiles à traiter et à conserver les données de localisation autres que les données de trafic notamment lorsque cela est nécessaire pour le bon fonctionnement ou la sécurité du réseau ou du service et lorsque cela est nécessaire pour détecter ou analyser les fraudes ou utilisations malveillantes du réseau.

L'APD souligne que cet article va plus loin que l'article 9 de la directive européenne ePrivacy (directive 2002/58/CE) qu'il prétend transposer. La directive ne permet en effet ces traitements de données que lorsqu'elles ont été rendues anonymes ou moyennant le consentement des utilisateurs. Pour prévoir d'autres cas, il faut en justifier la nécessité et la proportionnalité. Il rappelle que le Conseil d'état relève les mêmes éléments, en indiquant que le commentaire de l'article ne parle pas de ces ajouts, et ne permet donc pas d'en évaluer la nécessité et la proportionnalité. L'intervenant observe ne pas avoir trouvé la justification de ces deux éléments dans les développements du projet et aimerait donc entendre le gouvernement à ce propos.

La ministre des Télécommunications rappelle que les critères de nécessité et de durée maximale suggérés par l'APD et le Conseil d'État ont été retenus dans le projet de loi. Les autres aspects n'ont pas été retenus car ils peuvent changer dans le temps.

M. Nabil Boukili (PVDA-PTB) demande si le critère de proportionnalité a été écarté.

La ministre des Télécommunications répond que la spécification des données de localisation n'a pas été retenue car elle diffère selon le système employé par les opérateurs.

gevraagd aan nieuwe operatoren van het type *Signal*, zoals uiteengezet in de memorie van toelichting.

Art. 6

Dit artikel beoogt diverse wijzigingen aan te brengen in artikel 123 van de wet van 13 juni 2005, in het bijzonder om rekening te houden met technische en wettelijke ontwikkelingen.

De heer Nabil Boukili (PVDA-PTB)) stelt dat artikel 6 er onder meer toe strekt de eerste paragraaf van artikel 123 van de wet van 13 juni 2005 te vervangen. Het beoogt de operatoren van mobiele netwerken toe te staan andere locatiegegevens dan verkeersgegevens te verwerken en te bewaren, onder andere wanneer dat noodzakelijk is voor de goede werking of voor de veiligheid van het netwerk of van de dienst en wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren.

De GBA benadrukt dat dit artikel verder gaat dan artikel 9 van de Europese e-privacyrichtlijn (Richtlijn 2002/58/EG) dat het beweert om te zetten. De richtlijn staat een dergelijke gegevensverwerking immers enkel toe wanneer de gegevens geanonimiseerd zijn of wanneer de gebruikers daartoe toestemming hebben gegeven. Om in andere gevallen te voorzien moeten de noodzakelijkheid en de evenredigheid ervan worden aangetoond. Hij stelt dat de Raad van State de aandacht vestigt op dezelfde punten en aangeeft dat de toelichting bij het artikel geen melding maakt van deze toevoegingen en het dus niet mogelijk maakt de noodzakelijkheid en de evenredigheid ervan te beoordelen. De spreker stelt dat hij de verantwoording van deze twee elementen niet gevonden heeft in de toelichting bij het ontwerp en dat hij dus graag zou weten wat de regering in dat verband te zeggen heeft.

De minister van Telecommunicatie stelt dat de criteria van de noodzakelijkheid en van de maximale termijn zoals geopperd door de GBA en de Raad van State in het wetsontwerp werden opgenomen. De andere aspecten werden niet in aanmerking genomen omdat zij mettertijd kunnen veranderen.

De heer Nabil Boukili (PVDA-PTB) vraagt of het evenredigheidscriterium achterwege werd gelaten.

De minister van Telecommunicatie antwoordt dat de specificatie van de locatiegegevens niet werd behouden omdat zij verschilt naargelang van het systeem dat door de operatoren wordt gebruikt.

M. Nabil Boukili (PVDA-PTB) émet les plus nettes réserves sur ce choix qui risque d'être recadré par la Cour constitutionnelle.

Art. 7

Cet article ne donne lieu à aucune observation.

Art. 8

Cet article vise à remplacer l'article 126 de la loi du 13 juin 2005.

Le gouvernement présente l'*amendement n° 1* (DOC 55 2572/002), qui tend à remplacer l'article proposé par ce qui suit:

"Art. 126. § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, conservent les données suivantes, pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture de ces réseaux ou services:

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

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

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

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

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

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

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

De heer Nabil Boukili (PVDA-PTB) maakt zeer ernstig voorbehoud bij deze keuze, die weleens op kritiek zou kunnen stuiten vanwege het Grondwettelijk Hof.

Art. 7

Over dit artikel worden geen opmerkingen gemaakt.

Art. 8

Dit artikel strekt ertoe artikel 126 van de wet van 13 juni 2005 te vervangen.

De regering dient *amendement nr. 1* (DOC 55 2572/002) in, dat ertoe strekt het ontworpen artikel te vervangen door:

"Art. 126. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de volgende gegevens, voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten:

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

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

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

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

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

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

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

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

5° l'adresse physique de livraison du service;

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

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

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

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

10° le numéro de téléphone attribué;

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

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

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

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

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

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

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

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

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

5° het fysieke leveringsadres van de dienst;

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

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

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

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

10° het toegewezen telefoonnummer;

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

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

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

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

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

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

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

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

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

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

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

L'arrêté royal visé à l'alinéa 1er, 17°, ne porte pas sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication, ou sur la localisation de l'équipement terminal.

Le Roi:

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

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

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

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

Par dérogation à l'alinéa 2, la durée de conservation des données visées au paragraphe 1er, alinéa 1er, 16°, 3e tiret, est réduite à six mois après la fin de la session lorsque l'opérateur conserve une autre donnée visée au paragraphe 1er, alinéa 1er, 16°.

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

L'arrêté royal visé au paragraphe 1er, alinéa 1er, 17°, et alinéa 4 et au paragraphe 2, alinéa 4, est proposé

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

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

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

Het koninklijk besluit bedoeld in het eerste lid, 17°, slaat niet op de inhoud van de elektronische communicatie, noch op de elektronische-communicatiemetagegevens die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur.

De Koning:

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

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

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

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

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

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

Het koninklijk besluit bedoeld in paragraaf 1, eerste lid, 17°, en vierde lid, en in paragraaf 2, vierde lid, wordt

par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres.".

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

M. Nabil Boukili (PVDA-PTB) rappelle que l'article 8 du projet de loi à l'examen, tel que modifié par l'amendement n° 1, vise à remplacer l'article 126 de la loi télécom. L'article 126 ainsi proposé instaure l'obligation pour les opérateurs de conserver les données de souscription de l'abonné et les données nécessaires à l'identification de l'utilisateur final ou de l'équipement terminal, dans la mesure où ils traitent ou génèrent ces données.

L'APD a souligné, dans son avis n° 66/2022, que certains opérateurs sont déjà autorisés à traiter et à générer de telles données pendant une courte période, mais qu'ils choisissent de ne pas les conserver après cette période. L'article 126 proposé les oblige désormais à le faire, ce qui constitue une intrusion particulièrement grave dans la vie privée des intéressés. De plus, rien ne garantit que cette intrusion sera efficace pour atteindre le but recherché.

L'APD avertit donc que cette disposition interdirait *de facto* certains services de communication, tels que Signal, qui choisissent de ne pas conserver ces données afin d'assurer la confidentialité de la communication. Ces craintes se sont vérifiées lors de la discussion générale, lorsque la ministre a répondu qu'il n'était pas question d'une interdiction, tout en soulignant que ces opérateurs devraient se conformer à la loi. Cette interprétation a encore été confirmée lors de la discussion des articles, durant laquelle il a été affirmé que tous les opérateurs doivent être traités de la même manière. Pour les opérateurs comme Signal, cela ne laisse que deux options: changer leur modèle commercial ou cesser de proposer leurs services en Belgique.

L'article 126, § 1er, 15°, proposé, règle la conservation générale des adresses IP à la source de la connexion. Cette conservation est approuvée par la jurisprudence européenne, en particulier dans l'arrêt de la CJUE dans l'affaire C-140/20 (*The Commissioner of the Garda Síochána e.a.*), qui stipule que les adresses IP peuvent être stockées temporairement si c'est strictement nécessaire. Le projet de loi prévoit une période de conservation de douze mois après la fin de la session. Comment la

voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad."

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

De heer Nabil Boukili (PVDA-PTB) stipt aan dat artikel 8 van het voorliggende wetsontwerp, zoals geamendeerd door amendement 1, ertoe strekt artikel 126 van de telecomwet te vervangen. In het aldus ontworpen artikel 126 wordt voor operatoren de verplichting ingevoerd om de abonnementsgegevens van de abonnee en de gegevens die nodig zijn voor de identificatie van de eindgebruiker of de eindapparatuur te bewaren, voor zover ze die gegevens verwerken of genereren.

De GBA stipte in haar advies nr. 66/2022 aan dat bepaalde operatoren dergelijke gegevens al gedurende een korte periode mogen verwerken en genereren, maar ervoor kiezen ze na die periode niet bij te houden. Op grond van het ontworpen artikel 126 worden ze nu verplicht om zulks toch te doen, wat een bijzonder ernstige inmenging vormt van de persoonlijke levenssfeer van de betrokkenen. Er zijn daarenboven geen garanties dat die inmenging doeltreffend zal zijn om het beoogde doel te bereiken.

De GBA waarschuwt er dan ook voor dat deze bepaling *de facto* een verbod zou inhouden voor bepaalde communicatiediensten, zoals *Signal*, die ervoor kiezen dergelijke gegevens niet te bewaren om de vertrouwelijkheid van de communicatie te verzekeren. Die vrees werd tijdens de algemene bespreking bewaarheid, toen de minister antwoordde dat er geen sprake was van een verbod, maar er wel op wees dat dergelijke operatoren zich naar de wet moesten schikken. Dat werd nog eens bevestigd tijdens de artikelsgewijze bespreking, met de uitspraak dat alle operatoren op gelijke wijze behandeld moeten worden. Voor operatoren als *Signal* blijven er dan nog maar twee opties over: hun businessmodel veranderen of hun diensten niet langer in België aanbieden.

In het ontworpen artikel 126, § 1, 15°, wordt de algemene bewaring van IP-adressen aan de bron van de verbinding geregeld. Een dergelijke bewaring vindt goedkeuring in de Europese rechtspraak, meer bepaald in het arrest van het HvJ-EU in de zaak C-140/20 (*The Commissioner of the Garda Síochána e.a.*). In dat arrest werd gestipuleerd dat IP-adressen tijdelijk opgeslagen mogen worden als dat strikt noodzakelijk is. Het wetsontwerp voorziet in een bewaartermijn van

ministre concilie-t-elle cette disposition avec le critère de stricte nécessité tel qu'il ressort de l'arrêt de la CJUE?

La CJCE a en outre indiqué que la conservation générale n'est autorisée que pour les adresses IP. Or, le projet de loi à l'examen réglemente également la conservation d'autres données, telles que l'adresse du contrôleur d'accès au réseau (*Media Access Control* ou MAC), l'identifiant permanent de l'équipement (*Permanent Equipment Identifier* ou PEI) et l'identité internationale d'équipement mobile (*International Mobile Equipment Identity* ou IMEI). Comment la ministre justifie-t-elle l'intention de conserver malgré tout ces données?

La ministre des Télécommunications passe en revue les observations de l'APD. L'une d'entre elles concernait le fait que les opérateurs ne sont tenus de conserver que les données qu'ils génèrent pour leurs propres besoins, ce qu'ils ne font pas toujours à l'heure actuelle. La ministre estime néanmoins qu'une période de conservation présente également des avantages pour eux, principalement en termes de sécurité. La durée de conservation n'est pas toujours suffisante pour répondre aux besoins des autorités. En outre, il existe de nombreuses différences dans la manière dont les différents opérateurs stockent les données pour leurs propres besoins.

Une des critiques est que la conservation des adresses IP serait moins pertinente du fait que c'est facile à contourner. Toutefois, cela n'est possible que si l'adresse IP à la source fait partie d'un réseau tiers (par exemple, un restaurant). Il est toujours important de pouvoir identifier le tiers à partir de l'adresse IP conservée. Cela permet au moins de savoir où se trouvait la personne faisant l'objet de l'enquête.

Les données en question sont également énumérées dans l'article 126 en projet, tel que modifié par l'amendement n° 1 du gouvernement (DOC 55 2572/002). Dans l'exposé des motifs, le gouvernement a répondu à toutes les observations formulées par l'APD.

En ce qui concerne la conservation obligatoire de l'adresse IP à la source de la connexion, qui affecterait *Signal*, la ministre note que le gouvernement considère que la CJUE autorise une conservation générale et indifférenciée de ces données. Elle souligne que la CJUE n'est pas un législateur et ne peut donc pas se prononcer sur les données qui doivent être conservées.

twaalf maanden na het einde van de sessie. Hoe brengt de minister dat in overeenstemming met het criterium van strikte noodzakelijkheid zoals dat blijkt uit het arrest van het HvJ-EU?

Het HvJ-EU stelde bovendien dat een algemene bewaring enkel is toegestaan voor IP-adressen. Het wetsontwerp regelt echter ook de bewaring van andere gegevens, zoals het adres van de controller van de toegang tot het netwerk (*Media Access Control address* of MAC), de permanente *identifier* van de apparatuur (*Permanent Equipment Identifier* of PEI) en de internationale identiteit van de mobiele apparatuur (*International Mobile Equipment Identity* of IMEI). Hoe rechtvaardigt de minister het voornemen om die gegevens toch te bewaren?

De minister van Telecommunicatie gaat dieper in op de opmerkingen van de GBA. Een daarvan betrof het feit dat operatoren enkel verplicht zijn die gegevens te bewaren die ze voor hun eigen behoeften genereren, wat ze nu niet altijd doen. Toch meent de minister dat een bewaring ook voor hen voordelen inhoudt, voornamelijk op het vlak van veiligheid. De bewaartermijn is niet altijd lang genoeg om te beantwoorden aan de behoeften van de autoriteiten. Daarnaast zijn er veel verschillen in de wijze waarop de verschillende operatoren gegevens opslaan voor hun eigen behoeften.

Een van de punten van kritieken luidt dat de bewaring van IP-adressen minder relevant zou zijn omdat het gemakkelijk te omzeilen is. Dat is echter alleen maar mogelijk als het IP-adres aan de bron deel uitmaakt van een netwerk van een derde (bijvoorbeeld een restaurant). Het blijft belangrijk om dan toch nog die derde te kunnen identificeren aan de hand van het bewaarde IP-adres. Zo weet men op zijn minst waar de persoon naar wie men een onderzoek uitvoert, zich bevond.

De betrokken gegevens worden overigens ook opgesomd in het ontworpen artikel 126 zoals gewijzigd bij het door de regering ingediende amendement nr. 1 (DOC 55 2572/002). De regering heeft in de memorie van toelichting een antwoord geboden op alle opmerkingen van de GBA.

Met betrekking tot de verplichte bewaring van het IP-adres aan de bron van de verbinding, die *Signal* zou treffen, merkt de minister op dat de regering van mening is dat het HvJ-EU een algemene en ongedifferentieerde bewaring van dergelijke gegevens toestaat. Ze wijst erop dat het HvJ-EU geen wetgever is en zich derhalve niet kan uitspreken over gegevens die bewaard moeten worden.

M. Nabil Boukili (PVDA-PTB) conclut en indiquant que les opérateurs qui génèrent des données seront obligés de les conserver. Les opérateurs qui refusent de le faire – parce que leur politique prévoit qu'ils ne conservent pas de telles données – perdront dès lors le droit d'exercer leurs activités en Belgique. Cela équivaut à une interdiction.

La ministre des Télécommunications confirme que les opérateurs qui génèrent des données seront obligés de les conserver.

M. Nabil Boukili (PVDA-PTB) demande qu'il soit confirmé que les opérateurs tels que *Signal* devront conserver les données qu'ils génèrent s'ils veulent poursuivre leurs activités en Belgique.

Le ministre de la Justice souligne qu'il faut d'abord connaître le modèle économique de *Signal* pour répondre à cette question: cette entreprise génère-t-elle des données ou non? La politique de confidentialité de *Signal* indique que son application est conçue pour ne jamais collecter ou recueillir d'informations sensibles. En outre, tous les messages, appels téléphoniques, noms et photos de profil sont encryptés de bout en bout dans l'application afin que des tiers ne puissent pas y accéder. *Signal* ne conserve pas de messages ou d'informations sur les appels téléphoniques sur ses serveurs, mais met les messages en file d'attente sur ses serveurs s'ils doivent être délivrés à un appareil temporairement hors ligne. Selon le ministre, on ne peut pas en déduire que *Signal* génère ou non des données. La règle est cependant simple: quiconque génère des données doit les conserver.

Beaucoup s'accordent à dire que Proximus et Telenet doivent conserver les données. Toutefois, d'autres fournisseurs sont également des opérateurs. Selon la directive européenne, ils devront également respecter la législation. Pourtant, en ce qui concerne ces fournisseurs, il est souvent affirmé que la conservation des données n'est pas nécessaire. Pourquoi y a-t-il deux poids, deux mesures?

M. Nabil Boukili (PVDA-PTB) conclut en indiquant que les ministres ne savent pas si *Signal* entre dans le champ d'application du projet de loi à l'examen.

Le ministre de la Justice propose que l'IBPT se réunisse avec *Signal* pour vérifier si la législation s'applique à cette entreprise.

La ministre des Télécommunications se rallie à cette proposition. La société *Signal* doit indiquer si elle génère des données. Dans l'affirmative, le régulateur examinera

De heer Nabil Boukili (PVDA-PTB) besluit dat de operatoren die gegevens genereren, verplicht zullen worden om die ook te bewaren. Operatoren die dat weigeren, omdat hun beleid bepaalt dat ze dergelijke gegevens niet bewaren, zullen dan ook het recht verliezen om hun activiteiten in België uit te oefenen. Dat komt neer op een verbod.

De minister van Telecommunicatie bevestigt dat operatoren die gegevens genereren, verplicht zullen worden om ze te bewaren.

De heer Nabil Boukili (PVDA-PTB) vraagt bevestiging dat operatoren zoals *Signal* de gegevens die ze genereren zullen moeten bewaren als ze hun activiteiten in België willen blijven uitoefenen.

De minister van Justitie wijst erop dat men eerst het businessmodel van *Signal* moet kennen: genereert het bedrijf gegevens of niet? In het privacybeleid van *Signal* wordt bepaald dat de app ontworpen is om nooit gevoelige informatie te verzamelen of te vergaren. Voorts worden alle berichten, telefoongesprekken, profielnamen en profielafbeeldingen in de app versleuteld met *end-to-end*-encryptie zodat derden er geen toegang toe hebben. *Signal* bewaart geen berichten of informatie over telefoongesprekken op zijn servers, maar zet berichten wel in de wachtrij op zijn servers als ze bezorgd moeten worden aan een toestel dat tijdelijk offline is. Volgens de minister kan men daaruit niet opmaken of *Signal* al dan niet gegevens genereert. De regel is echter simpel: wie gegevens genereert, moet ze bewaren.

Velen zijn het erover eens dat Proximus en Telenet gegevens moeten bewaren. Andere aanbieders zijn echter ook operatoren. Volgens de Europese richtlijn moeten ook zij de wetgeving naleven. Toch wordt voor dergelijke aanbieders vaak beweerd dat gegevensbewaring niet nodig is. Waarom wordt er met twee maten en twee gewichten gemeten?

De heer Nabil Boukili (PVDA-PTB) concludeert dat de ministers niet weten of *Signal* onder het toepassingsveld van het wetsontwerp zou vallen.

De minister van Justitie stelt voor dat het BIPT met *Signal* om de tafel zou moeten zitten om na te gaan of de wetgeving op het bedrijf van toepassing is.

De minister van Telecommunicatie sluit zich daarbij aan. *Signal* moet aangeven of het gegevens genereert. Als dat het geval is, moet de regulator bekijken hoe de wet

comment la loi doit être appliquée. Cela vaudra pour tous les opérateurs actuels et futurs.

M. Nabil Boukili (PVDA-PTB) fait observer que les membres de la commission ne disposent pas de ces informations aujourd'hui et que le projet de loi soumis à leur vote comporte donc de nombreuses inconnues.

M. Koen Geens (CD&V) revient sur la version de l'article 126, § 1er, 17°, proposée par l'amendement n° 1 (DOC 55 2572/002), qui porte sur la détermination des autres identifiants concernant l'utilisateur final ou l'équipement terminal. Cette disposition habilite le Roi à déterminer ces identifiants par la voie d'un arrêté royal qui devra être confirmé par le Parlement dans les six mois qui suivront sa publication. Cette délégation de pouvoir n'est que brièvement expliquée dans la justification de l'amendement n° 1. Faut-il vraiment retirer ce pouvoir au Parlement pour le confier au Roi?

La période de conservation de douze mois a été ramenée à six mois à la demande du Conseil d'État. Est-il nécessaire que cette période soit aussi longue?

La ministre des Télécommunications souligne qu'il est important, en matière d'identifiants, de pouvoir suivre les évolutions technologiques et de réagir plus rapidement par le biais d'arrêtés royaux. Une telle délégation de pouvoirs au Roi est habituelle lorsqu'il s'agit de paramètres spécifiques soumis à une évolution rapide.

Art. 9

Cet article vise à insérer un article 126/1 dans la loi du 13 juin 2005. Il s'agit d'une disposition totalement nouvelle. Le contenu de l'ancien article 126/1, inséré par l'article 5 de la loi du 29 mai 2016, lui-même annulé par l'arrêt n° 57/2021 de la Cour constitutionnelle, est repris, moyennant des modifications, dans l'article 127/3 proposé (article 13 du projet de loi à l'examen).

