

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

26 februari 2016

WETSONTWERP

**betreffende het verzamelen en het bewaren
van de gegevens in de sector van de
elektronische communicatie**

VERSLAG VAN DE EERSTE LEZING

NAMENS DE COMMISSIE
VOOR DE INFRASTRUCTUUR, HET VERKEER EN DE
OVERHEIDSBEDRIJVEN
UITGEBRACHT DOOR
DE HEER **Peter DEDECKER**

INHOUD

Blz.

I. Procedure	3
II. Inleidende uiteenzetting door de heer Alexander De Croo, vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post	3
III. Algemene bespreking.....	8
A. Vragen en opmerkingen van de leden.....	8
B. Antwoorden van de minister	12
C. Replieken	15
D. Bijkomende antwoorden van de minister	16
IV. Artikelsgewijze bespreking en stemmingen	17
V. Verzoek tot tweede lezing	19

Zie:

Doc 54 **1567/ (2015/2016):**

001: Wetsontwerp.

002: Erratum.

003 en 004: Amendementen.

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

26 février 2016

PROJET DE LOI

**relatif à la collecte et à la conservation des
données dans le secteur des communications
électroniques**

RAPPORT DE LA PREMIÈRE LECTURE

FAIT AU NOM DE LA COMMISSION
DE L'INFRASTRUCTURE, DES COMMUNICATIONS ET
DES ENTREPRISES PUBLIQUES
PAR
M. **Peter DEDECKER**

SOMMAIRE

Pages

I. Procédure	3
II. Exposé introductif de M. Alexander De Croo, vice- premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste.....	3
III. Discussion générale.....	8
A. Questions et observations des membres	8
B. Réponses du ministre	12
C. Répliques.....	15
D. Réponses supplémentaires du ministre	16
IV. Discussion des articles et votes	17
V. Demande de deuxième lecture	19

Voir:

Doc 54 **1567/ (2015/2016):**

001: Projet de loi.

002: Erratum.

003 et 004: Amendements.

**Samenstelling van de commissie op de datum van indiening van het verslag/
Composition de la commission à la date de dépôt du rapport**

Voorzitter/Président: Karine Lalieux

A. — Vaste leden / Titulaires:

N-VA Inez De Coninck, Peter Dedecker, Daphné Dumery,
Wouter Raskin
PS Laurent Devin, Emir Kir, Karine Lalieux
MR Emmanuel Burton, Jean-Jacques Flahaux, Gilles Foret
CD&V Jef Van den Bergh, Veli Yüksel
Open Vld Sabien Lahaye-Battheu, Nele Lijnen
sp.a David Geerts
Ecolo-Groen Marcel Cheron
cdH Isabelle Poncelet

B. — Plaatsvervangers / Suppléants:

An Capoen, Christoph D'Haese, Koenraad Degroote, Yoleen Van Camp,
Bert Wollants
Julie Fernandez Fernandez, Gwenaëlle Grovonius, Eric Massin, Daniel
Senesael
Sybille de Coster-Bauchau, David Clarinval, Benoît Piedboeuf, Philippe
Pivin
Roel Deseyn, Veerle Heeren, Stefaan Vercamer
Luk Van Biesen, Dirk Van Mechelen, Tim Vandenput
Karin Temmerman, Alain Top
Stefaan Van Hecke, Gilles Vanden Burre
Benoît Lutgen, Vanessa Matz

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

VB Jan Penris

N-VA	:	Nieuw-Vlaamse Alliantie
PS	:	Parti Socialiste
MR	:	Mouvement Réformateur
CD&V	:	Christen-Democratisch en Vlaams
Open Vld	:	Open Vlaamse liberalen en democraten
sp.a	:	socialistische partij anders
Ecolo-Groen	:	Ecologistes Confédérés pour l'organisation de luttes originales – Groen
cdH	:	centre démocrate Humaniste
VB	:	Vlaams Belang
PTB-GOI	:	Parti du Travail de Belgique – Gauche d'Ouverture
DéFI	:	Démocrate Fédéraliste Indépendant
PP	:	Parti Populaire

Afkortingen bij de nummering van de publicaties:

DOC 54 0000/000: Parlementair document van de 54^e zittingsperiode +
basisnummer en volgnummer
QRVA: Schriftelijke Vragen en Antwoorden
CRIV: Voorlopige versie van het Integraal Verslag
CRABV: Beknopt Verslag
CRIV: Integraal Verslag, met links het definitieve integraal verslag
en rechts het vertaald beknopt verslag van de toespraken
(met de bijlagen)
PLEN: Plenum
COM: Commissievergadering
MOT: Moties tot besluit van interpellaties (beigekleurig papier)

Abréviations dans la numérotation des publications:

DOC 54 0000/000: Document parlementaire de la 54^e législature, suivi
du n° de base et du n° consécutif
QRVA: Questions et Réponses écrites
CRIV: Version Provisoire du Compte Rendu intégral
CRABV: Compte Rendu Analytique
CRIV: Compte Rendu Intégral, avec, à gauche, le
compte rendu intégral et, à droite, le compte rendu
analytique traduit des interventions (avec les an-
nexes)
PLEN: Séance plénière
COM: Réunion de commission
MOT: Motions déposées en conclusion d'interpellations
(papier beige)

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tél.: 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél.: 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

DAMES EN HEREN,

Uw commissie heeft dit wetsontwerp in eerste lezing besproken tijdens haar vergadering van 16 februari 2016.

I. — PROCEDURE

De commissie heeft met 9 tegen 2 stemmen het voorstel van de heer Benoit Hellings en mevrouw Fabienne Winckel tot een gedachtewisseling met de voor de privacy bevoegde staatssecretaris, de heer Bart Tommelein, enerzijds en anderzijds de organisatie van een gemeenschappelijke vergadering met de commissie Justitie over dit wetsontwerp verworpen.

II. — INLEIDENDE UITEENZETTING DOOR DE HEER ALEXANDER DE CROO, VICE-EERSTEMINISTER EN MINISTER VAN ONTWIKKELINGSSAMENWERKING, DIGITALE AGENDA, TELECOMMUNICATIE EN POST

De heer Alexander De Croo, vice-eersteminister en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecommunicatie en Post stelt dat het voorliggende wetsontwerp beoogt tegemoet te komen aan de vernietiging door het Grondwettelijk Hof in zijn arrest nr. 84/2015 van 11 juni 2015 van het artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie ("telecomwet"), zoals gewijzigd bij de wet van 30 juli 2013.

Het voert in de wet betreffende de elektronische communicatie voor de operatoren opnieuw de verplichting in om bepaalde gegevens betreffende de communicaties te bewaren, maar met een aantal verbeteringen (nieuwe artikelen 126 en 126/1).

Bovendien beoogt het wetsontwerp het Wetboek van Strafvordering en de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst te wijzigen en de waarborgen inzake de toegang tot de gegevens te versterken.

Voor die laatste wijzigingen verwijst de heer De Croo naar de minister van Justitie. Wat de aanpassingen aan de telecomwet betreft, gaat het in hoofdzaak om de volgende aspecten.

1. Herinvoering van de bewaarplicht

De vernietiging door het Grondwettelijk Hof van artikel 126 betekent niet zozeer dat het principe van een algemene bewaarplicht strijdig is met de grondrechten, wel dat dergelijke bewaarplicht niet kan opgelegd worden

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi en première lecture au cours de sa réunion du 16 février 2016.

I. — PROCÉDURE

Par 9 voix contre 2, la commission a rejeté la proposition de M. Benoit Hellings et Mme Fabienne Winckel visant à organiser, d'une part, un échange de vues avec le secrétaire d'État chargé de la protection de la vie privée, M. Bart Tommelein, et, d'autre part, une réunion commune avec la commission de la Justice au sujet du projet de loi à l'examen.

II. — EXPOSÉ INTRODUCTIF DE M. ALEXANDER DE CROO, VICE-PREMIER MINISTRE ET MINISTRE DE LA COOPÉRATION AU DÉVELOPPEMENT, DE L'AGENDA NUMÉRIQUE, DES TÉLÉCOMMUNICATIONS ET DE LA POSTE

M. Alexander De Croo, vice-premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste, indique que le projet de loi à l'examen vise à répondre à l'annulation par la Cour constitutionnelle, par son arrêt n° 84/2015 du 11 juin 2015, de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, tel que modifié par la loi du 30 juillet 2013.

Il réintroduit dans la loi sur les communications électroniques l'obligation pour les opérateurs de conserver certaines données relatives aux communications, mais avec des modifications (nouveaux articles 126 et 126/1).

Il modifie en outre le Code d'instruction criminelle et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en renforçant les garanties concernant l'accès aux données.