Le gouvernement présente l'*amendement n° 2* (DOC 55 2572/002), qui tend à apporter les modifications suivantes à l'article 126/1 proposé:

1° le paragraphe 2 est remplacé par ce qui suit:

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

moet worden toegepast. Dat geldt voor alle bestaande en toekomstige operatoren.

De heer Nabil Boukili (PVDA-PTB) wijst erop dat de commissieleden vandaag niet over die informatie beschikken en dus over een wetsontwerp moeten stemmen dat veel onbekende factoren bevat.

De heer Koen Geens (CD&V) gaat dieper in op artikel 126, § 1, 17°, in de versie zoals voorgesteld bij amendement nr. 1 (DOC 55 2572/002), dat de identificatie van de andere *identifiers* met betrekking tot de eindgebruiker of de eindapparatuur regelt. In deze bepaling krijgt de Koning de bevoegdheid om die *identifiers* te bepalen bij een koninklijk besluit dat binnen zes maanden na de bekendmaking ervan door het Parlement bekrachtigd moet worden. Deze bevoegdheidsdelegatie wordt slecht kort toegelicht in de verantwoording bij amendement nr. 1. Moet die bevoegdheid echt aan het Parlement ontnomen en aan de Koning toevertrouwd worden?

De bewaartermijn van twaalf maanden werd op verzoek van de Raad van State ingekort tot zes maanden. Is het nodig dat die termijn zo lang is?

De minister van Telecommunicatie stipt aan dat het inzake *identifiers* belangrijk is om de technologische ontwikkelingen te kunnen volgen en via koninklijk besluiten korter op de bal te kunnen spelen. Een dergelijke bevoegdheidsdelegatie aan de Koning is gebruikelijk als het gaat over specifieke parameters die aan een snelle evolutie onderhevig zijn.

Art. 9

Dit artikel strekt ertoe een artikel 126/1 in te voegen in de wet van 13 juni 2005. Het betreft een volledig nieuwe bepaling. De inhoud van het oude artikel 126/1, ingevoegd bij artikel 5 van de wet van 29 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt, mits wijzigingen, hernomen in het ontworpen artikel 127/3 (artikel 13 van het wetsontwerp).

De regering dient *amendement nr. 2* (DOC 55 2572/002) in, dat ertoe strekt, in het ontworpen artikel 126/1, de volgende wijzigingen aan te brengen:

1° paragraaf 2 wordt vervangen als volgt:

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

2° dans le paragraphe 4, alinéa 4, remplacer les mots “dans l’arrêté royal visé au paragraphe 2, alinéa 2“ par les mots “à l’article 126/2”.

Il est renvoyé à la discussion générale ainsi qu’à la justification écrite de l’amendement.

Mme Sophie De Wit (N-VA) souligne l’importance vitale du droit à la vie privée, mais indique que, lorsque la sécurité est compromise, la balance peut pencher en faveur de cette dernière. Divers exemples frappants ont été donnés au cours de la discussion générale.

Le système stratifié de conservation des données prévu à l’article 126/1 proposé – la “lasagne” – est très complexe. La jurisprudence de la CJUE, qui fournit certaines lignes directrices et met l’accent sur des critères objectifs, n’y est bien sûr pas étrangère.

Pour la N-VA, il est crucial que la justice dispose des outils nécessaires pour lutter contre la criminalité. Ce qui surprend toutefois Mme De Wit, c’est que la conservation des données à des fins judiciaires, pour lesquelles, comme il a déjà été mentionné, la restriction du droit à la vie privée est plus facilement envisageable, est beaucoup plus strictement réglementée dans le projet de loi à l’examen que la conservation des données à d’autres fins, les opérateurs étant autorisés à conserver de nombreuses données qui dès lors sont également accessibles pour de nombreuses instances.

La conservation ciblée sur base géographique est clairement délimitée, contrairement aux notions fourre-tout telles que “fraude” et “utilisation malveillante du réseau ou du service” utilisés ailleurs dans le projet de loi à l’examen.

L’article 126/1 proposé ne traite que des métadonnées des communications électroniques, à l’exclusion du contenu des communications électroniques. La conservation est différenciée en fonction des zones géographiques. La membre espère que la complexité du règlement ne soulèvera pas de problèmes dans la pratique. Elle se demande si le gouvernement, en élaborant cette réglementation, a confronté ces paramètres à la pratique.

Pour le critère de la criminalité grave il est renvoyé à l’article 90*ter* du Code d’instruction criminelle. Cet article est souvent utilisé pour désigner la criminalité grave, pour laquelle certains devoirs d’instruction importants sont alors considérés comme admissibles. La COC a posé la question de savoir s’il est techniquement possible aujourd’hui d’isoler avec précision les infractions énumérés dans cet article dans la Banque de données

2° in § 4, vierde lid, worden de woorden “in het koninklijk besluit bedoeld in paragraaf 2, tweede lid“ vervangen door de woorden “in artikel 126/2”.

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Mevrouw Sophie De Wit (N-VA) benadrukt het essentiële belang van privacy maar geeft aan dat, wanneer de veiligheid in het gedrang komt, de balans in het voordeel van dat laatste belang mag overhellen. Tijdens de algemene bespreking werden diverse sprekende voorbeelden gegeven.

Het gelaagd systeem van gegevensbewaring waarin het ontworpen artikel 126/1 voorziet – de “lasagne” – is erg complex. De rechtspraak van het HvJ-EU, waarin bepaalde kapstokken worden aangereikt en de nadruk ligt op objectieve criteria, is daaraan natuurlijk niet vreemd.

Voor de N-VA is het cruciaal dat justitie de nodige tools heeft om de strijd tegen de criminaliteit aan te gaan. Wat mevrouw De Wit evenwel verwondert, is dat de gegevensbewaring voor justitiële doeleinden, waarvoor zoals gezegd inperkingen van de privacy makkelijker voorstelbaar zijn, in het wetsontwerp veel strenger is gereguleerd dan dataretentie voor andere doeleinden, waarbij operatoren tal van gegevens mogen bewaren die dan ook nog eens toegankelijk zijn voor tal van instanties.

De gerichte bewaring op geografische basis is duidelijk afgebakend, in tegenstelling tot de vage containerbegrippen als “fraude” en “kwaadwillig gebruik van het netwerk of de dienst”, die elders in het wetsontwerp worden gebruikt.

In het ontworpen artikel 126/1 gaat het enkel over de metagegevens van de elektronische communicatie, met uitsluiting van de inhoud van elektronische communicatie. De bewaring wordt gedifferentieerd volgens geografische zones. De spreekster hoopt dat de complexiteit van de regeling in de praktijk niet tot problemen zal leiden. Zij vraagt zich af of de regering, bij het uitwerken van deze regeling, die parameters eens heeft losgelaten op de praktijk.

Bij het criterium van de zware criminaliteit wordt verwezen naar artikel 90*ter* van het Wetboek van strafvordering. Dat artikel wordt vaak gebruikt om zware criminaliteit, waarvoor dan bepaalde ingrijpende onderzoeksdaden toelaatbaar worden geacht, aan te wijzen. Het COC heeft de vraag gesteld of het vandaag technisch mogelijk is om de in dat artikel opgelijste misdrijven op accurate wijze te isoleren in de Algemene Nationale Gegevensbank

Nationale Générale (BDNG). C'est important afin de se conformer à la jurisprudence de la CJEU.

En outre, la question se pose de savoir s'il est possible que la conservation sur base du critère géographique couvre l'ensemble du pays. Si dans chaque zone, sur une moyenne des trois dernières années civiles, on enregistre trois infractions graves pour 1 000 habitants par an – ce qui, après tout, n'est pas beaucoup – on arrive à une grande zone, malgré l'utilisation de critères de conservation ciblée des données. Le gouvernement a-t-il fait cet exercice?

L'APD a recommandé de prendre en compte le nombre de condamnations et non le nombre d'infractions. La membre comprend que le gouvernement s'en tienne à ce dernier paramètre; toutes les infractions ne débouchent en effet pas sur une condamnation.

On se fie à la BNG pour les statistiques. Des qualifications pénales correctes sont indispensables pour rester dans les limites des infractions visées à l'article 90*ter* du Code d'instruction criminelle. Cependant, la qualification donnée lors du constat d'une infraction n'est que provisoire. Ne court-on pas le risque que lors du constat d'une infraction, on la surqualifie systématiquement, ce qui peut conduire à fausser la réalité? Il est important de se baser sur des statistiques correctes.

Le régime est si complexe que Mme De Wit se demande si les acteurs sur le terrain pourront s'en sortir. Les services seront-ils en mesure de définir les zones avec suffisamment de précision et d'objectivité? Dans le cas contraire, le régime mis en place n'est pas conforme à la jurisprudence de la Cour et risque d'être à nouveau annulé.

Tout cela est lié non seulement au critère statistique, mais aussi à la conservation des données sur base des zones stratégiques. Dans son avis, le Conseil d'État s'est montré critique à ce sujet. S'il n'y a pas de motivation claire quant à la raison pour laquelle une zone particulière est stratégique, cela risque d'affaiblir le régime.

Le ministre de la Justice peut-il garantir que les différentes zones de conservation des données ont été correctement et objectivement déterminées? Il est en effet essentiel que la justice puisse appliquer les règles.

Le rapport d'évaluation annuel mentionné dans le paragraphe 6 proposé sera d'une grande importance à cet égard.

M. Michael Freilich (N-VA) évoque le cas des personnes se déplaçant entre des zones où s'appliquent

(ANG). Dit is belangrijk om te kunnen voldoen aan de rechtspraak van het HvJ-EU.

Voorts stelt zich de vraag of het mogelijk is dat de bewaring volgens het geografisch criterium het hele land omvat. Als in elke zone, over een gemiddelde van de drie voorbije kalenderjaren, drie zware strafbare feiten per 1 000 inwoners per jaar worden vastgesteld – wat per slot van rekening niet heel veel is – komt men, spijts het gebruik van criteria voor gerichte dataretentie, tot één grote zone. Heeft de regering die oefening gemaakt?

De GBA beval aan om het aantal veroordelingen te beschouwen en niet het aantal strafbare feiten. De spreekster begrijpt dat de regering heeft vastgehouden aan laatstgenoemde parameter; niet elk strafbaar feit leidt immers tot een veroordeling.

Voor de statistieken doet men een beroep op de ANG. Correcte strafrechtelijke kwalificaties zijn essentieel om binnen de grenzen van de in artikel 90*ter* van het Wetboek van strafvordering bedoelde misdrijven te blijven. De kwalificatie die bij de vaststelling van een misdrijf wordt gegeven, is evenwel slechts voorlopig. Bestaat niet het gevaar dat men bij de vaststelling systematisch zwaarder kwalificeert, wat aanleiding kan geven tot een vertekend beeld? Het is belangrijk dat men zich baseert op correcte statistieken.

De regeling is dermate complex dat mevrouw De Wit zich afvraagt of de actoren op het terrein zich hiermee wel uit de slag kunnen trekken. Zullen de diensten de zones voldoende precies en objectief kunnen bepalen? Als dat niet het geval blijkt, schiet de regeling te kort in het licht van de rechtspraak van het Hof, en dreigt een nieuwe vernietiging.

Een en ander heeft niet enkel betrekking op het statistisch criterium, maar ook op gegevensbewaring op basis van strategische zones. In zijn advies heeft de Raad van State zich daaromtrent kritisch uitgelaten. Als niet duidelijk wordt gemotiveerd waarom een bepaalde zone strategisch is, dreigt dit de regeling onderuit te halen.

Kan de minister van Justitie garanderen dat de verschillende zones voor gegevensbewaring correct en objectief werden bepaald? Het is immers essentieel dat justitie hiermee uit de voeten kan.

Het jaarlijkse evaluatieverslag, bedoeld in de ontworpen paragraaf 6, zal hierbij van groot belang zijn.

De heer Michael Freilich (N-VA) verwijst naar het geval waarbij mensen zich verplaatsen tussen zones waarvoor

des modalités de conservation différentes. Dans leur avis, les opérateurs télécoms indiquent que cela est très difficile à organiser, et seulement à grands frais. Ils soulignent également les complications liées au fait que les zones changeront constamment. Ce n'est donc pas un hasard si ce régime ne s'appliquera que dans cinq ans. Le gouvernement a toutefois prévu une échappatoire, à l'alinéa 6 du paragraphe 4 proposé:"Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données à une zone visée au paragraphe 3, il conserve les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.". En d'autres termes, si le système de conservation ciblée des données mis en place par le gouvernement s'avérait techniquement inapplicable – ce à quoi s'attendent les opérateurs – le projet de loi prévoirait toujours la conservation générale des données. On dit qu'un âne ne trébuche pas deux fois sur la même pierre. Le gouvernement est sur le point de le faire pour la troisième fois.

M. Erik Gilissen (VB) note que l'article 126/1, § 3, proposé, prévoit toute une série de zones dans lesquelles des données peuvent être conservées. Il s'agit de zones stratégiques (3° à 5°), mais aussi de zones géographiques en fonction de criminalité grave identifiée (1°) ou du niveau de menace (2°). Le Roi détermine la taille du périmètre des zones stratégiques; le Parlement n'a donc que peu, voire pas voix au chapitre sur ce point. Le VB craint qu'une grande zone couvrant l'ensemble du territoire ne soit créée, ce qui placerait notre pays en terrain dangereux. Les modifications des zones seront publiées chaque année par un arrêté ministériel; le Parlement n'aura donc pas non plus son mot à dire.

Certes, le paragraphe 6 proposé dispose que le gouvernement doit soumettre à la Chambre des représentants un rapport d'évaluation annuel sur l'application de l'article 126/1 proposé. Toutefois, ce rapport laisse à désirer en termes de transparence; seul le pourcentage du territoire soumis à la conservation des données y sera mentionné. Est-il possible d'accroître la transparence pour les parlementaires, éventuellement par le biais d'une séance à huis clos?

M. Nabil Boukili (PVDA-PTB) rappelle avoir demandé quel pourcentage du territoire serait concerné par la conservation des données en vertu de cet article. Il a reçu comme réponse que "ce n'est pas au ministre de le déterminer" mais qu'il était possible que l'entièreté du territoire soit couverte. L'intervenant craint que cette

verschillende nadere regels inzake bewaring gelden. In hun advies laten de telecomoperatoren uitschijnen dat dit bijzonder moeilijk, en slechts tegen hoge kosten, te organiseren valt. Zij wijzen ook op de complicaties die voortspruiten uit het feit dat de zones voortdurend zullen veranderen. Het is dan ook geen toeval dat deze regeling pas binnen vijf jaar van toepassing zal worden. De regering heeft evenwel een ontsnappingsroute ingebouwd, en wel in het zesde lid van de ontworpen paragraaf 4: "Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot een in paragraaf 3 bedoelde zone, bewaart hij de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden". Met andere woorden, als de door de regering opgezette regeling van gerichte gegevensbewaring technisch onwerkbaar zou blijken – wat inderdaad de verwachting is van de operatoren – dan voorziet het wetsontwerp alsnog in een algemene gegevensbewaring. Men zegt dat een ezel zich geen tweemaal stoot aan dezelfde steen. De regering staat op het punt dat voor een derde keer te doen.

De heer Erik Gilissen (VB) merkt op dat het ontworpen artikel 126/1, § 3, een hele resem zones bepaalt waarin gegevensbewaring kan plaatsvinden. Het gaat onder meer om strategische zones (3° tot 5°), maar ook om geografische zones naargelang van de vastgestelde zware criminaliteit (1°) of het dreigingsniveau (2°). De Koning bepaalt de omvang van de perimeter van de strategische zones; het Parlement heeft daarin dus weinig of geen inspraak. Het VB vreest dat men een grote, het hele grondgebied bestrijkende zone zal zien ontstaan, waarmee ons land zich op gevaarlijk terrein zal begeven. Wijzigingen van de zones worden jaarlijks bekendgemaakt in een ministerieel besluit; ook daaraan komt het Parlement dus niet te pas.

Weliswaar bepaalt de ontworpen paragraaf 6 dat de regering jaarlijks een evaluatieverslag dient uit te brengen aan de Kamer van volksvertegenwoordigers over de toepassing van het ontworpen artikel 126/1. Evenwel laat deze rapportage aan transparantie te wensen over; enkel het percentage van het grondgebied dat aan gegevensbewaring onderhevig is, dient daarin vermeld. Is het mogelijk om de transparantie ten behoeve van de parlementsleden te verhogen, eventueel via een zitting met gesloten deuren?

De heer Nabil Boukili (PVDA-PTB) herinnert aan zijn eerdere vraag naar het percentage van het grondgebied waarop de krachtens dit artikel beoogde gegevensbewaring van toepassing zou zijn. "*Ce n'est pas au ministre de le déterminer*", luidde het letterlijke antwoord, maar eveneens dat het niet uitgesloten was dat het om het

disposition ne puisse aboutir à réintroduire, dans les faits, une obligation de conservation généralisée et indifférenciée des métadonnées. En tant que législateur, M. Boukili rappelle l'obligation de se conformer aux normes européennes et à la Constitution. Dans ce cas-ci, il est indispensable de savoir quel pourcentage de la population et du territoire sera ciblé, pour s'assurer de ne pas réintroduire une conservation généralisée et indifférenciée. Il souhaite avoir une projection de la proportion du territoire et de la population visée. En outre, l'intervenant aimerait savoir comment ce critère a été fixé, et si, dans ce cadre, une estimation du taux de couverture a été réalisée. Il estime pour sa part que le critère devrait être choisi dans l'objectif d'éviter une collecte généralisée en fonction des spécificités du territoire belge.

Sur la définition de la notion de criminalité grave, M. Boukili relève que le gouvernement a indiqué que, selon l'avis du COC, le critère de l'article 90*ter* C.i.cr. est le seul critère utilisable pour déterminer la criminalité grave. Or, selon lui, le gouvernement aurait pu prévoir un nouveau critère dans le projet de loi. À titre d'exemple, il cite Me Catherine Forget qui propose de cibler certaines infractions à partir du seuil de la peine, comme le fait la directive européenne s'appliquant à la collecte et au traitement des données des passagers[2], cette dernière visant pour les "formes graves de criminalité" les infractions passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre. Il se demande pourquoi ne pas avoir suivi ce type de piste.

L'intervenant souhaite également avoir une réponse par rapport aux différences entre la disposition de l'article 90*ter* C.i.cr. qui permet une surveillance ciblée après autorisation par un juge d'instruction et le projet de loi qui concerne une surveillance beaucoup plus générale sans autorisation préalable. Il se demande s'il est possible d'appliquer les mêmes critères à ces deux dispositifs fondamentalement différents.

En réponse à Mme De Wit, qui doute de la faisabilité de la mise en œuvre de la réglementation en projet pour les services compétents, *le ministre de la Justice* souligne

[2] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

hele grondgebied zou gaan. De spreker vreest dat deze bepaling *de facto* kan leiden tot de herinvoering van een verplichting tot veralgemeende en ongedifferentieerde bewaring van de metagegevens. De heer Boukili wijst erop dat een wetgever zich dient te schikken naar de Europese normen en naar de Grondwet. In dit geval is het absoluut noodzakelijk te weten welk percentage van de bevolking en van het grondgebied onder de ontworpen regeling zal vallen, zodat men er zeker van is dat geen veralgemeende, ongedifferentieerde gegevensbewaring ingevoerd wordt. De spreker had graag een prognose gehoord van het beoogde percentage van het grondgebied en van de bevolking. Bovendien wil de spreker weten hoe dat criterium bepaald is en of in dat verband de dekkingsgraad ingeschat geweest is. Zelf vindt hij dat het criterium gekozen zou moeten worden met de bedoeling een veralgemeende gegevensbewaring naargelang van de kenmerken van het Belgische grondgebied te voorkomen.

Wat de definitie van het begrip "zware criminaliteit" betreft, merkt de heer Boukili op dat de regering heeft aangegeven dat volgens het advies van het COC het criterium van artikel 90*ter* van het Wetboek van strafvordering het enige bruikbare is om de zware criminaliteit te definiëren. Volgens hem had de regering evengoed een nieuw criterium in het wetsontwerp kunnen opnemen. Ter illustratie citeert hij meester Catherine Forget, die voorstelt om bepaalde misdrijven vanaf de laagst mogelijke straf in ogenschouw te nemen, zoals het geval is in de Europese richtlijn die van toepassing is op de verzameling en verwerking van de passagiersgegevens[2]. Als "ernstige criminaliteit" beschouwt die richtlijn de strafbare feiten waarop in het nationale recht van een lidstaat een vrijheidsbenemende straf of een tot detentie strekkende maatregel met een maximumduur van ten minste drie jaar staat. Hij vraagt zich af waarom dat spoor niet gekozen is.

Ook had de spreker graag een antwoord gehad op de vraag naar de verschillen tussen artikel 90*ter* van het Wetboek van strafvordering., dat doelgericht toezicht na toestemming van een onderzoeksrechter mogelijk maakt, en het wetsontwerp, dat in een veel algemener toezicht zonder voorafgaande toestemming voorziet. Hij vraagt zich af of op die twee fundamenteel verschillende ingrepen wel dezelfde criteria kunnen worden toegepast.

Ter attentie van mevrouw De Wit, die betwijfelt of de ontworpen regeling werkbaar is voor de bevoegde diensten, merkt *de minister van Justitie* op dat die laatste

[2] Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

que ces services (le COC, le service NTSU et la Direction de l'information policière et des moyens ICT de la Police fédérale) ont été étroitement associés à la préparation du projet de loi à l'examen. En effet, ces services y ont apporté leur contribution et le gouvernement a fixé le cadre, en tenant compte de la jurisprudence de la Cour de justice de l'Union européenne.

Dans le cadre de la définition des zones stratégiques, le gouvernement a utilisé les éléments de base fournis par la Cour de justice de l'Union européenne (les parlements, les domaines militaires, les ports, etc.). Ces zones sont énumérées dans le projet de loi à l'examen. L'affirmation de M. Gilissen selon laquelle le Parlement n'a pas grand-chose à dire en la matière est donc fausse. Si Mme De Wit ne souscrit pas à la reconnaissance de la nature stratégique d'une zone donnée, le ministre est disposé à en débattre.

Le ministre de la Justice défend l'inscription des autoroutes sur la liste des zones stratégiques, à propos de laquelle certains membres avaient formulé des observations. Or, des phénomènes criminels comme le trafic d'êtres humains ou le trafic de drogues se produisent sur ces axes de circulation ou les acteurs de ces phénomènes y passent.

Au total, environ 30 % du territoire constituera une zone stratégique, ce qui montre avant tout que la Belgique est un pays de petite taille densément peuplé.

Il est exact que les opérateurs disposeront de cinq ans pour s'adapter à la réglementation en projet. Contrairement à ce que laisse entendre M. Freilich, l'alinéa 6 du § 4 en projet ne traduit pas l'impossibilité technique de la mise en œuvre de la réglementation à l'examen. Si un individu se déplace au sein d'une zone où différentes périodes de rétention sont prévues, la durée de conservation des données qui en découlent sera la plus courte prévue. L'alinéa en question concerne le cas où un opérateur technique n'est pas en mesure de localiser un appareil dans une zone précise. Cela ne vaudra que si l'ensemble du territoire est couvert. Dans le cas contraire, l'opérateur pourra effacer les données en question.

S'agissant du critère statistique, le ministre de la Justice souligne qu'il est effectivement possible d'isoler, dans la BNG, les infractions visées à l'article 90*ter* du Code d'Instruction criminelle. Le COC est justement chargé de réprimer toute manipulation des données de la BNG. Cet organe de contrôle effectuera en permanence des vérifications. Cet exercice statistique devra être réalisé chaque année.

– het COC, de NTSU, de Directie van de politionele informatie en de ICT-middelen van de Federale Politie – nauw betrokken zijn geweest bij de voorbereiding van het voorliggende wetsontwerp. Zij hebben input gegeven, en de regering heeft het kader vastgesteld, rekening houdend met de rechtspraak van het HvJ-EU.

Zo werd er bij het bepalen van de strategische zones gebruik gemaakt van de kapstokken aangereikt door het HvJ-EU (parlementen, militaire domeinen, havens enzovoort). De zones staan opgelijst in het wetsontwerp. De bewering van de heer Gilissen dat het Parlement ter zake niets in de pap te brokken heeft, klopt dus niet. Als mevrouw De Wit het oneens is met de omschrijving van een gegeven zone als strategisch, is de minister bereid daarover een debat te voeren.

De minister van Justitie verdedigt de opname van autosnelwegen in de lijst van strategische zones, waarbij bepaalde leden kanttekeningen hadden geplaatst. Het is op deze verkeersassen dat criminele fenomenen als mensen- en drugshandel zich afspelen of waarlangs zij passeren.

In totaal zal ongeveer 30 % van het grondgebied een strategische zone uitmaken, wat in de eerste plaats aantoont dat België een klein en dichtbevolkt land is.

Het klopt dat de operatoren vijf jaar tijd krijgen om zich aan te passen. Anders dan de heer Freilich suggereert, duidt de opname van het zesde lid van de ontworpen paragraaf 4 geenszins op de technische onmogelijkheid van de voorliggende regeling. Als iemand zich verplaatst tussen een gebied met verschillende retentieperiodes, worden de gegevens bewaard gedurende de kortste bewaringstermijn. Het bewuste lid ziet op de situatie waarin de operator technisch niet in staat is om een toestel te situeren in een precies gebied. Het geldt enkel als heel het territorium wordt gedekt; als dat niet het geval is, mag de operator de gegevens wissen.

Wat het statistisch criterium betreft, benadrukt de minister van Justitie dat het wel degelijk mogelijk is de in artikel 90*ter* van het Wetboek van strafvordering bedoelde misdrijven te isoleren in de ANG. Het is precies de taak van het COC om elke manipulatie van de ANG-gegevens tegen te gaan. Dat controleorgaan zal voortdurend verificaties uitvoeren. De statistische oefening zal elk jaar moeten worden gemaakt.

Le ministre méconnaîtrait le rôle crucial joué par le COC s'il pouvait aujourd'hui donner un chiffre pour le pourcentage du territoire qui, selon le critère statistique, relèvera du champ d'application du dispositif de conservation des données. S'il apparaissait qu'il s'agissait de l'ensemble du territoire, cela ne signifierait toutefois pas encore que le délai de conservation serait partout de douze mois. En effet, des délais de six ou de neuf mois pourraient être appliqués aux zones à plus faible criminalité. Le ministre de la Justice indique qu'il s'agit d'un tableau réaliste: une conservation applicable à l'ensemble du territoire, mais prévoyant une différenciation en matière de délais. C'est également indiqué tel quel dans l'exposé des motifs. Cet exercice devant être répété chaque année, sa date de réalisation pourra également varier.

En réponse à une question de Mme De Wit, le ministre de la Justice indique que la qualification de l'infraction est revue à la baisse *a posteriori* dans moins d'un pour cent des procès-verbaux. Ce décompte est effectué au moyen du système de gestion des informations (*information management system*) de la BNG et a été validé par le COC dans le cadre d'un test à blanc.

Mme Sophie De Wit (N-VA) répète qu'elle ne formule aucune objection de principe contre des zones de conservation de données très larges sur le plan géographique lorsque c'est à des fins judiciaires. Son inquiétude concerne surtout, dans le cas présent, le manque de clarté et d'objectivité des critères, avec pour conséquence que le projet de loi à l'examen pourrait être contraire à la jurisprudence de la Cour de justice de l'Union européenne et qu'il pourrait, à terme, porter préjudice à des enquêtes pénales. Cette préoccupation est partagée par le Conseil d'État.

En outre, l'intervenant juge problématique que le cadre de la rétention d'informations effectuée à des fins judiciaires soit, à juste titre, particulièrement strict, mais que le cadre de la conservation de données effectuée à d'autres fins le soit beaucoup moins.

M. Erik Gilissen (VB) souligne que son groupe considère que la lutte contre la criminalité constitue une priorité et rappelle qu'il a interpellé à deux reprises, en 2021, la ministre des Télécommunications à propos de la conservation de données ("L'annulation de la loi sur la conservation des données par la Cour constitutionnelle", interpellation 55000122I, CRIV 55 COM 457 et "L'obligation de conserver les données des utilisateurs" interpellation 55000154I, CRIV 55 COM 533).

De minister zou de cruciale rol van het COC miskennen mocht hij nu een cijfer kunnen plakken op het percentage van het grondgebied dat onder de gegevensbewaring volgens het statistisch criterium zou vallen. Mocht dit het gehele grondgebied blijken te zijn, wil dat nog niet zeggen dat de bewaartermijn overal twaalf maanden zou zijn; in gebieden met minder criminaliteit zouden termijnen van zes of negen maanden kunnen gelden. Volgens de minister van Justitie is dit een realistisch beeld: een bewaring die het hele grondgebied dekt, maar met een differentiatie in de bewaringtermijnen. Dit is ook zo aangegeven in de memorie van toelichting. Vermits de oefening jaarlijks moet worden overgedaan, kan dit ook wisselen in de tijd.

In antwoord op een vraag van mevrouw De Wit geeft de minister van Justitie aan dat in minder dan 1 % van de processen-verbaal de kwalificatie van het strafbaar feit achteraf naar beneden wordt bijgesteld. Deze telling gebeurt volgens het *information management system* van de ANG en is gevalideerd door het COC in het kader van een *dry run*.

Mevrouw Sophie De Wit (N-VA) herhaalt dat zij principieel geen bezwaar heeft tegen ruim opgevatte geografische gegevensbewaringszones voor justitiële doeleinden. Haar bezorgdheid is in dezen vooral dat de criteria onvoldoende duidelijk en objectief zouden zijn, waardoor men in aanvaring komt met de rechtspraak van het HvJ-EU en op termijn strafrechtelijke onderzoeken in het gedrang zouden kunnen komen. Deze bekommering wordt gedeeld door de Raad van State.

Daarnaast vindt zij het problematisch dat de retentie voor justitiële doeleinden – terecht – bijzonder strikt omkaderd wordt, maar dat dat voor gegevensbewaring voor andere finaliteiten veel minder het geval is.

De heer Erik Gilissen (VB) onderstreept dat criminaliteitsbestrijding een prioriteit is voor zijn fractie en herinnert eraan dat hij in 2021 de minister van Telecommunicatie tweemaal interpelleerde over dataretentie ("De vernietiging van de dataretentiewet door het Grondwettelijk Hof", interpellatie 55000122I, CRIV 55 COM 457 en "De verplichte bewaring van gebruikersdata", interpellatie 55000154I, CRIV 55 COM 533).

M. Gilissen redoute que l'article 9 débouche sur l'apparition d'une grande zone nationale, ce qui nous promettrait une nouvelle annulation par la Cour constitutionnelle.

M. Nabil Boukili (PVDA-PTB) retient de la réponse du ministre de la Justice que la conservation des données sera effectivement généralisée. Il demande également au ministre quelle est la raison précise pour laquelle le gouvernement a opté pour le critère de trois infractions graves par 1 000 habitants et par an.

Le ministre de la Justice a précisé dans son exposé introductif ainsi qu'au cours de la discussion générale ce en quoi consisterait concrètement ce critère pour trois arrondissements correspondant à de grandes villes. Les chiffres de la criminalité précités sont de nature à indiquer un problème non négligeable de criminalité.

M. Nabil Boukili déduit de la réponse du ministre de la Justice que les habitants de Bruxelles, d'Anvers et de Charleroi seront placés sous surveillance généralisée.

Le ministre de la Justice réfute cette conclusion. En effet, une surveillance généralisée impliquerait que l'État conserve toutes les données. Or, le projet de loi à l'examen instaure un dispositif réglant une conservation de données par les opérateurs, lesquelles pourront être demandées par les autorités publiques dans le respect de conditions et de modalités strictes. Cette conservation sera différenciée à l'aide de critères objectifs.

Art. 9/1 (*nouveau*)

Le gouvernement présente l'*amendement n° 3* (DOC 55 2572/002) tendant à insérer un article 9/1 visant à son tour à insérer un article 126/2 rédigé comme suit:

"Art. 126/2. § 1er. Pour l'application du présent article, il y a lieu d'entendre par: "Communication": toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit.

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

De heer Gilissen is bezorgd dat artikel 9 kan resulteren in het ontstaan van één grote, landelijke zone, waardoor we zouden afstevenen op een nieuwe vernietiging door het Grondwettelijk Hof.

De heer Nabil Boukili (PVDA-PTB) onthoudt uit het antwoord van de minister van Justitie dat de gegevensbewaring inderdaad algemeen is. Hij had nog graag van de minister vernomen waarom de regering precies het criterium van drie zware strafbare feiten per 1 000 inwoners per jaar heeft gekozen.

De minister van Justitie verduidelijkte in zijn inleidende uiteenzetting alsook tijdens de algemene bespreking wat dit criterium concreet zou betekenen voor drie grootstedelijke arrondissementen. De geciteerde criminaliteitscijfers zijn van aard om te wijzen op een niet-onaanzienlijke criminaliteitsproblematiek.

De heer Nabil Boukili leidt uit het antwoord van de minister van Justitie af dat de inwoners van Brussel, Antwerpen en Charleroi onder een algemeen toezicht zullen worden geplaatst.

De minister van Justitie betwist deze conclusie. Algemeen toezicht houdt in dat de overheid alle gegevens bijhoudt. De voorliggende tekst regelt een gegevensbewaring door de operatoren, die de overheid onder strikte voorwaarden en volgens strikte nadere regels kan opvragen. De bewaring is gedifferentieerd aan de hand van objectieve criteria.

Art. 9/1 (*nieuw*)

De regering dient *amendement nr. 3* (DOC 55 2572/002) in, dat beoogt een artikel 9/1 in te voegen, strekkende op zijn beurt tot invoeging van een artikel 126/2, luidende:

"Art. 126/2. § 1. Voor de toepassing van dit artikel wordt verstaan onder "communicatie", informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een publiek beschikbare elektronische-communicatiedienst, met uitsluiting van de informatie die via een openbare omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gelinkt aan de identificeerbare abonnee of gebruiker die deze informatie ontvangt.

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

électroniques qui permettent la fourniture de ces services, sont les suivantes:

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

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

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

4° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

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

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

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

8° pour ce qui concerne les services de communications électroniques mobiles, la date et l'heure de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement au réseau en raison de l'extinction de cet équipement;

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

10° les autres identifiants relatifs au destinataire de la communication électronique, à son équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, après avis de l'Autorité

aanbieden die het aanbieden van die diensten mogelijk maken, zijn de volgende:

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

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

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

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

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

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

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

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

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

10° de andere *identifiers* met betrekking tot de geadresseerde van de elektronische communicatie, tot zijn eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, na

de protection des données et de l'Institut, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

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

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

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

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

Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les exigences en matière de précision et de fiabilité auxquelles les données visées au présent article doivent répondre.".

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

Art. 10

Cet article modifie l'article 127, § 2, de la loi du 13 juin 2005. Cette modification découle de l'inscription des règles relatives aux systèmes d'encryptage à l'article 107/5.

Le gouvernement présente l'*amendement n° 6* (DOC 55 2572/002) tendant à remplacer l'article en projet par ce qui suit:

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

Il est interdit de distribuer en Belgique, en ce compris par internet, aux utilisateurs finaux, sans l'accord de

advies van de Gegevensbeschermingsautoriteit en het Instituut, op voorwaarde dat dit besluit door de wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

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

Het koninklijk besluit bedoeld in het eerste lid, 10°, slaat niet op de inhoud van de elektronische communicatie.

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

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

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten inzake nauwkeurigheid en betrouwbaarheid bepalen waaraan de gegevens bedoeld in dit artikel moeten beantwoorden.".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 10

Met dit artikel wordt paragraaf 2 van artikel 127 van de wet van 13 juni 2005 gewijzigd. Deze wijziging is het gevolg van het feit dat de regels inzake encryptiesystemen voortaan opgenomen zijn in artikel 107/5.

De regering dient *amendement nr. 6* (DOC 55 2572/002) in, dat ertoe strekt het ontworpen artikel te vervangen als volgt:

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

Het is verboden om in België, inclusief via het internet, zonder het akkoord van de buitenlandse onderneming

l'entreprise étrangère qui fournit le service de communications électroniques accessible au public:

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

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

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

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

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

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

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

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

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

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

4° "méthode d'identification indirecte": méthode par laquelle l'opérateur collecte et conserve des données

die de voor het publiek beschikbare elektronische-communicatiedienst verstrekt, het volgende aan te bieden aan de eindgebruikers:

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

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

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

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

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

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

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

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

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

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

4° "indirecte identificatiemethode": methode waarbij de operator gegevens verzamelt en bewaart aan de hand

qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés.

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

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

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

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

— les autres services déterminés par le Roi.

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

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

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

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

waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen;

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

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

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

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

— de andere diensten bepaald door de Koning.

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

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

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

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

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

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

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

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

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

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

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

— que ce document est relatif à la personne identifiée.

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

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

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

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

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

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

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

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

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

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

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

— dat dit document betrekking heeft op de geïdentificeerde persoon.

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

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

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

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

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

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

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

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

1° la carte d'identité électronique belge;

2° le passeport belge;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1° de Belgische elektronische identiteitskaart;

2° het Belgisch paspoort;

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

4° de beperkte verblijfstitel (A-kaart);

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

6° de onbeperkte verblijfstitel (B-kaart);

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

8° de vestigingsvergunning (K-kaart);

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

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

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

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

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

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

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

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

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

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

19° la carte bleue européenne (carte H);

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

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

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

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

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

25° l'acte de notoriété;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25° de akte van bekendheid;

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

27° het attest van immatriculatie (oranje kaart);

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

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

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

31° le passeport étranger;

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

Les opérateurs qui disposent de points de vente permettent à leurs abonnés de s'identifier à l'aide de n'importe lequel des documents d'identification visés à l'alinéa 1er, dans le cadre d'au moins une méthode d'identification de leur choix.

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

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

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

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

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

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

31° het buitenlands paspoort;

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

De operatoren die over fysieke verkooppunten beschikken, maken het voor hun abonnees mogelijk om zich te identificeren aan de hand van om het even welke van de in het eerste lid bedoelde identificatiedocumenten, in het kader van minstens één identificatiemethode van hun keuze.

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

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

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

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

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

1° le nom et le prénom;

2° la nationalité;

3° la date de naissance;

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

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

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

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

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

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

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

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

§ 9. L'opérateur permet aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'identifier ses abonnés par le biais d'une méthode d'identification indirecte:

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

1° de naam en voornaam;

2° de nationaliteit;

3° de geboortedatum;

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

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

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

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

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

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

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

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

§ 9. De operator maakt het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, mogelijk om zijn abonnees te identificeren via een indirecte identificatiemethode:

1° en conservant, en exécution de l'article 126 et pendant les délais prévus par cet article, l'adresse IP ayant servi à la souscription au service de communications électroniques ou à son activation, l'adresse IP à la source de la connexion et les données qui doivent être conservées avec ces adresses, ou;

2° en collectant et conservant le numéro de téléphone de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné conformément au présent article, ou;

3° en cas de paiement en ligne spécifique à la souscription d'un service de communications électroniques, en collectant et conservant:

— la référence de l'opération de paiement, et;

— le nom, le prénom, l'adresse du domicile et la date de naissance déclarés par la personne physique qui est l'abonné de l'opérateur ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir son obligation en matière d'identification, ou;

4° en cas de carte SIM ("*subscriber identity/identification module*") ou toute autre carte équivalente intégrée dans un véhicule, en collectant et conservant le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte;

5° en cas de souscription d'un abonné qui réside dans un centre fermé ou un lieu d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers à un service de communications électroniques mobile fourni au moyen d'une carte prépayée, en collectant et conservant le nom et le prénom de l'abonné, son numéro de sécurité publique, à savoir le numéro de dossier attribué par l'Office des Étrangers et les coordonnées du centre ou du lieu d'hébergement où la souscription a eu lieu, ou;

6° en cas de souscription à un service de communications électroniques par une personne morale au nom et pour le compte d'une personne physique qui rencontre des difficultés à effectuer cette souscription, en collectant et conservant la dénomination précise de cette personne morale et, pour ce qui concerne cette personne physique, au minimum son nom, son prénom, son adresse de résidence, lorsqu'elle en dispose, sa date de naissance et le numéro par lequel elle est identifiée,

1° door de bewaring, overeenkomstig artikel 126 en gedurende de in dat artikel bepaalde termijnen, van het IP-adres dat werd gebruikt om zich op de elektronische-communicatiedienst in te tekenen of om deze dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij bewaard moeten worden, of;

2° door de vergaring en bewaring van het telefoonnummer van de abonnee dat werd toegewezen in het kader van een elektronische-communicatiebetaaldienst waarvoor een operator de abonnee moet identificeren krachtens onderhavig artikel, of;

3° in geval van een onlinebetaling specifiek voor de intekening op een elektronische-communicatiedienst, door de vergaring en bewaring van:

— het kenmerk van de betalingsverrichting, en;

— de naam, de voornaam, het verblijfadres en de geboortedatum opgegeven door de natuurlijke persoon die de abonnee van de operator is of die handelt voor rekening van een rechtspersoon die de abonnee van de operator is, teneinde zijn verplichtingen inzake identificatie te vervullen, of;

4° in geval van een simkaart ("*subscriber identity/identification module*") of andere gelijkwaardige kaart die in een voertuig wordt ingebouwd, door de vergaring en bewaring van het chassisnummer van het voertuig en van de link tussen het chassisnummer en het nummer van de kaart;

5° in geval van een intekening van een abonnee die in een gesloten centrum of woonunit verblijft in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op een mobiele elektronische-communicatiedienst verstrekt door middel van een voorafbetaalde kaart, door de vergaring en bewaring van de naam en de voornaam van de abonnee, zijn openbaar veiligheidsnummer, zijnde het door de Dienst Vreemdelingenzaken toegekende dossiernummer, en de contactgegevens van het centrum of de woonunit waar de intekening heeft plaatsgevonden, of:

6° in geval van intekening op een elektronische-communicatiedienst door een rechtspersoon namens en voor rekening van een natuurlijke persoon die moeilijkheden heeft om die intekening te verrichten, door de vergaring en bewaring van de precieze benaming van de rechtspersoon en, wat de natuurlijke persoon in kwestie betreft, minimaal zijn naam, zijn voornaam, zijn verblijfadres als hij dat heeft, zijn geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals

tel un numéro de registre national, ces informations lui étant transmises par cette personne morale.