S'agissant de ces dernières modifications, M. De Croo renvoie au ministre de la Justice. En ce qui concerne les adaptations à la loi télécom, les principaux points sont les suivants.

1. Réintroduction de l'obligation de conservation

L'annulation par la Cour constitutionnelle de l'article 126 ne signifie pas que le principe d'une obligation générale de conservation est contraire aux droits fondamentaux, mais plutôt qu'une telle obligation ne peut

zonder de nodige waarborgen voor de privacy en de bescherming van de persoonsgegevens.

De bewaarplicht blijft immers noodzakelijk. De minister verwijst naar de recente terreuronderzoeken waarbij de toegang tot de communicatiegegevens is een noodzakelijke stap voor het identificeren van de personen en de banden die zij onderling hebben. Bij het onderzoek na een aanslag is het bijvoorbeeld noodzakelijk om terug te gaan in de communicaties van de verdachte, om na te gaan of hij alleen heeft gehandeld of om medeplichtigen te identificeren.

Ook in andere strafonderzoeken kunnen toegang tot communicatiegegevens van groot belang zijn voor het onderzoek: bijvoorbeeld bij industriële spionage, hacking van bankrekeningen, identiteitsdiefstal *etc.* Ook bijvoorbeeld bij onrustwekkende verdwijningen kunnen communicatiegegevens een sleutel zijn om tot oplossingen te komen.

Momenteel bewaren de operatoren de communicatiegegevens van hun klanten voor facturerings- en marketingdoeleinden, zolang dat daartoe nodig is. Die gegevens kunnen ongetwijfeld ook worden aangewend voor de strafonderzoeken of onderzoeken met het oog op inlichtingen. Het zou echter niet verstandig zijn de politieke en gerechtelijke overheden volledig afhankelijk te maken van de commerciële strategieën van de operatoren. Vandaar het belang van een wettelijke bewaringsplicht.

Een wettelijke bewaringsplicht is echter niet hetzelfde als “massaal toezicht”. Een wettelijke bewaringsplicht mag niet worden verward met het “grootschalig toezicht” dat wordt toegepast in sommige landen, waar heel veel informatie wordt gefilterd en verwerkt en waarbij ook de inhoud van de communicaties onderschept wordt.

De in dit wetsontwerp beoogde maatregel heeft niets te maken met dergelijke praktijken:

— de toegang tot de metagegevens (wie contacteert wie op welk moment en via welk kanaal) wordt verleend onder gerechtelijk toezicht voor wat het strafonderzoek betreft of onder toezicht van de BIM-commissie wat het onderzoek met het oog op inlichtingen betreft. Misbruiken zijn strafbaar.

— de bewaarplicht heeft in geen geval betrekking op de inhoud van de communicaties.

être imposée sans les garanties nécessaires quant à la protection de la vie privée et à la protection des données à caractère personnel.

L'obligation de conservation reste en effet une nécessité. Le ministre évoque les récentes enquêtes liées au terrorisme dans le cadre desquelles l'accès aux données de communication est nécessaire pour identifier les individus et les liens qui les unissent. Lors d'une enquête relative à un attentat, il est par exemple nécessaire d'analyser l'historique des communications du suspect pour déterminer s'il a agi seul ou pour identifier des complices.

L'accès aux données relatives aux communications peut également être un élément capital pour les enquêteurs dans d'autres enquêtes pénales: par exemple, en matière d'espionnage industriel, de piratage de comptes bancaires, de vol d'identité, *etc.* Les données relatives aux communications peuvent également jouer un rôle décisif dans la résolution d'affaires de disparition inquiétante.

À l'heure actuelle, les opérateurs conservent les données relatives aux communications de leurs clients pour les besoins de la facturation et du marketing tant que cela s'avère nécessaire pour ces objectifs. Ces données peuvent indubitablement aussi être utilisées pour les enquêtes pénales et de renseignement. Mais il ne serait pas judicieux de rendre les autorités policières et judiciaires entièrement dépendantes des stratégies commerciales des opérateurs. D'où l'importance d'une obligation légale de conservation.

Qui dit obligation légale de conservation ne dit pas “surveillance de masse”. Il ne faut toutefois pas confondre une obligation légale de conservation avec les pratiques de surveillance massive qu'appliquent certains pays où un nombre énorme de données sont filtrées et traitées, et où le contenu des communications est également intercepté.