Pour l'application de l'alinéa 1er, 6°, la personne morale:

1° doit, avant de pouvoir souscrire à un service de communications électroniques pour la personne physique, obtenir un agrément, délivré par le ministre et le ministre de la Justice, et ayant pour objet de vérifier qu'elle respecte les valeurs démocratiques inscrites dans la Constitution ainsi que le présent article;

2° s'identifie auprès de l'opérateur conformément au présent article;

3° identifie les abonnés à l'aide d'un des documents d'identification visés au paragraphe 5, conformément aux exigences de fiabilité visées au paragraphe 4, ou à l'aide d'une autre méthode autorisée dans l'agrément visé au 1°;

4° conserve une copie du document d'identification des abonnés autre que la carte d'identité électronique belge, sauf dérogation accordée dans l'agrément visé au 1°;

5° conserve une liste actualisée permettant de faire le lien entre le service de communications électroniques et les abonnés, comprenant au minimum le nom, le prénom, l'adresse de la résidence, lorsque la personne en dispose, la date de naissance et le numéro par lequel elle est identifiée, tel le numéro de registre national.

Le Roi peut:

1° prévoir par méthode visée à l'alinéa 1er les conditions à respecter, une condition pouvant être l'obtention d'une autorisation préalable du ministre et du ministre de la Justice;

2° imposer des obligations aux opérateurs, aux personnes morales visées à l'alinéa 1er, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 10. Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

een rijksregisternummer, welke hem wordt meegedeeld door de rechtspersoon.

Voor de toepassing van het eerste lid, 6°:

1° moet de rechtspersoon, alvorens te kunnen intekenen op een elektronische-communicatiedienst voor de natuurlijke persoon, een erkenning verkrijgen, verstrekt door de minister en de minister van Justitie, en met als voorwerp om na te gaan dat de persoon de democratische waarden vastgelegd in de Grondwet alsook dit artikel nakomt;

2° identificeert de rechtspersoon zich bij de operator overeenkomstig dit artikel;

3° identificeert de rechtspersoon de abonnees aan de hand van een van de identificatiedocumenten bedoeld in paragraaf 5, conform de vereisten inzake betrouwbaarheid bedoeld in paragraaf 4, of aan de hand van een andere methode die toegestaan is in de in de bepaling onder 1° bedoelde erkenning;

4° bewaart de rechtspersoon een kopie van het andere identificatiedocument van de abonnees dan de Belgische elektronische identiteitskaart, behoudens afwijking toegestaan in de in de bepaling onder 1° bedoelde erkenning;

5° bewaart de rechtspersoon een geactualiseerde lijst aan de hand waarvan het verband kan worden vastgesteld tussen de elektronische-communicatiedienst en de abonnees, met daarin ten minste de naam, de voornaam, het verblijfadres als de persoon dat heeft, de geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals het rijksregisternummer.

De Koning kan:

1° per in het eerste lid vermelde methode de voorwaarden vastleggen die moeten worden nageleefd, waarbij een voorwaarde het verkrijgen van een voorafgaande machtiging van de minister en van de minister van Justitie kan zijn;

2° verplichtingen opleggen aan de operatoren, aan de in het eerste lid bedoelde rechtspersonen, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 10. Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

Pour les services de communications électroniques mobiles fournis au moyen d'une carte prépayée, le Roi:

1° restreint la possibilité pour l'abonné de permettre à des tiers de bénéficier du service;

2° impose des obligations aux abonnés qui sont des personnes morales afin de déterminer les utilisateurs habituels du service.

L'opérateur qui offre une carte SIM ou toute carte équivalente, destinée à être intégrée dans un véhicule, conserve le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte. À la demande d'une autorité, l'opérateur ne lui communique que ce numéro de châssis ou le numéro de cette carte.

Le Roi peut fixer les modalités de l'obligation visée à l'alinéa 3 et peut imposer aux entreprises qui disposent du numéro de châssis de le transmettre aux opérateurs.

§ 11. Si un opérateur ne respecte pas les mesures qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

Les opérateurs déconnectent les abonnés qui ne respectent pas les mesures qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces abonnés ne sont en aucune manière indemnisés pour la déconnexion.

L'arrêté royal visé dans le présent article est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres.".

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

Art. 11

Cet article vise à insérer un article 127/1 dans la loi du 13 juin 2005. Il énumère notamment les autorités

De Koning, voor de mobiele elektronische-communicatiediensten verstrekt op basis van een voorafbetaalde kaart:

1° beperkt de mogelijkheid voor de abonnee om derden gebruik te laten maken van de dienst;

2° legt verplichtingen aan de abonnees die rechtspersonen zijn op om de gewoonlijke gebruikers van de dienst te identificeren.

De operator die een simkaart of een gelijkwaardige kaart aanbiedt die bestemd is om in een voertuig te worden ingebouwd, bewaart het chassisnummer van dat voertuig, evenals de link tussen het chassisnummer en het nummer van deze kaart. Op verzoek van een autoriteit deelt de operator haar enkel dat chassisnummer of het nummer van deze kaart mee.

De Koning kan de nadere bepalingen van de verplichting bedoeld in het derde lid vastleggen en kan de ondernemingen die over het chassisnummer beschikken, verplichten om dat door te geven aan de operatoren.

§ 11. Indien een operator niet voldoet aan de hem door dit artikel of door de Koning opgelegde maatregelen, is het hem verboden de dienst waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.

De operatoren sluiten de abonnees die niet voldoen aan de hen door dit artikel of door de Koning opgelegde maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die abonnees worden op geen enkele wijze vergoed voor de afsluiting.

Het koninklijk besluit bedoeld in dit artikel wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad.".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 11

Dit artikel strekt ertoe een artikel 127/1 in te voegen in de wet van 13 juni 2005. Het somt onder meer de

pouvant avoir accès aux données conservées et décrit la finalité et les modalités de cet accès.

Mme Sophie De Wit (N-VA) souligne que l'article 127/1 proposé soulève des questions en ce qui concerne la protection de la vie privée. Il contient en effet une liste de finalités sur laquelle il conviendra de se baser pour déterminer quelles autorités peuvent demander les données conservées aux opérateurs.

Le § 1er en projet définit la notion de "criminalité grave". L'intervenante souligne que cette définition diffère de celle de l'article 126/1 en projet, qui renvoie à l'article 90*ter* du Code d'instruction criminelle. L'article 127/1 en projet renvoie quant à lui à la peine minimale d'emprisonnement correctionnel principal visée à l'article 88*bis*, alinéa 1er, du même Code, à des niveaux de sanction prévus dans le Code de droit économique, et au Règlement (UE) n° 596/2014. Quelles sont les raisons qui justifient l'utilisation d'une définition différente de la criminalité grave dans cet article?

L'exposé des motifs indique que l'article 127/1 vise à désigner les autorités en fonction d'une liste de finalités poursuivies et qu'il ne contient plus une liste détaillée d'autorités car cette liste risquerait de se révéler rapidement incomplète.

Pour garantir la transparence, le § 5 proposé dispose qu'une circulaire établissant une liste de toutes les autorités habilitées devra être publiée. L'intervenante présume que le ministre dispose déjà de cette liste. Il s'agit en effet des autorités qui sont actuellement habilitées par une norme législative formelle à réclamer des données conformément aux §§ 2 et 4 proposés de l'article 127/1.

La liste des finalités poursuivies renvoie non seulement aux services de renseignement et de sécurité et aux "autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique", mais aussi aux autorités administratives. La presse en a conclu que le fisc pourra notamment réclamer certaines données.

L'intervenante demande au ministre quelles autorités sont actuellement habilitées par une norme législative formelle à demander des données d'identification et/ou des métadonnées. Elle déplore que la liste de finalités figurant à l'article en projet soit si longue. Les §§ 2 à 4 en projet permettent en outre de délivrer de nouvelles autorisations à l'avenir par le biais de nouvelles normes

autoriteiten op die toegang kunnen hebben tot de bewaarde gegevens en omschrijft de finaliteit en de nadere regels van die toegang.

Mevrouw Sophie De Wit (N-VA) stipt aan dat het ontworpen artikel 127/1 vragen oproept over de bescherming van de privacy. Het bevat immers een lijst met beoogde doeleinden op basis waarvan bepaald wordt welke autoriteiten de bewaarde gegevens mogen opvragen bij de operatoren.

In de ontworpen paragraaf 1 wordt het begrip "zware criminaliteit" omschreven. De spreekster wijst erop dat dit een andere omschrijving is dan in het ontworpen artikel 126/1, waarin wordt verwezen naar artikel 90*ter* van het Wetboek van strafvordering In het voorliggende artikel wordt daarentegen verwezen naar de minimale correctionele hoofdgevangenisstraf zoals bedoeld in artikel 88*bis*, eerste lid, van datzelfde Wetboek, naar sanctieniveaus zoals bepaald in het Wetboek van economisch recht en naar Verordening (EU) nr. 596/2014. Is er een reden waarom zware criminaliteit in het voorliggende artikel anders omschreven wordt?

In de memorie van toelichting wordt verklaard dat het ontworpen artikel 127/1 ertoe strekt de autoriteiten aan te wijzen op basis van een lijst van nagestreefde doeleinden en dat het niet langer een uitvoerige lijst van autoriteiten bevat. Een dergelijke lijst kan immers te snel onvolledig blijken.

Om de transparantie te verzekeren, stipuleert de ontworpen paragraaf 5 dat er een omzendbrief bekendgemaakt moet worden met alle gemachtigde autoriteiten. De spreekster gaat ervan uit dat de minister al over een dergelijke lijst beschikt. Het gaat immers over de autoriteiten die thans door een formele wettelijke norm gemachtigd zijn om gegevens op te vragen, zoals bepaald in de ontworpen paragrafen 2 tot 4 van het voorliggende artikel.

In de lijst met nagestreefde doeleinden wordt niet alleen verwezen naar de inlichtingen- en veiligheidsdiensten en "de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid", maar ook naar administratieve autoriteiten. Dat deed in de pers de indruk ontstaan dat onder andere de belastingdienst bepaalde gegevens mag opvragen.

De spreekster zou graag van de minister vernemen welke autoriteiten thans door een formele wettelijke norm gemachtigd zijn om identificatie- en/of metagegevens op te vragen. Ze laakt het feit dat de in het ontworpen artikel opgenomen lijst met doeleinden erg ruim is opgevat. De ontworpen paragrafen 2 tot 4 laten eveneens de mogelijkheid open om in de toekomst nog andere machtigingen

législatives. Il n'existe donc aucune garantie quant à l'identification des autorités ayant déjà accès aux données concernées, ni des autorités qui y auront accès à l'avenir. Les autorités pourront du reste également demander des données dans des dossiers non liés à des faits de criminalité grave.

M. Erik Gilissen (VB) indique qu'il partage les préoccupations de l'intervenante précédente, en particulier en ce qui concerne la liste des finalités sur laquelle il faudra se baser pour déterminer les autorités compétentes. Le 5° de l'article 127/1, § 2, proposé renvoie par exemple aux "autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques" et le 8° évoque "les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave". Cette liste n'ouvre-t-elle pas la porte à une situation dans laquelle à peu près n'importe quelle autorité pourra demander des données dans une grande variété de situations?

M. Nabil Boukili (PVDA-PTB) constate que les finalités de l'accès aux données conservées définies à l'article 127/1 § 2, en projet ne coïncident pas entièrement avec les finalités qui avaient été fixées pour la conservation des données. En effet, les données conservées dans le cadre de la lutte contre la fraude pourront également être demandées par les autorités judiciaires pour un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave.

Dans son avis n° 108/2021, l'APD a constaté que cette disposition n'est pas conforme à la jurisprudence de la CJUE, en vertu de laquelle "l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs […] ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs." (La Quadrature du Net, affaires jointes C-511/18, C-512/18 et C-520/18, § 166). Ce n'est que lorsque des données ont été conservées aux fins de lutter contre la criminalité grave que l'accès à ces données peut être justifié par l'objectif de protection de la sécurité nationale. L'APD a demandé au gouvernement de retravailler l'avant-projet afin d'y inclure cette restriction. Quelle est la position du ministre à ce sujet?

La ministre des Télécommunications rappelle que les autorités administratives mentionnées dans la liste

toe te kennen via nieuwe wettelijke normen. Er zijn dan ook geen garanties over welke autoriteiten al toegang hebben tot de betrokken gegevens en welke die toegang in de toekomst nog zullen krijgen. Bovendien kunnen ze ook gegevens opvragen in dossiers die losstaan van zware criminaliteit.

De heer Erik Gilissen (VB) geeft aan dat hij de bezorgdheid van de vorige spreekster deelt, meer bepaald inzake de lijst met doeleinden op basis waarvan de autoriteiten worden bepaald. De bepaling onder 5°, van het ontworpen artikel 127/1, § 2, heeft bijvoorbeeld betrekking op "de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronischecommunicatienetwerk of -dienst" en de bepaling onder 8° verwijst naar "de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt." Zet deze lijst de deur niet open naar een situatie waarin zowat alle autoriteiten in de meest uiteenlopende scenario's gegevens kunnen opvragen?

De heer Nabil Boukili (PVDA-PTB) merkt op dat de doeleinden van de toegang tot bewaarde gegevens zoals bepaald in het ontworpen artikel 127/1, § 2, niet volledig overeenstemmen met de doeleinden die bepaald werden voor de bewaring van de gegevens. Gegevens die bewaard worden in het kader van fraudebestrijding kunnen immers eveneens opgevraagd worden door gerechtelijke overheden in het raam van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt.

De GBA merkt in haar advies nr. 108/2021 op dat dit niet in overeenstemming is met de rechtspraak van het HvJ-EU, dat stelde dat "de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommmunicatiediensten worden bewaard (…), in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd." (*La Quadrature du Net*, gevoegde zaken C-511/18, C-512/18 en C-520/18, paragraaf 166) Enkel in het geval van gegevens die bewaard werden met het oog op de bestrijding van zware criminaliteit kan de toegang daartoe gerechtvaardigd worden op grond van de doelstelling van de bescherming van de nationale veiligheid. De GBA verzocht de regering het voorontwerp te herzien om deze beperking in de tekst op te nemen. Wat is het standpunt van de minister op dit stuk?

De minister van Telecommunicatie stipt aan dat de administratieve autoriteiten zoals bedoeld in de voormelde

précitée ne sont sollicitées qu'en cas d'infractions très spécifiques. Il s'agit, par exemple, de fraudes en ligne ou d'infractions sur le plan de la santé publique. Dans ces cas, les autorités concernées reprennent de plus en plus de tâches du parquet.

La ministre souligne toutefois que l'article à l'examen doit être considéré comme une disposition-cadre, imposant une double condition aux autorités concernées. Premièrement, elles doivent agir en vue d'atteindre l'une des finalités fixées dans le paragraphe 2 en projet. Deuxièmement, il doit également exister une base législative organique ou sectorielle autorisant ces autorités à demander les métadonnées des opérateurs. Cette norme législative formelle doit, conformément au paragraphe 5 en projet, préciser ce qui suit: les catégories d'entreprises auxquelles l'autorité peut demander des données, les catégories de données qui peuvent être demandées, les finalités poursuivies et les mécanismes de contrôle de la demande de données. En raison des deux conditions susmentionnées, la ministre estime que la liste des finalités n'est pas conçue de manière trop large.

Dans le cadre de certaines infractions en ligne, il est possible que même des autorités administratives aient besoin d'adresses IP ou de métadonnées pour investiguer sur des faits. La CJUE a confirmé dans l'arrêt *La Quadrature du Net* que l'adresse IP est parfois le seul élément pouvant être utilisé pour poursuivre certaines infractions en ligne.

En outre, l'article 127/1, § 4, alinéa 1er, en projet, réduit le nombre de finalités permettant d'accéder aux données conservées en vertu de l'article 126/1 en projet. Il n'est donc pas exact que l'article en projet ne serait pas conforme à la réglementation européenne.

Le ministre de la Justice explique pourquoi, dans l'article à l'examen, la criminalité grave est définie au moyen de l'article 88*bis* du Code d'instruction criminelle au lieu de l'article 90*ter* du même Code. Le Collège des procureurs généraux indique, dans son avis à la commission sur le projet de loi à l'examen, que la référence à la peine minimale d'un an visée à l'article 88*bis* est la seule définition utilisable. Le Collège ajoute ce qui suit: "Si ce seuil est fixé à trois ans ou limité aux faits mentionnés dans la "liste des écoutes" de l'article 90*ter* du Code d'instruction criminelle, on risque de se retrouver dans la situation non souhaitable dans laquelle un suspect de certains faits peut certes être placé en détention préventive à partir du seuil de la peine d'un an, mais dans laquelle aucun accès à des données de roulage ne serait prévu, si le seuil de trois ans n'est pas atteint ou si cela ne concerne aucun fait prévu à l'article 90*ter* lijst enkel bij heel specifieke overtredingen ingeschakeld worden. Het gaat daarbij bijvoorbeeld over onlinefraude of inbreuken op het vlak van de volksgezondheid. In die gevallen nemen de betrokken autoriteiten meer en meer taken van het parket over.

De minister wijst er wel op dat het voorliggende artikel beschouwd moet worden als een kaderbepaling, waarbij een dubbele voorwaarde wordt opgelegd aan de betrokken autoriteiten. Ten eerste moet er sprake zijn van de in de ontworpen paragraaf 2 vastgelegde doeleinden. Ten tweede moet er ook een organieke of sectorale wetgevingsgrond bestaan waarin die autoriteiten gemachtigd worden om de metagegevens van operatoren op te vragen. Die formele wettelijke norm moet krachtens de ontworpen paragraaf 5 de volgende zaken preciseren: de categorieën van ondernemingen waarvan de autoriteit gegevens kan opvragen, de categorieën van gegevens die opgevraagd mogen worden, de beoogde doeleinden en de mechanismen ter controle van het verzoek om gegevens. Vanwege de twee voormelde voorwaarden is de minister van oordeel dat de lijst met doeleinden niet te ruim is opgevat.

In het kader van bepaalde onlinemisdrijven is het mogelijk dat zelfs administratieve autoriteiten IP-adressen of metagegevens nodig hebben om de feiten te onderzoeken. Het HvJ-EU bevestigde in het arrest *La Quadrature du Net* dat het IP-adres soms het enige element is op basis waarvan bepaalde onlinemisdrijven vervolgd kunnen worden.

In het ontworpen artikel 127/1, § 4, eerste lid, wordt bovendien het aantal doeleinden verminderd om toegang te verkrijgen tot gegevens die op grond van het ontworpen artikel 126/1 bewaard worden. Het klopt dus niet dat het ontworpen artikel niet in overeenstemming zou zijn met de Europese regelgeving.

De minister van Justitie licht toe waarom zware criminaliteit in het voorliggende artikel wordt omschreven aan de hand van artikel 88*bis* van het Wetboek van strafvordering in plaats van artikel 90*ter* van datzelfde Wetboek. Het College van procureurs-generaal stelt in zijn advies aan de commissie over het onderhavige wetsontwerp dat de verwijzing naar de strafdrempel van één jaar zoals bedoeld in artikel 88*bis* de enige werkbare definitie is. Het College voegt daar het volgende aan toe: "Indien deze drempel op drie jaar gesteld zou worden of beperkt zou worden tot de feiten vermeld in de zogenaamde taplijst van artikel 90*ter* van het Wetboek van strafvordering, riskeert men de onwenselijke situatie dat een verdachte voor bepaalde feiten wel in voorlopige hechtenis geplaatst kan worden vanaf de strafdrempel van één jaar, maar dat niet in een toegang tot verkeersgegevens voorzien zou zijn, indien de drempel van drie jaar niet gehaald

du Code d'instruction criminelle."Cela signifierait qu'une personne pourrait être placée en détention préventive sur la base de métadonnées, mais que la personne concernée ne pourrait pas consulter ces données afin de prouver son innocence. Le gouvernement a donc choisi de définir la notion de "criminalité grave" sur la base de l'article 88*bis* du Code d'instruction criminelle, ce qui ne constitue d'ailleurs pas une nouvelle manière de faire.

En ce qui concerne les autorités qui pourraient demander à consulter les données conservées, il a été affirmé dans la presse que les services fiscaux auraient accès à ce type de données. Toutefois, le projet de loi à l'examen rend la chose difficile. En effet, le paragraphe 3 de l'article 127/1 en projet prévoit que les autorités visées au paragraphe 2 du même article, qui comprennent les autorités administratives telles que le fisc, peuvent uniquement obtenir les données d'identification visées aux articles 126 et 127 en projet "pour autant que prévu par et aux conditions fixées dans une norme législative formelle".

L'article 127/1, § 5, en projet, prévoit que la norme législative formelle doit préciser certaines choses, et notamment, en particulier, "les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante."

Ainsi, le fisc sera soumis pour la première fois à un contrôle préalable. En effet, l'exigence d'une norme législative formelle n'existe actuellement pas pour les services fiscaux. L'article 322 du Code des impôts sur les revenus 1992 confère certes au fisc un large pouvoir d'investigation, mais il ne constitue pas la norme législative formelle visée par le projet de loi à l'examen. Le ministre souligne que ce texte suit la jurisprudence européenne.

Le SPF Finances sera donc obligé d'élaborer un cadre légal spécifique pour permettre au fisc d'accéder aux métadonnées. Les données de trafic et de localisation nécessitent le consentement préalable d'une instance judiciaire, telle qu'un juge d'instruction, ou d'une autorité administrative indépendante, telle que l'APD. Pour les données d'identification, qui sont un peu moins intrusives, le consentement d'un supérieur hiérarchique ou du *data protection officer* (DPO) est suffisant. Dans les deux cas, la réglementation est conforme à la jurisprudence européenne.

Par conséquent, s'il existe des indices qu'une infraction pénale a été commise, le fisc a deux options,

zou worden of het geen feit als bedoeld in artikel 90*ter* van het Wetboek van strafvordering zou betreffen." Dit zou betekenen dat een persoon in voorlopige hechtenis kan worden geplaatst op basis van metagegevens, maar dat de betrokkene die gegevens niet zou kunnen inkijken om zijn onschuld te bewijzen. De regering heeft er dan ook voor gekozen om het begrip "zware criminaliteit" te definiëren aan de hand van artikel 88*bis* van het Wetboek van strafvordering, wat overigens geen nieuwe werkwijze is.

Met betrekking tot de autoriteiten die de bewaarde gegevens zouden kunnen opvragen, werd in de pers beweerd werd dat de belastingdienst toegang tot dergelijke gegevens zou krijgen. Het onderhavige wetsontwerp bemoeilijkt dat echter net. In paragraaf 3 van het ontworpen artikel 127/1 wordt immers bepaald dat de autoriteiten bedoeld in paragraaf 2 van datzelfde artikel, waaronder ook administratieve overheden zoals de fiscus vallen, de identificatiegegevens bedoeld in de ontworpen artikelen 126 en 127 enkel mogen ontvangen "voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm."

In het ontworpen artikel 127/1, § 5, wordt voorgeschreven dat de formele wettelijke norm bepaalde zaken moet preciseren, waaronder meer bepaald "de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit."

De fiscus zal dus voor de eerste keer onderworpen worden aan een voorafgaande controle. De vereiste inzake een formele wettelijke norm bestaat vandaag immers niet voor de belastingdienst. Artikel 322 van het Wetboek van de Inkomstenbelastingen 1992 biedt de fiscus wel een ruime onderzoeksbevoegdheid, maar vormt niet de formele wettelijke norm waarvan sprake is in het voorliggende wetsontwerp. De minister benadrukt dat in deze tekst de Europese rechtsspraak gevolgd wordt.

De FOD Financiën zal dus verplicht zijn om een specifiek wettelijk kader op te stellen om de fiscus toegang te geven tot de metagegevens. Voor de verkeers- en de locatiegegevens is er voorafgaandelijke toestemming nodig van een gerechtelijke instantie, zoals een onderzoeksrechter, of door een onafhankelijke administratieve autoriteit, zoals de GBA. Voor de identificatiegegevens, die iets minder indringend zijn, volstaat de toestemming van een hiërarchische meerdere of de *data protection officer* (DPO). In beide gevallen is de regeling in overeenstemming met de Europese rechtsspraak.

Als er aanwijzingen bestaan dat een strafrechtelijke inbreuk werd gepleegd, heeft de fiscus dan ook twee

conformément à la loi du 20 septembre 2012 instaurant le principe “una via” dans le cadre de la poursuite des infractions à la législation fiscale et majorant les amendes pénales fiscales. Tout d’abord, une enquête pénale peut être ouverte. Dans ce cas, en ce qui concerne l’accès aux métadonnées, les règles de l’article 88*bis* du Code d’instruction criminelle sont d’application, ce qui implique l’autorisation d’un juge d’instruction. Deuxièmement, le fisc peut ouvrir une enquête administrative. Dans ce cas, une norme législative formelle doit être émise ou un juge ou l’APD doit donner l’autorisation de demander les données de trafic et de localisation aux opérateurs.

Le ministre complète son argumentation en renvoyant à l’article 33 du projet de loi à l’examen, qui modifie l’article 84 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers. L’article 84, § 1er*bis*/1, en projet, prévoit que la FSMA peut avoir accès aux métadonnées lors d’une enquête sur un abus de marché si elle reçoit une autorisation préalable du juge d’instruction. L’abus de marché est l’une des infractions les plus graves dans le secteur financier. En témoigne notamment le fait que le Règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (Règlement relatif aux abus de marché) exige pour ces infractions des amendes maximales d’un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement.

Le ministre conclut que la CJUE a été sévère mais juste dans la protection de la confidentialité des métadonnées, non seulement à l’égard des services de renseignement et de sécurité, mais aussi à l’égard des services d’inspection fiscale et sociale. Le ministre, en collaboration avec la ministre des Télécommunications, a veillé à ce que la jurisprudence européenne soit correctement appliquée. Le projet de loi à l’examen ne prévoit donc en aucun cas un libre accès aux métadonnées, mais définit au contraire un cadre légal strict auquel les différentes autorités doivent se conformer si elles souhaitent avoir accès à ces données.

Enfin, le ministre fait remarquer que le projet de loi accorde l’accès à une liste spécifique d’autorités, dont, effectivement, les services d’inspection du SPF Santé publique, mais uniquement en ce qui concerne les données d’identification.

Mme Sophie De Wit (N-VA) fait observer que l’article 88*bis* du Code d’instruction criminelle utilise le seuil d’une peine d’un an. L’intervenante présume que dans le nouveau Code pénal que concocte le ministre de la Justice une peine d’emprisonnement d’un an

mogelijkheden, overeenkomstig de wet van 20 september 2012 tot instelling van het “una via”-principe in de vervolging van overtredingen van de fiscale wetgeving en tot verhoging van de fiscale penale boetes. Ten eerste kan een strafrechtelijk onderzoek worden geopend. In dat geval gelden, wat de toegang tot de metagegevens betreft, de regels van artikel 88*bis* van het Wetboek van strafvordering, wat de toestemming van een onderzoeksrechter inhoudt. Ten tweede kan er bij de fiscus een administratief onderzoek worden opgestart. In dat geval moet er een formele wettelijke norm worden uitgevaardigd of moet een rechter of de GBA goedkeuring geven om de verkeers- en locatiegegevens op te vragen bij de operatoren.

De minister vervolledigt zijn argumentatie met een verwijzing naar artikel 33 van het onderhavige wetsontwerp, dat artikel 84 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wijzigt. In het ontworpen artikel 84, § 1*bis*/1, wordt bepaald dat de FSMA toegang kan krijgen tot metadata bij onderzoeken naar marktmisbruik wanneer ze daartoe voorafgaand toestemming krijgt van de onderzoeksrechter. Marktmisbruik betreft een van de meest ernstige inbreuken in de financiële sector. Dat blijkt onder meer uit het feit dat in Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik) de minimale maximumboetes aanzienlijk hoger liggen voor deze inbreuken dan voor de inbreuken op de andere bepalingen van de verordening.

De minister concludeert dat het HvJ-EU streng doch rechtvaardig is geweest met als doel de privacy van de metadata te beschermen, niet alleen ten opzichte van inlichtingen- en veiligheidsdiensten, maar ook ten aanzien van fiscale en sociale inspectiediensten. De minister heeft er samen met de minister van Telecommunicatie op toegezien dat de Europese rechtsspraak correct werd toegepast. Het voorliggende wetsontwerp voorziet dan ook geenszins in een vrije toegang tot metagegevens, maar omschrijft net een strikt wettelijk kader waaraan de verschillende overheden moeten voldoen als ze over die gegevens willen beschikken.

Tot slot merkt de minister op dat in het wetsontwerp toegang wordt verleend aan een specifieke lijst van autoriteiten, waaronder inderdaad de inspectiediensten van de FOD Volksgezondheid, al is dat enkel met betrekking tot de identificatiegegevens.

Mevrouw Sophie De Wit (N-VA) wijst erop dat in artikel 88*bis* van het Wetboek van strafvordering een strafdrempel van één jaar wordt gehanteerd. De spreekster vermoedt dat in het toekomstige nieuwe Strafwetboek, waaraan de minister van Justitie werkt, er voor bijna

s'appliquera à presque toutes les infractions. Dans ce cas, la criminalité grave telle que définie à l'article 127/1, § 1er, 1°, en projet correspondrait à presque toutes les infractions du futur Code pénal. En ce qui la concerne, l'intervenante délimiterait plus précisément la notion de "criminalité grave".

Le ministre de la Justice a cité l'exemple d'une personne placée en détention préventive qui, si l'article 127/1, § 1er , 1°, en projet définissait la notion de "criminalité grave" sur la base de l'article 90*ter* du Code d'instruction criminelle, ne pourrait accéder aux métadonnées la concernant, car dans ce cas un seuil de trois ans serait applicable à cette consultation. Cet exemple ne concerne toutefois que le cadre spécifique des enquêtes pénales, alors que l'article 127/1, en projet va bien au-delà des enquêtes judiciaires.

Le projet de loi montre qu'une autorité judiciaire doit satisfaire à davantage de critères pour avoir accès aux métadonnées, comme les conditions relatives à une délimitation géographique des zones ou à l'ordre du juge d'instruction. Pour les autorités administratives, en revanche, les règles sont beaucoup plus vagues. Les normes légales formelles en vertu desquelles l'accès leur sera accordé doivent encore être élaborées. Il est possible que celles-ci soient fondées sur des critères plus souples et que seule l'autorisation d'une autorité administrative indépendante soit encore nécessaire, et non plus celle d'un juge d'instruction. Il est ainsi possible de contourner la jurisprudence stricte de la CJUE.

Si l'intervenante est bien sûr opposée à la fraude sociale et fiscale, elle estime néanmoins qu'il est important de mettre en balance la protection de la vie privée et la protection de la société.

M. Michael Freilich (N-VA) ajoute que le ministre de la Justice prétend rendre plus difficile l'accès du fisc aux métadonnées. Mais dans le même temps, l'article 127/1, § 2, 10°, en projet, permet l'accès aux données pour "les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques." Auront-elles besoin de l'autorisation du juge?

M. Nabil Boukili (PVDA-PTB) précise qu'il n'exprimait pas une opinion personnelle en affirmant que le projet de loi n'est pas conforme à la jurisprudence européenne. C'est une observation formulée à l'égard du projet de loi par l'APD.

Le ministre de la Justice détaille la différence entre les articles 90*ter* et 88*bis* du Code d'instruction criminelle.

alles een gevangenisstraf van één jaar zal gelden. In dat geval zou de zware criminaliteit zoals bepaald in het ontworpen artikel 127/1, § 1, 1°, overeenkomen met zowat alle inbreuken van het toekomstige Strafwetboek. De spreekster zou het begrip "zware criminaliteit" toch scherper afbakenen.

De minister van Justitie haalde het voorbeeld aan van een persoon in voorlopige hechtenis die, indien het ontworpen artikel 127/1, § 1, 1°, het begrip "zware criminaliteit" zou definiëren aan de hand van artikel 90*ter* van het Wetboek van strafvordering, de metagegevens die op hem betrekking hebben niet zou kunnen inzien omdat er voor die inzage dan een strafdrempel van drie jaar zou gelden. Dat voorbeeld betreft echter enkel het specifieke kader van het strafonderzoek, terwijl het ontworpen artikel 127/1 veel ruimer gaat dan gerechtelijke onderzoeken.

Uit het wetsontwerp blijkt dat een gerechtelijke autoriteit aan meer criteria moet voldoen om toegang te krijgen tot metagegevens, zoals de voorwaarden inzake een geografische afbakening van zones of het bevel van de onderzoeksrechter. Voor administratieve autoriteiten zijn de regels echter veel vager. De formele wettelijke normen op basis waarvan ze toegang zullen krijgen, moeten nog uitgewerkt worden. Het is mogelijk dat daarin soepelere criteria gehanteerd zullen worden en er bijvoorbeeld enkel nog toestemming nodig is van een onafhankelijke administratieve autoriteit, en niet meer van een onderzoeksrechter. Zo kan de strenge rechtsspraak van het HvJ-EU omzeild worden.

De spreekster is uiteraard gekant tegen sociale en fiscale fraude, maar vindt het belangrijk dat de afweging tussen privacy en de bescherming van de samenleving wordt gemaakt.

De heer Michael Freilich (N-VA) voegt daaraan toe dat de minister van Justitie beweert dat hij de toegang van de fiscus tot de metagegevens moeilijker maakt. Tegelijk wordt echter in het ontworpen artikel 127/1, § 2, 10°, de toegang tot de gegevens mogelijk gemaakt voor "de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden." Zullen zij de toestemming van de rechter nodig hebben?

De heer Nabil Boukili (PVDA-PTB) verduidelijkt dat hij niet op persoonlijke titel stelde dat het wetontwerp niet conform de Europese rechtsspraak is. Het is een opmerking van de GBA ten aanzien van het wetsontwerp.

De minister van Justitie gaat dieper in op het verschil tussen de artikelen 90*ter* en 88*bis* van het Wetboek

L'article 90*ter* n'est utilisé que pour définir le critère de conservation, tandis que l'article 88*bis* du même Code est utilisé pour déterminer l'accès aux données à des fins judiciaires. Mme De Wit a qualifié une peine d'un an de trop faible, mais relever le niveau de la peine rendrait le travail des services plus compliqué sur le terrain.

S'agissant de l'accès accordé au fisc, Mme De Wit a qualifié l'autorisation préalable de l'autorité administrative indépendante de détail. C'est pourtant l'APD qui interviendra en qualité d'autorité administrative indépendante lorsque l'approbation du juge d'instruction n'est pas nécessaire. Le ministre fait observer que M. Freilich, qui appartient au même parti que Mme De Wit, cite systématiquement l'APD en exemple.

Qui plus est, le fisc peut jusqu'à présent accéder librement aux métadonnées dans le cadre du Code des impôts sur les revenus 1992 comme dans le cadre du Code de la taxe sur la valeur ajoutée. Le projet de loi à l'examen met fin à cette situation. Il en va d'ailleurs de même pour les services de l'inspection sociale.

S'agissant des autorités scientifiques visées au paragraphe 2, 10°, en projet, le ministre fait observer que le traitement des données à des fins scientifiques est réglé par l'APD.

Un collaborateur de la ministre de la Défense communique des compléments d'information en la matière de la part du vice-premier ministre et ministre de l'Économie et du Travail, en charge de Statbel, auquel s'applique la disposition 10° précitée. Eurostat impose des critères de qualité à Statbel, qui, pour cette raison, doit pouvoir disposer de données avec identifiants directs. Pour fournir cet accès, il faut une norme juridique formelle. Lorsque le ministre de l'Économie souhaitera permettre cet accès, il viendra dès lors présenter en commission un projet de loi à cet effet.

Mme Sophie De Wit (N-VA) précise qu'elle considère qu'une peine d'un an ne pose pas de problème dans le cadre des enquêtes pénales déjà assorties de toutes sorte de garanties. En revanche, si l'accès est accordé dans un contexte plus large, elle juge le critère relatif à ce niveau de peine problématique.

Le ministre indique que, d'une part, il faut édicter une norme juridique pour permettre au fisc d'accéder aux données, mais que, d'autre part, ce dernier a déjà accès à ces données. Est-il effectivement exact que cette norme juridique existe déjà? Faut-il la rendre plus stricte? L'intervenante souligne toutefois que lorsque

van strafvordering Artikel 90*ter* wordt enkel gebruikt om het criterium van bewaring vast te leggen, terwijl artikel 88*bis* van datzelfde wetboek aangewend wordt voor de toegang tot gegevens in het kader van justitiële doeleinden. Mevrouw De Wit noemde de strafmaat van één jaar te laag, maar een verhoging van die strafmaat zou het voor de diensten moeilijker maken om hun werk in de praktijk uit te voeren.

Met betrekking tot de toegang voor de fiscus deed mevrouw De Wit de voorafgaande toestemming van de onafhankelijke administratieve autoriteit af als een kleinigheid. Het is evenwel de GBA die zal optreden als onafhankelijke administratieve autoriteit wanneer de goedkeuring van de onderzoeksrechter niet nodig is. De minister merkt op dat de heer Freilich, partijgenoot van mevrouw De Wit, die GBA steevast als een lichtend voorbeeld aanhaalt.

Bovendien kan de fiscus tot nog toe vrijelijk toegang krijgen tot metagegevens in het kader van zowel het Wetboek van de Inkomstenbelasting 1992 als het Wetboek van de belasting over de toegevoegde waarde. Dit wetsontwerp maakt daar een einde aan. Hetzelfde geldt overigens voor de sociale inspectiediensten.

Inzake de wetenschappelijke autoriteiten, bedoeld in de ontworpen paragraaf 2, 10°, merkt de minister op dat gegevensverwerking voor wetenschappelijke doeleinden geregeld wordt door de AVG.

Een medewerker van de minister van Defensie geeft ter zake nadere toelichting vanwege de vice-eersteminister en minister van Economie en Werk, bevoegd voor Statbel, waarop de voornoemde bepaling onder 10° van toepassing is. Eurostat legt kwaliteitseisen op aan Statbel, dat om die reden over gegevens met directe *identifiers* moet kunnen beschikken. Er is een formele wettelijke norm nodig om die toegang te verschaffen. Wanneer de minister van Economie die toegang mogelijk wil maken, zal hij daartoe dan ook een wetsontwerp in de commissie komen voorstellen.

Mevrouw Sophie De Wit (N-VA) verduidelijkt dat ze de strafmaat van één jaar geen probleem vindt bij strafonderzoeken, waarvoor een hele reeks waarborgen gelden. Als de toegang in een ruimere context wordt verstrekt, vindt ze het criterium inzake die strafmaat wel problematisch.

De minister stelt dat er enerzijds een wettelijke norm moet uitgevaardigd worden om de fiscus toegang te geven tot de gegevens, maar dat de fiscus anderzijds al toegang heeft tot die gegevens. Is het dan toch zo dat die wettelijke norm al bestaat? Moet die dan verstrengd worden? De spreekster wijst er wel op dat wanneer de

l'administration fiscale demande l'approbation d'une autorité administrative indépendante, les autres critères deviennent encore et toujours sans objet.

Art. 12 et 13

Ces articles ne donnent lieu à aucune observation.

Art. 14

Cet article apporte plusieurs modifications à l'article 145 de la loi du 13 juin 2005. Ainsi, la liste des articles dont le non-respect est puni pénalement est adaptée aux articles visés par l'actuel projet de loi, qui ont pour objectif la fourniture de données de communications électroniques aux autorités. Parallèlement, le montant de l'amende a été revu à la hausse, étant donné que le montant actuel n'est plus de nature dissuasive au vu de la capacité financière de certains opérateurs. Enfin, le paragraphe 3*ter*, annulé par la Cour constitutionnelle dans son arrêt n° 57/2021, a été réintroduit.

Le gouvernement présente l'*amendement n° 4* (DOC 55 2572/002), qui tend à remplacer, dans l'article 145, § 1er , de la loi du 13 juin 2005, les mots "126, 126/1" par les mots "126 à 126/2".

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

belastingdienst de goedkeuring vraagt van een onafhankelijke administratieve overheid, de andere criteria nog steeds vervallen.

Art. 12 en 13

Over deze artikelen worden geen opmerkingen gemaakt.

Art. 14

Dit artikel brengt verschillende wijzigingen aan in artikel 145 van de wet van 13 juni 2005. Zo wordt de lijst van de artikelen waarvan de niet-inachtneming strafrechtelijk wordt bestraft, aangepast aan de door het huidig wetsontwerp beoogde artikelen omtrent de verstrekking van elektronische communicatiegegevens aan de autoriteiten. Daarnaast wordt het bedrag van de geldboete opwaarts herzien, aangezien het huidige bedrag niet meer ontradend werkt, gelet op het financiele vermogen van sommige operatoren. Tot slot wordt paragraaf 3*ter*, vernietigd door het Grondwettelijk Hof in zijn arrest nr. 57/2021, opnieuw ingevoegd.

De regering dient *amendement nr. 4* (DOC 55 2572/002) in, dat ertoe strekt, in artikel 145, § 1, van de wet van 13 juni 2005, de woorden "126, 126/1" te vervangen door de woorden "126 tot 126/2".

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

CHAPITRE 3

Modification de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques

Art. 15

Cet article ne donne lieu à aucune observation.

CHAPITRE 4

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

Art. 16

Cet article vise à compléter l'article 2, alinéa 1er, de la loi du 17 janvier 2003 relative au statut de l'IBPT par un 5° en vue d'insérer une définition de la notion de "données relatives à l'utilisateur final ou à l'abonné".

Le gouvernement présente l'*amendement n° 8* (DOC 55 2572/002) tendant à remplacer le 5° de l'article 2, alinéa 1er, en projet, par ce qui suit, et à compléter cet alinéa par un 6° rédigé comme suit:

"5° demande de données d'identification: demande de l'Institut ou de ses officiers de police judiciaire adressée à un opérateur ou à une autre personne morale de communiquer des données autres que celles conservées en vertu de l'article 126/1 de la loi du 13 juin 2005 relative aux communications électroniques, et visant à identifier:

— l'abonné ou l'utilisateur habituel du service de communications électroniques, son équipement terminal ou le dispositif matériel ou logiciel intégré dans cet équipement terminal ou installé auprès de l'abonné en vue de la fourniture du service de communications électroniques, ou;

— les services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée;

6° demande de métadonnées: demande de l'Institut ou de ses officiers de police judiciaire adressée à un opérateur de communiquer des métadonnées de communications électroniques autres que celles conservées en vertu de l'article 126/1 de la loi du 13 juin 2005 relative

HOOFDSTUK 3

Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

Art. 15

Over dit artikel worden geen opmerkingen gemaakt.

HOOFDSTUK 4

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

Art. 16

Dit artikel beoogt artikel 2, eerste lid, van de wet van 17 januari 2003 betreffende het BIPT-statuut aan te vullen met een bepaling onder 5°, waarbij een definitie van het begrip "gegevens betreffende de eindgebruiker of de abonnee" wordt ingevoegd.