La mesure visée dans ce projet de loi n'a strictement rien à voir avec ce genre de pratiques:

— L'accès aux métadonnées (qui a contacté qui, quand et par quel canal) se fait sous contrôle judiciaire pour les enquêtes pénales ou sous contrôle de la Commission BIM pour les enquêtes de renseignement. Les abus sont punissables.

— L'obligation légale de conservation ne concerne en aucun cas le contenu des communications.

— de toegang en het gebruik van gegevens zal steeds gericht zijn en beperkt zijn tot een concreet geval.

— de toegang tot de bewaarde gegevens zal bovendien steeds beperkt zijn in de tijd, met een maximum van 12 maanden. Men moet zeer aandachtig blijven omtrent de precieze hoeveelheid gegevens die moeten worden bewaard en omtrent de noodzaak van een bewarings-termijn van 12 maanden.

Om diezelfde reden voorziet het wetsontwerp in een dubbele grondige evaluatie: naast een jaarlijkse evaluatie komt er een heel grondige evaluatie van de termijnen en van de te bewaren gegevens, twee jaar na de inwerkingtreding van de nieuwe reglementering.

2. Antwoord op de kritieken van het Grondwettelijk Hof

De argumentatie van het Grondwettelijk Hof is heel kort en verwijst vooral naar de beslissing van het Hof van Justitie van de Europese Unie in verband met Europese Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (*"Data Retention"*).

Het Grondwettelijk Hof besluit dat het bestreden artikel 126 alsook de richtlijn een onevenredige beperking van het recht op inachtneming van de persoonlijke levenssfeer inhouden. Die schending van het evenredigheidsbeginsel vloeit voort uit de uit de combinatie van vier elementen:

— het gegeven dat de bewaring van de gegevens voor alle personen geldt;

— het gebrek aan differentiatie op grond van de categorieën van bewaarde gegevens en het nut ervan;

— het gebrek aan of de ontoereikendheid van regels inzake de toegang van de overheden tot de betrokken gegevens;

— het gebrek aan of het tekortschieten van de regels inzake de beveiliging van de gegevens bij de aanbieders of de operatoren.

Een aantal van die elementen hebben betrekking tot de verplichtingen die aan operatoren opgelegd worden in de telecomwet. Voor wat betreft de overige elementen verwijst de minister naar de minister van Justitie.

— L'accès et l'utilisation des données seront toujours ciblés et limités à un cas concret.

— En outre, l'accès aux données conservées sera toujours limité dans le temps (maximum 12 mois). On doit rester très attentifs à la quantité précise de données qui doivent être conservées et à la nécessité d'un délai de conservation de 12 mois.

C'est aussi pour cette raison que ce projet de loi prévoit une double évaluation approfondie. Outre une évaluation annuelle, une évaluation très approfondie des délais et des données à conserver est prévue, deux ans après l'entrée en vigueur de la nouvelle réglementation.

2. Réponse aux critiques de la Cour constitutionnelle

L'argumentaire de la Cour constitutionnelle est très bref et renvoie surtout à la décision de la Cour de Justice de l'Union européenne concernant la directive européenne 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (*"Data Retention"*).

La Cour conclut que l'article 126 attaqué, comme la directive, constitue une limitation disproportionnée du droit au respect de la vie privée. Cette violation du principe de proportionnalité découle de la combinaison de quatre éléments:

— le fait que la conservation des données concerne toutes les personnes;

— l'absence de différenciation en fonction des catégories de données conservées et leur utilité;

— l'absence ou l'insuffisance de règles quant à l'accès des autorités aux données concernées;

— et enfin, l'absence ou la faiblesse des règles sur la sécurisation des données chez les fournisseurs ou les opérateurs.

Un certain nombre de ces éléments concernent les obligations qui sont imposées aux opérateurs dans la loi sur les télécommunications. S'agissant des autres éléments, le ministre renvoie au ministre de la Justice.

Een eerste element is de differentiatie op grond van categorieën van gegevens. Het Grondwettelijk Hof wijst erop dat “[w]at [...] de bewaarperiode van de gegevens betreft, [...] de wet geen enkel onderscheid [maakt] tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken personen” (arrest nr. 84/2015, p. 34).