De regering dient *amendement nr. 8* (DOC 55 2572/002) in, dat ertoe strekt de ontworpen bepaling onder 5° van genoemd artikel 2, eerste lid, te vervangen als volgt, en dit lid aan te vullen met een bepaling onder 6°, luidende:

"5° verzoek om identificatiegegevens: verzoek van het Instituut of van zijn officieren van gerechtelijke politie gericht aan een operator of een andere rechtspersoon om andere gegevens te verstrekken dan deze bewaard krachtens artikel 126/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie en met het oog op de identificatie van:

— de abonnee of de gewoonlijke gebruiker van de elektronische-communicatiedienst, zijn eindapparatuur of de hardware of software die is ingebouwd in deze eindapparatuur of is geïnstalleerd bij de abonnee met het oog op de verstrekking van de elektronische-communicatiedienst, of;

— de elektronische-communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden;

6° verzoek om metagegevens: verzoek van het Instituut of van zijn officieren van gerechtelijke politie gericht aan een operator om andere elektronische-communicatiemetagegevens te verstrekken dan deze bewaard krachtens artikel 126/1 van de wet van 13 juni 2005 betreffende de

aux communications électroniques, autre qu'une demande de données d'identification et visant notamment à:

a) déterminer les métadonnées liées à une communication électronique;

b) localiser l'équipement terminal;

c) déterminer si l'équipement terminal est allumé ou éteint.".

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement à l'examen.

Art. 17

Cet article modifie l'article 14 de la loi relative au statut de l'IBPT afin de permettre au régulateur de contrôler le respect de certaines dispositions visées par le projet de loi à l'examen, d'une part, et pour régler un cas spécifique de demande de renseignements, d'autre part.

Le gouvernement présente l'*amendement n° 9* (DOC 55 2572/002) tendant à remplacer cet article par ce qui suit:

"Art. 17. À l'article 14 de la même loi, modifié en dernier lieu par la loi du 17 février 2022, le chiffre "15" est inséré entre les mots "les articles 14, § 2, 2°," et les mots "et 21, §§ 5 à 7".".

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement à l'examen.

Art. 18

Cet article vise à compléter l'article 25 de la loi relative au statut de l'IBPT par quatre paragraphes concernant les demandes des officiers de police judiciaire de l'IBPT de communication, par les opérateurs, de certaines données nécessaires à la répression de certaines infractions à la loi du 13 juin 2005, au Code pénal et aux lois spéciales.

Le gouvernement présente l'*amendement n° 10* (DOC 55 2572/002) tendant à remplacer cet article par ce qui suit:

elektronische communicatie en dat geen verzoek om identificatiegegevens is, teneinde met name:

a) de metagegevens in verband met een elektronische communicatie te bepalen;

b) de eindapparatuur te lokaliseren;

c) te bepalen of de eindapparatuur is ingeschakeld of uitgeschakeld.".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 17

Dit artikel wijzigt artikel 14 van de wet betreffende het BIPT-statuut, enerzijds om ervoor te zorgen dat de regulator kan toezien op de naleving van enkele door dit wetsontwerp beoogde bepalingen en anderzijds om een specifiek geval van verzoek om inlichtingen te regelen.

De regering dient *amendement nr. 9* (DOC 55 2572/002) in, dat ertoe strekt het artikel te vervangen als volgt:

"Art. 17. In artikel 14 van dezelfde wet, laatstelijk gewijzigd bij de wet van 17 februari 2022, wordt het cijfer "15" ingevoegd tussen de woorden "de artikelen 14, § 2, 2°," en de woorden "en 21, §§ 5 tot 7".".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 18

Dit artikel beoogt artikel 25 van de wet betreffende het BIPT-statuut aan te vullen met vier paragrafen aangaande verzoeken vanwege officieren van gerechtelijke politie van het BIPT tot verstrekking, door de operatoren, van bepaalde gegevens die nodig zijn om bepaalde inbreuken op de wet van 13 juni 2005, het Strafwetboek en de bijzondere wetten, te beteugelen.

De regering dient *amendement nr. 10* (DOC 55 2572/002) in, dat ertoe strekt het artikel te vervangen als volgt:

"Art. 18. Dans la même loi, l'article 15, abrogé par la loi du 16 mars 2015, est rétabli dans la rédaction suivante:

"Art. 15. § 1er. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), ce dernier peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de données d'identification. L'Institut fixe le délai de communication des données demandées.

§ 2. Lorsque c'est nécessaire pour permettre à l'Institut d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), ce dernier peut exiger, par demande écrite et motivée, d'un opérateur de répondre à une demande de métadonnées. L'Institut fixe le délai de communication des données demandées.

Sauf en cas d'urgence dûment justifié et sauf lorsque des métadonnées anonymes sont demandées à l'opérateur, l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée à l'Autorité de protection des données et après avoir obtenu l'autorisation écrite de cette dernière.

En cas d'urgence dûment justifiée, l'Institut communique à l'Autorité de protection des données, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande ainsi que la justification de l'urgence. L'Autorité de protection des données effectue ultérieurement un contrôle.

Pour l'application du présent paragraphe, l'Institut demande à l'opérateur des métadonnées anonymisées ou pseudonymisées, sauf lorsqu'elles ne lui permettent pas de rencontrer l'objectif poursuivi.

§ 3. Par dérogation aux paragraphes 1 et 2 et afin de contrôler le respect par un opérateur de l'article 122, de l'article 123, de l'article 126, de l'article 126/1, de l'article 126/2 ou de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques ou d'un arrêté d'exécution d'un de ces articles, l'Institut peut exiger d'un opérateur, par demande écrite et motivée, de lui fournir l'accès lui permettant de consulter une base de données qui met en œuvre un de ces articles ou un de ces arrêtés d'exécution.

L'alinéa 1er n'est applicable pour ce qui concerne les articles 126, 126/1, 126/2 et 127 et leurs arrêtés d'exécution que pour autant que l'Institut soit chargé

"Art. 18. In dezelfde wet wordt artikel 15, opgeheven bij de wet van 16 maart 2015, hersteld als volgt:

"Art. 15. § 1. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, § 1, 3°, a) en g) tot i) uit te voeren, mag het Instituut van een operator, schriftelijk en met redenen omkleed, eisen dat hij antwoordt op een verzoek om identificatiegegevens. Het Instituut bepaalt de termijn waarbinnen de gegevens moeten worden meegedeeld.

§ 2. Wanneer het noodzakelijk is om het Instituut in staat te stellen een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, § 1, 3°, a) en g) tot i) uit te voeren, mag het Instituut van een operator, schriftelijk en met redenen omkleed, eisen dat hij antwoordt op een verzoek om metagegevens. Het Instituut bepaalt de termijn waarbinnen de gegevens moeten worden meegedeeld.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid en tenzij anonieme metagegevens worden gevraagd aan de operator, mag het Instituut het verzoek aan de operator pas richten na het voorleggen van een met redenen omkleed en schriftelijk verzoek aan de Gegevensbeschermingsautoriteit en na het ontvangen van de schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid deelt het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dat verzoek, de motivering van het verzoek, alsook de rechtvaardiging van de hoogdringendheid mee aan de Gegevensbeschermingsautoriteit. De Gegevensbes chermingsautoriteit voert daarna een controle uit.

Voor de toepassing van deze paragraaf vraagt het Instituut aan de operator geanonimiseerde of gepseudonimiseerde metagegevens tenzij op basis daarvan niet aan het beoogde doel kan worden beantwoord.

§ 3. In afwijking van de paragrafen 1 en 2 en om de naleving door een operator van de artikelen 122, 123, 126, 126/1, 126/2 of 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie of van een besluit ter uitvoering van een van deze artikelen te controleren, kan het Instituut met een schriftelijk en met redenen omkleed verzoek van een operator eisen om aan het Instituut toegang te verlenen zodat het een databank kan raadplegen die een van deze artikelen of een van deze uitvoeringsbesluiten ten uitvoer legt.

Het eerste lid is wat betreft de artikelen 126, 126/1, 126/2 en 127 en de uitvoeringsbesluiten ervan slechts van toepassing voor zover het Instituut na het in

de sanctionner l'opérateur après la concertation avec le procureur du Roi visée à l'article 21/1.

La demande adressée à l'opérateur précise les noms des membres du personnel de l'Institut qui peuvent consulter cette base de données.

Ces membres du personnel ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des manquements commis par l'opérateur.

§ 4. Pour l'application des paragraphes 1 à 3, la motivation de la demande adressée à l'opérateur ou à l'Autorité de protection des données doit être développée au regard des circonstances.

Pour l'application des paragraphes 1er et 2, l'Institut doit motiver:

1° le lien entre les données demandées et la mission attribuée à l'Institut;

2° le caractère strictement nécessaire des données demandées dans le cadre de cette mission.

Pour l'application du paragraphe 2, l'Institut indique dans la demande adressée à l'Autorité de protection des données:

1° le motif pour lequel la communication par l'opérateur de métadonnées anonymisées ne permet pas de rencontrer l'objectif poursuivi;

2° le motif pour lequel la communication par l'opérateur de métadonnées pseudonymisées ne permet pas de rencontrer l'objectif poursuivi, sauf lorsque la demande précise que l'opérateur doit fournir de telles données.

Sont consignées dans un registre tenu auprès de l'Institut:

1° les demandes adressées aux opérateurs et à l'Autorité de protection des données;

2° la motivation de la demande et la justification de l'urgence communiquées à l'Autorité de protection des données conformément au paragraphe 2, alinéa 3;

artikel 21/1 bedoelde overleg met de procureur des Konings, ermee belast wordt de operator te sanctioneren.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de personeelsleden van het Instituut die deze databank mogen raadplegen.

Deze personeelsleden mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

§ 4. Voor de toepassing van de paragrafen 1 tot 3, moet de motivering van het verzoek gericht aan de operator of aan de Gegevensbeschermingsautoriteit uitgewerkt zijn in het licht van de omstandigheden.

Voor de toepassing van de paragrafen 1 en 2, moet het Instituut:

1° het verband motiveren tussen de gevraagde gegevens en de aan het Instituut toegewezen opdracht;

2° motiveren dat het niet meer gegevens vraagt dan die welke strikt nodig zijn in het kader van die opdracht.

Voor de toepassing van paragraaf 2 geeft het Instituut in het verzoek gericht aan de Gegevensbeschermingsautoriteit het volgende aan:

1° de reden waarom de verstrekking door de operator van geanonimiseerde metagegevens niet volstaat om het nagestreefde doel te bereiken;

2° de reden waarom de verstrekking door de operator van gepseudonimiseerde gegevens niet volstaat om het nagestreefde doel te bereiken, behalve wanneer het verzoek preciseert dat de operator dergelijke gegevens moet verstrekken.

Moeten worden opgenomen in een inventaris die bij het Instituut wordt bijgehouden:

1° de verzoeken gericht aan de operatoren en aan de Gegevensbeschermingsautoriteit;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de Gegevensbeschermingsautoriteit overeenkomstig paragraaf 2, derde lid;

3° les autorisations données par l'Autorité de protection des données.".”

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement à l'examen.

Art. 19

Cet article vise à insérer, dans la loi relative au statut de l'IBPT, un article 28/1 concernant les demandes des membres du personnel de l'IBPT de communication, par les opérateurs, de certaines données nécessaires pour permettre à l'Institut d'accomplir ses missions de contrôle (hors cadre pénal).

Le gouvernement présente l'*amendement n° 11* (DOC 55 2572/002) tendant à remplacer cet article par ce qui suit:

"Art. 19. L'article 24 de la même loi, dont le texte actuel devient le paragraphe 1er, est complété par le paragraphe 2 suivant:

"§ 2. Le Roi désigne, parmi les officiers de police judiciaire de l'Institut visés au § 1er, ceux qui sont chargés du contrôle des demandes visées à l'article 25/1, §§ 1 et 3.

Sans préjudice de l'article 25, paragraphe 5, les officiers de police judiciaire de l'Institut désignés par le Roi en vertu de l'alinéa 1er, exécutent leur mission en toute indépendance. Ils ne peuvent être soumis à aucun lien de subordination à l'égard des autres officiers de police judiciaire de l'Institut.".”

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement à l'examen.

Art. 19/1 (*nouveau*)

Le gouvernement présente l'*amendement n° 12* (DOC 55 2572/002) tendant à insérer un article 19/1 rédigé comme suit:

"Art. 19/1. Dans l'article 25 de la même loi, les modifications suivantes sont apportées:

3° de toestemmingen verleend door de Gegevensbeschermingsautoriteit.".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 19

Dit artikel beoogt een artikel 28/1 in te voegen in de wet op het BIPT-statuut, betreffende de verzoeken vanwege personeelsleden van het BIPT tot verstrekking, door de operatoren, van bepaalde gegevens die nodig zijn om het Instituut in staat te stellen zijn toezichtsopdrachten te vervullen (buiten een strafrechtelijk kader).

De regering dient *amendement nr. 11* (DOC 55 2572/002) in, dat ertoe strekt het artikel te vervangen als volgt:

"Art. 19. Artikel 24 van dezelfde wet, waarvan de huidige tekst paragraaf 1 wordt, wordt aangevuld met de volgende paragraaf 2:

"§ 2. De Koning wijst onder de in § 1 bedoelde officieren van gerechtelijke politie van het Instituut diegenen aan die belast worden met de controle van de in artikel 25/1, §§ 1 en 3 beoogde verzoeken.

Onverminderd artikel 25, paragraaf 5, voeren de officieren van gerechtelijke politie van het Instituut die krachtens het eerste lid door de Koning aangesteld zijn, hun opdracht volledig onafhankelijk uit. Zij mogen niet worden onderworpen aan een ondergeschikt verband ten opzichte van de andere officieren van gerechtelijke politie van het Instituut.".”

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 19/1 (*nieuw*)

De regering dient *amendement nr. 12* (DOC 55 2572/002) in, dat ertoe strekt een artikel 19/1 in te voegen, luidende:

Art. 19/1. In artikel 25 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° au paragraphe 1er, alinéa 1er, les mots “membres du personnel visés à l’article 24“ sont remplacés par les mots ”officiers de police judiciaire de l’Institut”;

2° au paragraphe 1er, alinéa 1er, les mots “, dans l’exercice de leur mission de police judiciaire” sont supprimés;

3° au paragraphe 3, les mots “membres du personnel visés à l’article 24“ sont remplacés par les mots ”officiers de police judiciaire de l’Institut”;

4° au paragraphe 3, les mots “,en leur qualité d’officier de police judiciaire,” sont supprimés;

5° aux paragraphes 4, 5, 6 et 7 les mots “de l’Institut“ sont insérés après les mots ”officiers de police judiciaire”.”.

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l’amendement à l’examen.

Art. 19/2 (*nouveau*)

Le gouvernement présente l’*amendement n° 13* (DOC 55 2572/002) tendant à insérer un article 19/2, qui vise à son tour à insérer, dans le chapitre III, section 4, sous-section 1e, de la loi du 17 janvier 2003 relative au statut de l’IBPT, un article 25/1 rédigé comme suit:

“Art. 25/1. § 1er. Afin de rechercher, de constater ou de poursuivre une infraction visée à l’article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l’article 24, § 1er, 2°, un officier de police judiciaire de l’Institut peut, par écrit:

1° exiger d’un opérateur de répondre à une demande de données d’identification qui est nécessaire à ces fins;

2° requérir la collaboration des personnes et institutions visées à l’article 46*quater*, § 1er, du Code d’instruction criminelle et d’associations les représentant, sur la base de la référence de paiement en ligne spécifique à un service de communications électroniques qui a préalablement été communiquée par un opérateur conformément au 1°, afin d’identifier la personne qui a payé le service;

1° in paragraaf 1, eerste lid, worden de woorden “personeelsleden vermeld in artikel 24” vervangen door de woorden “officieren van gerechtelijke politie van het Instituut”;

2° in paragraaf 1, eerste lid, worden de woorden “in hun hoedanigheid van officier van gerechtelijke politie” geschrapt;

3° in paragraaf 3, worden de woorden “personeelsleden vermeld in artikel 24” vervangen door de woorden “officieren van gerechtelijke politie van het Instituut”;

4° in paragraaf 3, worden de woorden “in hun hoedanigheid van officier van gerechtelijke politie” geschrapt;

5° in de paragrafen 4, 5, 6 en 7 worden de woorden “van het Instituut” telkens ingevoegd na de woorden “officieren van gerechtelijke politie”.”.

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 19/2 (*nieuw*)

De regering dient *amendement nr. 13* (DOC 55 2572/002) in, dat ertoe strekt een artikel 19/2 in te voegen, dat op zijn beurt beoogt in hoofdstuk III, afdeling 4, onderafdeling 1, van de wet van 17 januari 2003 inzake het BIPT-statuut, een artikel 25/1 in te voegen, luidende:

“Art. 25/1. § 1. Om een inbreuk bedoeld in artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen, kan een officier van gerechtelijke politie van het Instituut, schriftelijk:

1° van een operator eisen om te antwoorden op een verzoek om identificatiegegevens, dat voor deze doeleinden noodzakelijk is;

2° de medewerking vorderen van de personen en instellingen bedoeld in artikel 46*quater*, § 1, van het Wetboek van strafvordering en van verenigingen die hen vertegenwoordigen, op basis van het kenmerk van de onlinebetaling specifiek voor een elektronische-communicatiedienst die voorafgaandelijk meegedeeld is door een operator overeenkomstig de bepaling onder 1°, om de persoon te identificeren die de dienst heeft betaald;

3° requérir la collaboration des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, où la souscription de l'abonné à un service de communications électroniques a été effectué, sur la base des coordonnées du centre ou du lieu d'hébergement qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné;

4° requérir la collaboration de toute autre personne morale qui est l'abonnée d'un opérateur ou qui souscrit à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné ou l'utilisateur habituel du service.

Une demande visée à l'alinéa 1er ne peut être transmise à un acteur visé à l'alinéa 1er qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée adressée à cet officier conformément au § 5.

§ 2. Pour les besoins de l'accomplissement de ses missions, un officier de police judiciaire de l'Institut peut exiger d'un opérateur, par écrit, de répondre à une demande de métadonnées, qui est nécessaire afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3, ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°.

Sauf en cas d'urgence dûment justifié, l'officier de police judiciaire ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée au juge d'instruction et après autorisation écrite de ce dernier.

En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande et la justification de l'urgence. Un contrôle ultérieur est effectué par le juge d'instruction.

§ 3. Par dérogation aux paragraphes 1 et 2, afin de contrôler le respect des articles 126, 126/1, 126/2 ou 127 de la loi du 13 juin 2005 relative aux

3° de medewerking vorderen van de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, waar de inschrijving van de abonnee op een elektronische-communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee te identificeren;

4° de medewerking vorderen van alle andere rechtspersonen die abonnee zijn van een operator, of die intekenen in naam en voor rekening van natuurlijke personen op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee of de gewoonlijke gebruiker van de dienst te identificeren.

Een in het eerste lid bedoeld verzoek mag aan een in het eerste lid bedoelde actor pas worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek gericht aan deze officier overeenkomstig paragraaf 5.

§ 2. Ten behoeve van de vervulling van zijn opdrachten kan een officier van gerechtelijke politie van het Instituut van een operator schriftelijk eisen om te antwoorden op een verzoek om metagegevens, die nodig zijn om een inbreuk bedoeld in artikel 145, § 3, of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid, mag de officier van gerechtelijke politie het verzoek aan de operator pas richten na het voorleggen van een schriftelijk en met redenen omkleed verzoek aan de onderzoeksrechter en na schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dit verzoek, de motivering van het verzoek alsook de rechtvaardiging van de hoogdringendheid mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.

§ 3. In afwijking van de paragrafen 1 en 2, teneinde de naleving te controleren van de artikelen 126, 126/1, 126/2 of 127 van de wet van 13 juni 2005 betreffende de

communications électroniques et de leurs arrêtés d'exécution et à la demande écrite et motivée d'un officier de police judiciaire de l'Institut, un opérateur fournit, dans le délai fixé dans le réquisitoire, un accès permettant de consulter ses bases de données qui mettent en œuvre un de ces articles ou un de ces arrêtés d'exécution.

Une demande visée à l'alinéa 1er ne peut être transmise à un opérateur qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, paragraphe 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée conformément au § 5.

La demande adressée à l'opérateur précise les noms des officiers de police judiciaire de l'Institut qui peuvent consulter la base de données.

Ces officiers ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

§ 4. Pour l'application des paragraphes 1er et 2, les acteurs visés au paragraphe 1er, alinéa 1er, 1° à 4°, auxquels un officier de police judiciaire de l'Institut a demandé des données lui communiquent ces données en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire.

Pour l'application des paragraphes 1 à 3, toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

Toute personne qui refuse de permettre la consultation de la base de données conformément au paragraphe 3 ou qui ne permet pas cette consultation dans le délai fixé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

§ 5. Pour l'application des paragraphes 1 à 3, la motivation de la demande adressée à l'officier de police judiciaire visé à l'article 24, § 2, ou au juge d'instruction doit être développée au regard des circonstances de l'enquête.

elektronische communicatie en van de uitvoeringsbesluiten ervan en op schriftelijk en met redenen omkleed verzoek van een officier van gerechtelijke politie van het Instituut, verleent een operator binnen de termijn die vastgesteld is in de vordering toegang zodat zijn databanken die een van deze artikelen of een van deze uitvoeringsbesluiten uitvoeren, geraadpleegd kunnen worden.

Een in het eerste lid bedoeld verzoek mag pas naar een operator worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek overeenkomstig paragraaf 5.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de officieren van gerechtelijke politie van het Instituut die de databank kunnen raadplegen.

Deze officieren mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

§ 4. Voor de toepassing van de paragrafen 1 en 2, delen de actoren bedoeld in paragraaf 1, eerste lid, 1° tot 4°, aan wie een officier van gerechtelijke politie van het Instituut gegevens gevraagd heeft, de gevraagde gegevens mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

Voor de toepassing van de paragrafen 1 tot 3, is iedere persoon die uit hoofde van zijn functie kennis krijgt van de maatregel of daaraan zijn medewerking verleent, tot geheimhouding verplicht. Iedere schending van de geheimhoudingsplicht wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

Iedere persoon die weigert de raadpleging van de databank mogelijk te maken overeenkomstig paragraaf 3 of die deze raadpleging niet mogelijk maakt binnen de termijn bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

§ 5. Voor de toepassing van de paragrafen 1 tot 3 moet de motivering van het verzoek gericht aan de officier van gerechtelijke politie bedoeld in artikel 24, § 2, of aan de onderzoeksrechter uitgewerkt zijn in het licht van de omstandigheden van het onderzoek.

Pour l'application des paragraphes 1 et 2, cette motivation doit indiquer:

1° le lien entre les données demandées et l'objectif de recherche, de constat ou de poursuite de l'infraction spécifique qui justifie la demande;

2° le caractère strictement nécessaire des données demandées dans le cadre de l'enquête.

§ 6. Les officiers de police judiciaire de l'Institut consignent dans un registre:

1° l'ensemble des demandes visées aux paragraphes 1, 2 et 3;

2° la motivation de la demande et la justification de l'urgence communiquées au juge d'instruction conformément au paragraphe 2, alinéa 3;

3° les autorisations prévues aux paragraphes 1, 2 et 3.".

*
* *

Il est renvoyé à la discussion générale et à la justification de l'amendement.

CHAPITRE 5

Modifications du Code d'instruction criminelle

Art. 20

Cet article ne donne lieu à aucune observation.

Art. 20/1 (*nouveau*)

Le gouvernement présente l'*amendement n° 14* tendant à insérer un article 20/1, qui vise à son tour à apporter les modifications suivantes dans l'article 46*bis* du Code d'instruction criminelle, modifié en dernier lieu par la loi du 25 décembre 2016:

1° dans le paragraphe 1er un alinéa rédigé comme suit est inséré entre les alinéas 2 et 3:

"Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, il peut également requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:

Voor de toepassing van de paragrafen 1 en 2 moet deze motivering vermelden:

1° het verband tussen de gevraagde gegevens en het doel van de opsporing, vaststelling of de vervolging van de specifieke inbreuk dat het verzoek rechtvaardigt;

2° de strikt noodzakelijke aard van de gegevens die worden gevraagd in het kader van het onderzoek.

§ 6. De officieren van gerechtelijke politie van het Instituut nemen op in een inventaris:

1° alle verzoeken waarvan sprake in de paragrafen 1, 2 en 3;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de onderzoeksrechter overeenkomstig paragraaf 2, derde lid;

3° de in de paragrafen 1, 2 en 3 bedoelde toestemmingen.".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

HOOFDSTUK 5

Wijzigingen van het Wetboek van strafvordering

Art. 20

Over dit artikel worden geen opmerkingen gemaakt.

Art. 20/1 (*nieuw*)

De regering dient *amendement nr. 14* (DOC 55 2572/002) in, dat ertoe strekt een artikel 20/1 in te voegen, dat op zijn beurt beoogt de volgende wijzigingen aan te brengen in artikel 46*bis* Sv., laatstelijk gewijzigd bij de wet van 25 december 2016:

1° in paragraaf 1 wordt tussen het tweede en het derde lid een lid ingevoegd, luidende:

"Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid, tweede streepje, kan hij ook, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

— des personnes et institutions visées à l'article 46*quater*, § 1er, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, en application du paragraphe 1er;

— des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectué, et qui ont préalablement été communiquées par un des acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, en application du paragraphe 1er;

— des autres personnes morales qui sont l'abonné d'un des acteurs visés au paragraphe 2, premier ou deuxième tiret, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés au § 1er, alinéa 2, 1er et 2e tirets, en application du paragraphe 1er.";

2° dans le paragraphe 2, les alinéas 3 et 4 sont abrogés;

3° l'article est complété par les paragraphes 3 et 4, rédigés comme suit:

"§ 3. Les acteurs visés au § 1er, alinéa 3, 1er à 3e tirets, requis de communiquer l'identification de l'abonné ou de l'utilisateur habituel d'un service visé au paragraphe 1er, l'alinéa 2, deuxième tiret, communiquent au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition.

§ 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le

— de personen of instellingen bedoeld in artikel 46*quater*, § 1, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, in toepassing van het eerste lid;

— de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden, die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, in toepassing van het eerste lid;

— andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, eerste of tweede streepje, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, in toepassing van het eerste lid.";

2° in paragraaf 2 worden het derde en het vierde lid opgeheven;

3° het artikel wordt aangevuld met de paragrafen 3 en 4, luidende:

"§ 3. De actoren bedoeld in paragraaf 1, derde lid, eerste tot derde streepje, van wie de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in § 1, tweede lid, tweede streepje gevorderd wordt, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval,

cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros."."

*
* *

Il est renvoyé à la discussion générale et à la justification de l'amendement.

Art. 21

Cet article ne donne lieu à aucune observation.

CHAPITRE 6

Modification de la loi du 5 août 1992 sur la fonction de police

Art. 22

Cet article ne donne lieu à aucune observation.

CHAPITRE 7

Modification de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 23

Cet article vise à adapter la définition de la notion de "communications" inscrite dans l'article 3, 10°, de la loi du 30 novembre 1998 à la nouvelle réalité technologique.

M. Michael Freilich (N-VA) indique que cet article vise à préciser que les communications "*Machine-to-Machine*" relèvent également de la notion de communications telle que visée dans la loi du 30 novembre 1998.

On peut lire dans le commentaire de cet article (DOC 2572/001) que "ce ne sont pas uniquement les acteurs traditionnels de communications électroniques qui sont visés mais aussi les fournisseurs de services de communications interpersonnelles, de services permettant la communication comme élément accessoire à l'activité principale (exemple, le chat pendant les jeux), ou les fournisseurs d'un réseau privé (par exemple, un réseau interne d'entreprise)." Cette dernière précision fait suite à une observation de l'APD relative à l'avant-projet de loi (avis n° 108/2021), dans le cadre de laquelle l'autorité se demandait si la notion de "réseaux privés" a vocation à viser uniquement les réseaux des entreprises

op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro."."

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 21

Over dit artikel worden geen opmerkingen gemaakt.

HOOFDSTUK 6

Wijziging van de wet van 5 augustus 1992 op het politieambt

Art. 22

Over dit artikel worden geen opmerkingen gemaakt.

HOOFDSTUK 7

Wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Art. 23

Dit artikel beoogt de definitie van "communicatie" in artikel 3, 10°, van de wet van 30 november 1998 aan te passen aan de nieuwe technologische realiteit.

De heer Michael Freilich (N-VA) stelt dat de bedoeling van dit artikel is om te verduidelijken dat ook *machine-to-machine* communicatie begrepen wordt onder het begrip "communicatie" in de zin van de wet van 30 november 1998.

In de toelichting bij dit artikel (DOC 55 2572/001) staat te lezen dat "[n]iet alleen de traditionele actoren op het gebied van elektronische communicatie worden [] beoogd, maar ook de aanbieders van interpersoonlijke communicatiediensten, van diensten die communicatie mogelijk maken als een bijkomstig element bij de hoofdactiviteit (bijvoorbeeld chatten tijdens het gamen), of aanbieders van een privaat netwerk (bijvoorbeeld een intern bedrijfsnetwerk)." Die laatste verduidelijking geeft gevolg aan een opmerking van de GBA met betrekking tot het voorontwerp van wet (advies nr. 108/2021), waarbij de autoriteit zich met name afvroeg of met het begrip"private netwerken" enkel de netwerken van de

ou n'importe quel réseau privé, y compris, ceux qui sont mis en place par une personne à son domicile?

En réponse à la question de l'intervenant, posée au cours de la discussion générale, de savoir si cette disposition signifie que toute entreprise devra dorénavant conserver toutes les données, la ministre des Télécommunications a indiqué que ce n'était pas le cas. Elle estime que l'obligation de conserver des données ne concernerait que les opérateurs. Si tel est le cas, pourquoi le commentaire évoque-t-il les réseaux internes d'entreprise? Ne vaudrait-il pas mieux supprimer cet élément? Les ministres peuvent-il indiquer une nouvelle fois quels sont les réseaux visés?

Le ministre de la Justice souligne qu'il faut distinguer l'accès des services de renseignement à certaines données de l'obligation générale de conservation des données.

Les services de renseignement peuvent imposer aux opérateurs une réquisition de conservation, à la suite de laquelle les opérateurs doivent conserver les données qui ont déjà été générées (*quick freeze*), afin que l'enquête puisse être menée. Il s'agit donc d'une conservation spécifique à la demande des services de renseignement.

M. Michael Freilich (N-VA) a-t-il alors bien compris que cette réquisition de conservation peut être adressée non seulement aux opérateurs télécom, mais aussi à des réseaux d'entreprise privés?

Le ministre de la Justice indique que cette possibilité n'existe que dans le contexte de menaces pour la sécurité nationale. Il estime qu'il est normal que les services de renseignement bénéficient de la liberté d'action nécessaire dans de telles circonstances.

Art. 24 à 26

Ces articles ne donnent lieu à aucune observation.

Art. 27 et 28

Ces articles visent respectivement à instaurer la réquisition généralisée et la réquisition indifférenciée pour les besoins des services de renseignement et de sécurité. Ils définissent notamment les conditions, la procédure et les modalités de cette réquisition.

ondernemingen worden bedoeld dan wel om het even welk privaat netwerk, ook de netwerken die personen bij hen thuis hebben geïnstalleerd.

Op de vraag van de spreker, tijdens de algemene bespreking, of deze bepaling impliceert dat elke onderneming nu gegevens zal moeten bewaren, antwoordde de minister van Telecommunicatie ontkennend. Volgens haar trof de verplichting tot gegevensbewaring enkel operatoren. Als dat zo is, waarom wordt er in de toelichting dan gewag gemaakt van interne bedrijfsnetwerken? Wordt dit dan niet beter geschrapt? Kunnen de ministers nog eens duidelijk aangeven welke netwerken nu worden bedoeld?

De minister van Justitie wijst erop dat de toegang door de inlichtingendiensten tot bepaalde gegevens te onderscheiden valt van de algemene verplichting tot gegevensbewaring.

De inlichtingendiensten kunnen operatoren een bewaarbevel geven. Daarop moeten de operatoren reeds gegenereerde gegevens bewaren (*quick freeze*), zodat het onderzoek kan worden gevoerd. Het betreft dus een specifieke bewaring op vraag van de inlichtingendiensten.

Heeft *de heer Michael Freilich (N-VA)* dan goed begrepen dat dit bewaarbevel niet enkel kan gericht worden aan de telecomoperatoren, maar ook aan private bedrijfsnetwerken?

De minister van Justitie benadrukt dat deze mogelijkheid enkel bestaat in het kader van dreigingen tegen de nationale veiligheid. Hij vindt het maar normaal dat de inlichtingendiensten in die omstandigheden de nodige armslag krijgen.

Art. 24 tot 26

Over deze artikelen worden geen opmerkingen gemaakt.

Art. 27 en 28

Deze artikelen strekken ertoe een vordering tot gerichte respectievelijk algemene en ongedifferentieerde bewaring in te voeren ten behoeve van de inlichtingen- en veiligheidsdiensten. De artikelen bepalen onder meer de voorwaarden, procedure en modaliteiten van deze vordering.

M. Michael Freilich (N-VA) souhaiterait savoir ce qu'il doit advenir des données conservées après l'expiration du délai de conservation. Aucun des deux articles ne contient d'indication à ce propos, contrairement, par exemple, à l'article 22, qui modifie la loi du 5 août 1992 sur la fonction de police.

Le ministre de la Justice répond que les données doivent être détruites, et ce, conformément au RGPD, qui s'applique à tous les opérateurs. Il n'est pas nécessaire de le préciser dans le projet de loi à l'examen.

Le collaborateur du ministre précise qu'après utilisation, les données sont soit placées dans le dossier judiciaire, soit détruites. Toutes les données de la BNG sont ventilées, conformément aux directives en vigueur.

M. Michael Freilich (N-VA) prône la cohérence: soit le sort des données après l'expiration du délai de conservation est mentionné dans tous les chapitres applicables, soit il est omis partout.

Art. 29

Cet article vise à modifier à plusieurs égards l'article 18/7 de la loi du 30 novembre. Il harmonise ainsi la formulation de l'article 18/7 avec celle qui est utilisée pour les autres méthodes de renseignement. Il prévoit par ailleurs que les services de renseignement peuvent également demander les factures relatives à un abonnement spécifique.

M. Erik Gilissen (VB) demande des explications concernant la modification apportée par le 1°, qui remplace, dans l'article 18/7, les mots "Dans l'intérêt de l'exercice des missions, le dirigeant du service peut, par une décision écrite" par les mots "Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions". Pourquoi abandonner l'exigence de décision écrite?

Le ministre de la Justice explique que cette modification a été suggérée par le Comité permanent R. Il s'agit d'une simple reformulation, qui vise à renforcer la cohérence avec d'autres articles. Une décision écrite reste nécessaire.

Art. 30

Cet article ne donne lieu à aucune observation.

De heer Michael Freilich (N-VA) zou graag vernemen wat er dient te gebeuren met de bewaarde data na het verstrijken van de bewaartermijn. Geen van beide artikelen bevat daaromtrent enige indicatie, in tegenstelling tot bijvoorbeeld artikel 22, dat de wet van 5 augustus 1992 op het politieambt wijzigt.

De minister van Justitie antwoordt dat de gegevens wel degelijk moeten vernietigd worden, en wel op grond van de AVG die van toepassing is op alle operatoren. Het is niet nodig dit te expliciteren in het voorliggende wetsontwerp.

De medewerker van de minister verduidelijkt dat de gegevens na gebruik ofwel in het gerechtsdossier worden geplaatst, ofwel worden vernietigd. Alle gegevens in de ANG worden uitgesplitst, in overeenstemming met de geldende richtlijnen.

De heer Michael Freilich (N-VA) breekt een lans voor consistentie: ofwel wordt het lot van de gegevens na het verstrijken van de bewaartermijn in alle toepasselijke hoofdstukken vermeld, ofwel laat men het overal achterwege.

Art. 29

Dit artikel beoogt artikel 18/7 van de wet van 30 november 1998 op diverse punten te wijzigen. Zo wordt de bewoording van artikel 18/7 in lijn gebracht met de formulering gebruikt bij de andere inlichtingenmethoden. Voorts wordt bepaald dat de inlichtingendiensten ook de facturen met betrekking tot een welbepaald abonnement kunnen opvragen.

De heer Erik Gilissen (VB) had graag duiding bekomen omtrent de wijziging aangebracht door de bepaling onder 1°, waarbij in artikel 18/7, § 1, de woorden "In het belang van de uitoefening van de opdrachten, kan het diensthoofd, bij schriftelijke beslissing,"vervangen worden door de woorden "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten,". Waarom wordt het vereiste van een schriftelijke beslissing achterwege gelaten?

De minister van Justitie verduidelijkt dat deze wijziging werd voorgesteld door het Vast Comité I. Het betreft een loutere herformulering, met als doel de coherentie te verzekeren met andere artikelen. Een schriftelijke beslissing blijft noodzakelijk.

Art. 30

Over dit artikel worden geen opmerkingen gemaakt.

Art. 31

Il est renvoyé aux observations relatives à l'article 29.

Art. 32

Cet article ne donne lieu à aucune observation.

CHAPITRE 8

Modification de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 32/1 (*nouveau*)

Le gouvernement présente l'*amendement n° 15* (DOC 55 2572/002), qui tend à insérer un article 32/1, lequel apporte à son tour les modifications suivantes à l'article 81 de la loi du 2 août 2002, rétabli par la loi du 2 mai 2007 et modifié par les lois des 25 avril 2014 et 31 juillet 2017:

1° au paragraphe 1er, alinéa 3, les mots "visée à l'alinéa 1er" sont insérés entre les mots "dans sa décision" et les mots "les circonstances de fait";

2° le paragraphe 1er est complété par un alinéa, rédigé comme suit:

"Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, 2°, l'auditeur ou, en son absence, l'auditeur adjoint peut également requérir la collaboration:

— des personnes et institutions visées à l'article 5, § 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er;

— des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectuée, et qui ont

Art. 31

Er wordt verwezen naar de opmerkingen onder artikel 29.

Art. 32

Over dit artikel worden geen opmerkingen gemaakt.

HOOFDSTUK 8

Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 32/1 (*nieuw*)

De regering dient *amendement nr. 15* (DOC 55 2572/002) in, dat ertoe strekt een artikel 32/1 in te voegen, dat op zijn beurt beoogt de volgende wijzigingen aan te brengen in artikel 81 van de wet van 2 augustus 2002, hersteld bij de wet van 2 mei 2007 en gewijzigd bij de wetten van 25 april 2014 en 31 juli 2017:

1° in paragraaf 1 worden in het derde lid de woorden "bedoeld in het eerste lid" ingevoegd tussen de woorden "in zijn beslissing" en de woorden "opgave van";

2° paragraaf 1 wordt aangevuld met een lid, luidende:

"Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een in het tweede lid, 2°, bedoelde dienst, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, ook de medewerking vorderen van:

— de personen of instellingen bedoeld in artikel 5, § 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid;

— de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft

préalablement été communiquées par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er;

— des autres personnes morales qui sont l'abonné d'un des acteurs visés à l'alinéa 2, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, en application de l'alinéa 1er.";

3° au paragraphe 2, alinéa 2, les mots "les acteurs visés à l'alinéa 1er" sont remplacés par les mots "les acteurs visés au § 1er, alinéa 2, ainsi que les personnes et institutions visées au § 1er, alinéa 4,"."

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

Art. 33

Cet article ne donne lieu à aucune observation.

CHAPITRE 9

Modification de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS")

Art. 34 et 35

Ces articles ne donnent lieu à aucune observation.

CHAPITRE 10

Modification de la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits

Art. 36

Cet article ne donne lieu à aucune observation.

plaatsgevonden, die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid;

— andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaand meegedeeld zijn door een van de actoren bedoeld in het tweede lid, in toepassing van het eerste lid.";

3° in paragraaf 2, tweede lid, worden de woorden "de in het eerste lid bedoelde actoren" vervangen door de woorden "de actoren bedoeld in paragraaf 1, tweede lid, en de personen en instellingen bedoeld in paragraaf 1, vierde lid,".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 33

Over dit artikel worden geen opmerkingen gemaakt.

HOOFDSTUK 9

Wijzigingen van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet")

Art. 34 en 35

Over deze artikelen worden geen opmerkingen gemaakt.

HOOFDSTUK 10

Wijziging van de wet 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten

Art. 36

Over dit artikel worden geen opmerkingen gemaakt.

Art. 36/1 (*nouveau*)

Le gouvernement présente l'*amendement n° 16* (DOC 55 2572/002) qui tend à insérer un article 36/1 rédigé comme suit:

"Art. 36/1. L'article 11, § 1er, de la même loi, remplacé par la loi du 10 avril 2014, est complété par un alinéa rédigé comme suit:

"Pour procéder à l'identification de la personne concernée, le chef du service Inspection produits de consommation peut requérir la collaboration des personnes ou institutions visées à l'article 5, § 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un opérateur au sens de l'article 2, 11° de la loi du 13 juin 2005 relative aux communications électroniques.".".

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

CHAPITRE 11

Dispositions transitoires

Art. 37 et 38

L'article 37 règle l'entrée en vigueur de la conservation des données visée à l'article 126/1, § 3, alinéa 1er, 3° à 5°, de la loi du 13 juin 2005, à savoir la conservation de données dans les zones stratégiques. L'article 38 prévoit une période transitoire entre l'entrée en vigueur de la loi et la publication de l'arrêté ministériel visé à l'article 126/1, § 3, alinéa 1er, 1° de la loi précitée, relatif à la conservation sur la base de lieux caractérisés par un nombre élevé d'actes de criminalité grave

Mme Sophie De Wit (N-VA) indique que ces articles ne figuraient pas dans l'avant-projet de loi examiné par le Conseil d'État.

L'article 37 prévoit que l'entrée en vigueur n'aura lieu que dans cinq ans. Mme De Wit peut comprendre que la préparation de la mise en œuvre du régime concerné prenne un certain temps. Cependant, le report de l'entrée en vigueur est à peine motivé dans le projet de loi. Le ministre de la Justice peut-il fournir plus d'explications sur

Art. 36/1 (*nieuw*)

De regering dient *amendement nr. 16* (DOC 55 2572/002) in, dat ertoe strekt een artikel 36/1 in te voegen, luidende:

"Art. 36/1. Artikel 11, § 1, van dezelfde wet, vervangen bij de wet van 10 april 2014, wordt aangevuld met een lid, luidende:

"Met het oog op de identificatie van de betrokkene kan het diensthoofd van de inspectiedienst consumptieproducten de medewerking vorderen van de personen of instellingen, bedoeld in artikel 5, § 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een operator in de zin van artikel 2, 11° van de wet van 13 juni 2005 betreffende de elektronische communicatie.".".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

HOOFDSTUK 11

Overgangsbepalingen

Art. 37 en 38

Artikel 37 regelt de inwerkingtreding van de gegevensbewaring bedoeld in artikel 126/1, § 3, eerste lid, 3° tot 5°, van de wet van 13 juni 2005, namelijk de gegevensbewaring op basis van strategische zones. Artikel 38 voorziet in een overgangsperiode tussen de inwerkingtreding van de wet en de publicatie van het ministerieel besluit bedoeld in artikel 126/1, § 3, eerste lid, 1°, van voornoemde wet, betreffende de retentie op basis van plaatsen die worden gekenmerkt door een hoog aantal daden van zware criminaliteit.