Om aan deze kritiek van het Hof tegemoet te komen, stelt het ontwerp een nieuw onderscheid in op grond van drie categorieën van gegevens:

— de eerste categorie heeft betrekking op de identificatiegegevens (wie is houder van een bepaald gsm-nummer, wat is het gsm-nummer van een bepaalde persoon, wie zit achter een bepaald IP-adres, enzovoort). Die gegevens worden het meest gevraagd;

— de tweede categorie heeft betrekking op de verbindings- en de lokalisatiegegevens (wat is inzonderheid de plaats en de duur van een communicatie);

— de derde categorie heeft betrekking op de persoonlijke communicatiegegevens (wie heeft gebeld of gecorrespondeerd met wie).

De voorwaarden inzake de toegang tot die gegevens variëren van de ene categorie tot de andere.

Aan deze categorieën van gegevens worden evenwel geen verschillende bewaarperiodes gekoppeld. Na veelvuldige besprekingen in de Regering en met de betrokken diensten en overheden werd immers geconcludeerd dat, gelet op de noodwendigheden inzake de strijd tegen terrorisme, een bewaringsperiode van 12 maanden noodzakelijk is voor elk van de drie categorieën.

Een tweede element is de versterking van de garanties op het niveau van de toegang van de overheden tot de gegevens.

Ook al werden de autoriteiten die gemachtigd zijn tot toegang tot de bewaarde gegevens, opgesomd in het vernietigd artikel 126, het Hof merkt op dat deze wet geen enkele materiële of procedurele voorwaarde vastgelegde met betrekking tot die toegang.

In het vernietigde artikel 126 werd, voor de twee voornaamste toegangsregelingen, verwezen naar de regels in het Wetboek van strafvordering voor het strafrechtelijke kader en in de wet van 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten. Deze regels worden door het ontwerp verder versterkt

Un premier élément est la différenciation sur la base des catégories de données. La Cour constitutionnelle note que “[...] en ce qui concerne la durée de conservation des données, la loi n’opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l’objectif poursuivi ou selon les personnes concernées” (arrêt n° 84/2015, p. 34).

Afin de répondre à la critique de la Cour, le projet de loi à l’examen introduit une nouvelle distinction sur base de trois catégories de données:

— La première catégorie concerne les données d’identification (qui est titulaire de tel numéro de gsm, quel est le numéro de gsm de telle personne, qui se trouve derrière telle adresse IP, ...). Ces données sont les plus demandées;

— La deuxième catégorie concerne les données de connexion et localisation (quel est notamment le lieu et la durée d’une communication);

— La troisième catégorie concerne les données de communication personnelles (qui a appelé ou a été en correspondance avec qui).

Les conditions d’accès à ces données varieront d’une catégorie à l’autre.

Les périodes de conservation liées à ces catégories de données sont toutefois identiques. Après de nombreuses discussions au sein du gouvernement et avec les services et autorités concernés, il a en effet été conclu que, vu les nécessités liées à la lutte contre les infractions terroristes, une période de 12 mois de conservation est nécessaire pour chacune des 3 catégories

Un deuxième élément est le renforcement des garanties au niveau de l’accès des autorités aux données.

Même si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l’article 126 annulé, la Cour observe qu’aucune condition matérielle ou procédurale n’est définie par la loi quant à cet accès.

L’article 126 annulé renvoyait, pour les deux régimes d’accès principaux, aux règles du Code d’instruction criminelle pour le cadre pénal et de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le projet à l’examen renforce encore davantage ces règles (compétence du ministre

(een bevoegdheid van de minister van Justitie) en ook het verband tussen artikel 126 en de voornoemde wetgeving wordt versterkt.

Het verduidelijkt ook het gegeven dat de toegang tot de bewaarde gegevens enkel mogelijk is voor de in artikel 126 uitdrukkelijk vermelde doeleinden.

Het wetsontwerp heeft, net zoals de vernietigde wet, ook andere secundaire doeleinden. Het voegt bepaalde gerichte doeleinden toe, maar voorziet tevens in belangrijke beperkingen.

— Zo zal de cel “Vermiste Personen” van de politie, via een door de Koning aangewezen politiedienst, weliswaar toegang krijgen tot de gegevens in het kader van een onrustwekkende verdwijning, maar alleen voor een periode van 48 uur, met dien verstande dat een ruimere toegang in het kader van het gerechtelijk onderzoek mogelijk is.

— De spoeddiensten die ter plaatse hulp bieden, kunnen in sommige situaties toegang krijgen tot bepaalde bewaarde gegevens, op voorwaarde dat de aanvraag aan de operator uiterlijk binnen 24 uur na de oproep wordt ingediend.