Mevrouw Sophie De Wit (N-VA) geeft aan dat deze artikelen geen deel uitmaakten van het voorontwerp van wet waarover de Raad van State zich heeft gebogen.

Volgens artikel 37 zal de inwerkingtreding pas binnen vijf jaar plaatsvinden. Mevrouw De Wit kan begrijpen dat het enige tijd duurt om de uitvoering van de betrokken regeling voor te bereiden. De uitgestelde inwerkingtreding wordt echter amper gemotiveerd in het wetsontwerp. Kan de minister van Justitie hierover meer toelichting

ce point? Peut-il également indiquer ce qu'il adviendra dans l'intervalle?

Le projet de loi contient également peu d'explications à propos de l'article 38. Existe-t-il une garantie que l'arrêté ministériel sera pris rapidement? Cet arrêté prévoira-t-il des restrictions en matière de délai de conservation?

Le ministre de la Justice précise que seule la conservation de données dans les zones stratégiques entrera en vigueur en 2027. Les autres formes de conservation de données sur une base géographique, y compris la conservation de données sur la base du critère statistique, entreront en vigueur le plus rapidement possible. Si l'application de ce dernier critère, sur la base d'une objectivité différenciée, entraînait une couverture de l'ensemble du pays, cela ne poserait aucun problème.

Mme Sophie De Wit (N-VA) espère qu'entre-temps, ce système sera en effet étanche, comme l'affirme le ministre. Il convient d'éviter à tout prix que des enquêtes criminelles en cours ne soient jugées caduques.

Le ministre de la Justice partage cette préoccupation et fait observer que c'est précisément pour cette raison que le gouvernement a déposé le projet de loi à l'examen. Il souligne en outre qu'il est actuellement toujours possible, malgré l'annulation de la législation précédente, de conserver des données à des fins judiciaires, en vertu de la législation Antigone. La Cour de Cassation a accepté ce point de vue dans un arrêt récent.

Mme Sophie De Wit (N-VA) réplique que ce risque n'est pas inexistant. Elle estime qu'il est important que le ministre motive l'entrée en vigueur et les dispositions transitoires aux fins du rapport.

M. Erik Gilissen (VB) fait observer que l'arrêté ministériel visé à l'article 126/1, § 3, alinéa 1er, établira la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que leur durée de conservation. Sur ce point, le Parlement n'a donc pas voix au chapitre. Les délais de conservation peuvent en outre différer par arrondissement judiciaire et par zone de police, ce qui présente le risque, selon l'intervenant, d'aboutir à un enchevêtrement de délais de conservation qui sera incompréhensible pour le citoyen. Comment le citoyen pourra-t-il savoir combien de temps ses données seront conservées?

Le ministre de la Justice renvoie au rapport d'évaluation annuel soumis à la Chambre des représentants, conformément à l'article 126/1, § 6, en projet. Ce rapport mentionnera les délais de conservation par arrondissement judiciaire et, le cas échéant, par zone de police.

verschaffen? Kan hij ook aangeven wat er in de tussentijd zal gebeuren?

Ook omtrent artikel 38 bevat het wetsontwerp weinig toelichting. Is er een garantie dat het ministerieel besluit snel genomen zal worden? Gelden er beperkingen inzake de bewaartermijn die in dat besluit zal bepaald worden?

De minister van Justitie verduidelijkt dat enkel de gegevensbewaring op basis van strategische zones in 2027 in werking zal treden. De andere vormen van gegevensbewaring op geografische basis, inclusief de dataretentie volgens het statistisch criterium, zullen zo snel mogelijk in werking treden. Als de toepassing van dat laatste criterium, op basis van een gedifferentieerde objectiviteit, ertoe zou leiden dat het ganse land wordt bestreken, vormt dat geen probleem.

Mevrouw Sophie De Wit (N-VA) hoopt dat het systeem in de tussentijd inderdaad waterdicht is, zoals de minister beweert. Het moet te allen prijze worden vermeden dat lopende strafonderzoeken kaduuk bevonden worden.

De minister van Justitie deelt die bekommernis en merkt op dat het net om die reden is dat de regering dit wetsontwerp heeft ingediend. Hij wijst er bovendien op dat op dit moment, ondanks de vernietiging van de vorige wetgeving, nog steeds aan dataretentie voor justitiële doeleinden kan worden gedaan, en wel op grond van de Antigoon-wetgeving. Het Hof van Cassatie heeft deze zienswijze in een recent arrest aanvaard.

Mevrouw Sophie De Wit (N-VA) repliceert dat het risico niet nul is. Ze acht het belangrijk dat de minister de inwerkingtreding en overgangsbepalingen motiveert ten behoeve van het verslag.

De heer Erik Gilissen (VB) merkt op dat het ministerieel besluit bedoeld in artikel 126/1, § 3, eerste lid, 1°, de lijst zal vaststellen van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn. Het Parlement heeft hierin dus geen zeggenschap. De bewaartermijnen kunnen daarenboven verschillen per gerechtelijk arrondissement en per politiezone, wat volgens de spreker het risico met zich brengt van een wirwar van bewaartermijnen waarbij de burger door de bomen het bos niet ziet. Hoe zal de burger kunnen weten hoe lang zijn gegevens bewaard zullen worden?

De minister van Justitie verwijst naar het evaluatieverslag dat jaarlijks aan de Kamer van volksvertegenwoordigers zal worden uitgebracht, overeenkomstig het ontworpen artikel 126/1, § 6. De bewaartermijnen zullen daarin per gerechtelijk arrondissement en desgevallend

Le ministre souligne également que l'arrêté ministériel sera publié au *Moniteur belge.*

Art. 39 (*nouveau*)

Le gouvernement présente l'*amendement n° 5* (DOC 55 2572/002) tendant à compléter le projet de loi par un article 39 rédigé comme suit:

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

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

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

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

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

Art. 40 (*nouveau*)

Le gouvernement présente l'*amendement n° 7* (DOC 55 2572/002) tendant à compléter le projet de loi par un article 40 rédigé comme suit:

"Art. 40. Les modifications à l'article 127 ne s'applique que pour les identifications par les opérateurs des abonnés qui sont réalisées après l'entrée en vigueur de la présente loi.

L'article 127, § 5, alinéa 2, entre au vigueur deux ans après la publication de la présente loi.

Entre l'entrée en vigueur de la présente loi et la date fixée à l'alinéa 2, les opérateurs visés à l'article 127, § 5, alinéa 2, permettent aux abonnés de s'identifier à

per politiezone worden vermeld. Hij wijst er ook op dat het ministerieel besluit in het *Belgisch Staatsblad* zal worden gepubliceerd.

Art. 39 (*nieuw*)

De regering dient *amendement nr. 5* (DOC 55 2572/002) in, dat ertoe strekt het wetsontwerp aan te vullen met een artikel 39, luidende:

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

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

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

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

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

Art. 40 (*nieuw*)

De regering dient *amendement nr. 7* (DOC 55 2572/002) in, dat ertoe strekt het wetsontwerp aan te vullen met een artikel 40, luidende:

"Art. 40. De wijzigingen van artikel 127 zijn enkel van toepassing voor de identificaties door de operatoren van de abonnees die gebeuren na de inwerkingtreding van deze wet.

Artikel 127, § 5, tweede lid, wordt van kracht twee jaar na de bekendmaking van deze wet.

Tussen de inwerkingtreding van deze wet en de in het tweede lid vastgestelde datum maken de in artikel 127, § 5, tweede lid, bedoelde operatoren het voor de abonnees

l'aide des documents visés à l'article 127, § 5, alinéa 2, 1° à 18°, 20° à 24°, 26°, 28° et 31°, dans le cadre d'au moins une méthode d'identification de leur choix.

Les opérateurs mettent en œuvre l'article 127, § 6, au plus tard 24 mois après la publication de la présente loi.

Lorsqu'un opérateur met en œuvre la méthode d'identification indirecte visée à l'article 127, § 9, alinéa 1er, 3°, il conserve les données qui y sont visées au plus tard 24 mois après la publication de la présente loi.

Les opérateurs mettent en œuvre l'article 127, § 9, alinéa 1er, 6°, et alinéa 2 au plus tard 24 mois après la publication de la présente loi. Les personnes morales visées par ces dispositions obtiennent l'agrément au plus tard 24 mois après la publication de la présente loi."

*
* *

Il est renvoyé à la discussion générale et à la justification écrite de l'amendement.

V. — **VOTES**

CHAPITRE 1ER

Disposition générale

Article 1er

L'article 1 est adopté à l'unanimité.

CHAPITRE 2

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

Art. 2

L'article 2 est adopté par 12 voix contre 4.

Art. 3

L'article 3 est adopté par 10 voix contre 4 et 2 abstentions.

mogelijk om zich te identificeren aan de hand van de documenten bedoeld in artikel 127, § 5, tweede lid, 1° tot 18°, 20° tot 24°, 26°, 28°, en 31°, in het kader van minstens één identificatiemethode van hun keuze.

De operatoren leggen artikel 127, § 6, uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer.

Wanneer een operator de indirecte identificatiemethode bedoeld in artikel 127, § 9, eerste lid, 3°, ten uitvoer legt, bewaart hij de gegevens die erin worden beoogd uiterlijk 24 maanden na de bekendmaking van deze wet.

De operatoren leggen artikel 127, § 9, eerste lid, 6°, en tweede lid, uiterlijk 24 maanden na de bekendmaking van deze wet ten uitvoer. De in deze bepalingen bedoelde rechtspersonen verkrijgen de erkenning uiterlijk 24 maanden na de bekendmaking van deze wet.".

*
* *

Er wordt verwezen naar de algemene bespreking en naar de schriftelijke verantwoording bij het amendement.

V. — **STEMMINGEN**

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Artikel 1 wordt eenparig aangenomen.

HOOFDSTUK 2

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

Art. 2

Artikel 2 wordt aangenomen met 12 tegen 4 stemmen.

Art. 3

Artikel 3 wordt aangenomen met 10 tegen 4 stemmen en 2 onthoudingen.

Art. 4

L'article 4 est adopté par 12 voix contre 4.

Art. 5

L'article 5 est adopté par 10 voix contre 6.

Art. 6 et 7

Les articles 6 et 7 sont successivement adoptés par 15 voix contre 1.

Art. 8

L'amendement n° 1 tendant à remplacer l'article 8 est adopté par 10 voix contre 4 et 2 abstentions.

Art. 9

L'amendement n° 2 est adopté par 15 voix contre 1.

L'article 9, ainsi modifié, est adopté par 10 voix contre 3 et 3 abstentions.

Art. 9/1 *(nouveau)*

L'amendement n° 3 tendant à insérer un article 9/1 est adopté par 10 voix contre 6.

Art. 10

L'amendement n° 6 tendant à remplacer l'article 10 est adopté par 10 voix contre 4 et 2 abstentions.

Art. 11

L'article 11 est adopté par 10 voix contre 6.

Art. 12

L'article 12 est adopté par 12 voix contre 4.

Art. 4

Artikel 4 wordt aangenomen met 12 tegen 4 stemmen.

Art. 5

Artikel 5 wordt aangenomen met 10 tegen 6 stemmen.

Art. 6 en 7

De artikelen 6 en 7 worden achtereenvolgens aangenomen met 15 stemmen tegen 1.

Art. 8

Amendement nr. 1, dat ertoe strekt artikel 8 te vervangen, wordt aangenomen met 10 tegen 4 stemmen en 2 onthoudingen.

Art. 9

Amendement nr. 2 wordt aangenomen met 15 stemmen tegen 1.

Het aldus gewijzigde artikel 9 wordt aangenomen met 10 tegen 3 stemmen en 3 onthoudingen.

Art. 9/1 (*nieuw*)

Amendement nr. 3, dat tot doel heeft een artikel 9/1 in te voegen, wordt aangenomen met 10 tegen 6 stemmen.

Art. 10

Amendement nr. 6, dat beoogt artikel 10 te vervangen, wordt aangenomen met 10 tegen 4 stemmen en 2 onthoudingen.

Art. 11

Artikel 11 wordt aangenomen met 10 tegen 6 stemmen.

Art. 12

Artikel 12 wordt aangenomen met 12 tegen 4 stemmen.

Art. 13

L'article 13 est adopté par 10 voix contre 4 et 2 abstentions.

Art. 14

L'amendement n° 4 est adopté par 15 voix contre 1.

L'article 14, ainsi modifié, est adopté par 12 voix contre 4.

CHAPITRE 3

Modifications à la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques

Art. 15

L'article 15 est adopté par 13 voix contre 1 et 2 abstentions.

CHAPITRE 4

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

Art. 16

L'amendement n° 8 tendant à remplacer l'article 16 est adopté par 12 voix contre 1 et 3 abstentions.

Art. 17

L'amendement n° 9 tendant à remplacer l'article 17 est adopté par 12 voix contre 1 et 3 abstentions.

Art. 18

L'amendement n° 10 tendant à remplacer l'article 18 est adopté par 12 voix contre 1 et 3 abstentions.

Art. 13

Artikel 13 wordt aangenomen met 10 tegen 4 stemmen en 2 onthoudingen.

Art. 14

Amendement nr. 4 wordt aangenomen met 15 stemmen tegen 1.

Het aldus gewijzigde artikel 14 wordt aangenomen met 12 tegen 4 stemmen.

HOOFDSTUK 3

Wijzigingen aan de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

Art. 15

Artikel 15 wordt aangenomen met 13 stemmen tegen 1 en 2 onthoudingen.

HOOFDSTUK 4

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

Art. 16

Amendement nr. 8, dat ertoe strekt artikel 16 te vervangen, wordt aangenomen met 12 stemmen tegen 1 en 3 onthoudingen.

Art. 17

Amendement nr. 9, dat beoogt artikel 17 te vervangen, wordt aangenomen met 12 stemmen tegen 1 en 3 onthoudingen.

Art. 18

Amendement nr. 10, dat tot doel heeft artikel 18 te vervangen, wordt aangenomen met 12 stemmen tegen 1 en 3 onthoudingen.

Art. 19

L'amendement n° 11 tendant à remplacer l'article 19 est adopté par 15 voix contre 1.

Art. 19/1 *(nouveau)*

L'amendement n° 12 tendant à insérer un article 19/1 est adopté par 15 voix contre 1.

Art. 19/2 *(nouveau)*

L'amendement n° 13 tendant à insérer un article 19/2 est adopté par 12 voix contre 1 et 3 abstentions.

CHAPITRE 5

Modifications au Code d'instruction criminelle

Art. 20

L'article 20 est adopté par 13 voix contre 1 et 2 abstentions.

Art. 20/1 *(nouveau)*

L'amendement n° 14 tendant à insérer un article 20/1 est adopté par 12 voix contre 1 et 3 abstentions.

Art. 21

L'article 21 est adopté par 15 voix contre 1.

CHAPITRE 6

Modifications à la loi du 5 août 1992 sur la fonction de police

Art. 22

L'article 22 est adopté par 13 voix contre 3.

Art. 19

Amendement nr. 11, dat ertoe strekt artikel 19 te vervangen, wordt aangenomen met 15 stemmen tegen 1.

Art. 19/1 (*nieuw*)

Amendement nr. 12, dat ertoe strekt een artikel 19/1 in te voegen, wordt aangenomen met 15 stemmen tegen 1.

Art. 19/2 (*nieuw*)

Amendement nr. 13, tot invoeging van een artikel 19/2, wordt aangenomen met 12 stemmen tegen 1 en 3 onthoudingen.

HOOFDSTUK 5

Wijzigingen aan het Wetboek van strafvordering

Art. 20

Artikel 20 wordt aangenomen met 13 stemmen tegen 1 en 2 onthoudingen.

Art. 20/1 (*nieuw*)

Amendement nr. 14, dat ertoe strekt een artikel 20/1 in te voegen, wordt aangenomen met 12 stemmen tegen 1 en 3 onthoudingen.

Art. 21

Artikel 21 wordt aangenomen met 15 stemmen tegen 1.

HOOFDSTUK 6

Wijzigingen aan de wet van 5 augustus 1992 op het politieambt

Art. 22

Artikel 22 wordt aangenomen met 13 tegen 3 stemmen.

CHAPITRE 7

Modifications à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Art. 23

L'article 23 est adopté 12 voix contre 4.

Art. 24 et 25

Les articles 24 et 25 sont successivement adoptés par 15 voix et 1 abstention.

Art. 26

L'article 26 est adopté par 15 voix contre 1.

Art. 27 à 30

Les articles 27 à 30 sont successivement adoptés par 10 voix contre 4 et 2 abstentions.

Art. 31

L'article 31 est adopté par 14 voix et 2 abstentions.

Art. 32

L'article 32 est adopté par 12 voix contre 4.

CHAPITRE 8

Modifications à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 32/1 *(nouveau)*

L'amendement n° 15 tendant à insérer un article 32/1 est adopté par 13 voix et 3 abstentions.

Art. 33

L'article 33 est adopté par 13 voix contre 3.

HOOFDSTUK 7

Wijzigingen aan de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Art. 23

Artikel 23 wordt aangenomen met 12 tegen 4 stemmen.

Art. 24 en 25

De artikelen 24 en 25 worden achtereenvolgens aangenomen met 15 stemmen en 1 onthouding.

Art. 26

Artikel 26 wordt aangenomen met 15 stemmen tegen 1.

Art. 27 tot 30

De artikelen 27 tot 30 worden achtereenvolgens aangenomen met 10 tegen 4 stemmen en 2 onthoudingen.

Art. 31

Artikel 31 wordt aangenomen met 14 stemmen en 2 onthoudingen.

Art. 32

Artikel 32 wordt aangenomen met 12 tegen 4 stemmen.

HOOFDSTUK 8

Wijzigingen aan de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 32/1 (*nieuw*)

Amendement nr. 15, dat ertoe strekt een artikel 32/1 in te voegen, wordt aangenomen met 13 stemmen en 3 onthoudingen.

Art. 33

Artikel 33 wordt aangenomen met 13 tegen 3 stemmen.

CHAPITRE 9

Modifications à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ("loi NIS")

Art. 34 et 35

Les articles 34 et 35 sont successivement adoptés par 13 voix contre 3.

CHAPITRE 10

Modification à la loi du 24 janvier 1977 relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits

Art. 36

L'article 36 est adopté par 13 voix et 3 abstentions.

Art. 36/1 *(nouveau)*

L'amendement n° 16 tendant à insérer un article 36/1 est adopté par 13 voix et 3 abstentions.

CHAPITRE 11

Dispositions transitoires

Art. 37

L'article 37 est adopté par 12 voix contre 1 et 3 abstentions.

Art. 38

L'article 38 est adopté par 10 voix contre 1 et 5 abstentions.

Art. 39 *(nouveau)*

L'amendement n° 5 tendant à compléter le projet de loi par un article 39 est adopté par 10 voix contre 1 et 5 abstentions.

HOOFDSTUK 9

Wijzigingen aan de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid ("NIS-wet")

Art. 34 en 35

De artikelen 34 en 35 worden achtereenvolgens aangenomen met 13 tegen 3 stemmen.

HOOFDSTUK 10

Wijziging aan de wet van 24 januari 1977 betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere producten

Art. 36

Artikel 36 wordt aangenomen met 13 stemmen en 3 onthoudingen.

Art. 36/1 (*nieuw*)

Amendement nr. 16, dat ertoe strekt een artikel 36/1 in te voegen, wordt aangenomen met 13 stemmen en 3 onthoudingen.

HOOFDSTUK 11

Overgangsbepalingen

Art. 37

Artikel 37 wordt aangenomen met 12 stemmen tegen 1 en 3 onthoudingen.

Art. 38

Artikel 38 wordt aangenomen met 10 stemmen tegen 1 en 5 onthoudingen.

Art. 39 *(nieuw)*

Amendement nr. 5, dat ertoe strekt een artikel 39 in te voegen, wordt aangenomen met 10 stemmen tegen 1 en 5 onthoudingen.

Art. 40 *(nouveau)*

L'amendement n° 7 tendant à compléter le projet de loi par un article 40 est adopté par 10 voix contre 1 et 5 abstentions.

À la demande de *Mme Sophie De Wit (N-VA)*, la commission décide, en application de l'article 83.1 du Règlement, de procéder à une deuxième lecture du projet de loi à l'examen. Elle souhaite disposer d'une note de légistique du Service juridique à cette fin.

Lors de sa réunion du 9 juin 2022, la commission, en application de l'article 78.6 du Règlement, a approuvé le rapport avec 16 voix et 1 abstention.

Les rapporteurs, *Le président,*

Dieter VANBESIEN Stefaan VAN HECKE

Albert VICAIRE

Art. 40 *(nieuw)*

Amendement nr. 7, dat ertoe strekt een artikel 40 in te voegen, wordt aangenomen met 10 stemmen tegen 1 en 5 onthoudingen.

Op verzoek van *mevrouw Sophie De Wit (N-VA)* beslist de commissie, met toepassing van artikel 83.1 van het Reglement, over te gaan tot een tweede lezing van het ter bespreking voorliggende wetsontwerp. De commissie wenst daartoe te beschikken over een wetgevingstechnische nota van de Juridische Dienst.

Tijdens haar vergadering van 9 juni 2022 heeft de commissie, met toepassing van artikel 78.6 van het Reglement, het verslag goedgekeurd met 16 stemmen en 1 onthouding.

De rapporteurs, *De voorzitter,*

Dieter VANBESIEN Stefaan VAN HECKE

Albert VICAIRE

Imprimerie centrale – Centrale drukkerij