Wat een kwaadwillig gebruik van een elektronisch communicatienetwerk of elektronische communicatiedienst betreft, kan de Ombudsdienst voor Telecommunicatie de identificatiegegevens verkrijgen van de persoon die aan de oorsprong ligt van dat kwaadwillig gebruik.

Een derde element is de versterking van de beveiliging van de door de operatoren bewaarde gegevens.

Naar aanleiding van de bekommernissen geuit door het Hof van Justitie van de Europese Unie versterkt het ontwerp van wet de maatregelen die moeten worden genomen door de operatoren en aanbieders om de gegevens en de toegang ertoe te beschermen en te beveiligen.

Het gaat inzonderheid erom technologische beschermingsmaatregelen te nemen ten aanzien van die gegevens, de traceerbaarheid van de toegangen te waarborgen, de gegevens te vernietigen na het verstrijken van de termijn, of nog een aangestelde voor de gegevensbescherming aan te wijzen die moet toezien op de inachtneming van de verschillende regels ter zake. Er werd over gewaakt dat deze bijkomende beschermingsmaatregelen zo weinig mogelijk administratieve lasten voor de operatoren met zich zouden meebrengen, en hier werd ook met de sector over overlegd.

de la Justice), ainsi que le lien entre l'article 126 et les dispositions légales précitées.

Il clarifie aussi le fait que l'accès aux données conservées n'est possible que pour les finalités explicitement énumérées à l'article 126.

Le projet de loi, comme la loi annulée, prévoit aussi d'autres finalités secondaires. Il ajoute certaines finalités ciblées mais prévoit des limitations importantes.

— Ainsi, la cellule “personnes disparues” de la Police aura accès, par l'intermédiaire d'un service de police désigné par le Roi, aux données dans le cadre d'une disparition inquiétante mais seulement pour une période de 48 heures étant entendu qu'un accès plus large dans le cadre de l'enquête judiciaire est possible.

— Les services d'urgence offrant de l'aide sur place pourront obtenir certaines données conservées dans certaines situations mais pour autant que la demande envers l'opérateur intervienne au plus tard dans les 24 heures de l'appel.

— Pour ce qui concerne l'utilisation malveillante d'un réseau ou service de communication électronique, le Service de médiation pour les télécommunications pourra obtenir les données d'identification de la personne qui est à l'origine de cette utilisation malveillante.

Un troisième élément est le renforcement de la sécurisation des données conservées par les opérateurs.

Faisant suite aux préoccupations émises par la Cour de justice de l'Union européenne, le projet de loi renforce les mesures que doivent prendre les opérateurs et les fournisseurs de manière à protéger et à sécuriser les données et l'accès à celles-ci.

Il s'agit notamment de prendre des mesures de protection technologique à l'égard de ces données, d'assurer la traçabilité des accès, de détruire les données à l'expiration du délai, ou encore de désigner un préposé à la protection des données chargé de veiller au respect des différentes règles en la matière. Il a été veillé à ce que la charge administrative liée à ces mesures de protection complémentaires soit aussi réduite que possible pour les opérateurs et une concertation a également eu lieu avec le secteur à ce sujet.

III. — ALGEMENE BESPREKING

A. Vragen en opmerkingen van de leden

De heer Peter Dedecker (N-VA) looft de verbetering die dit wetsontwerp aan de wetgeving aanbrengt, vergeleken met de vorige legislatuur. In 2013 wilde regering dit op een drafje regelen, terwijl de Europese regelgeving al van 2006 dateerde. Het is een goede zaak om de artikelen 8 tot 13 die het Wetboek van strafvordering en de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten wijzigen naar de commissie Justitie te verzenden. Inhoudelijk vormt het wetsontwerp een verbetering met betrekking tot de toegang tot de bewaarde gegevens. De diverse termijnen komen ditmaal in de wet te staan, in plaats van in een koninklijk besluit.

Zal bij de aangekondigde dubbele evaluatie van deze wetgeving, waaronder de nieuw voorziene jaarlijkse evaluatie aan de Kamer van volksvertegenwoordigers, een onderscheid worden gemaakt naargelang de ouderdom van de gevraagde gegevens en de overheidsinstantie die ze opvraagt?

Ook met deze nieuwe wetgeving is het louter de ambitie om gegevens waarover men reeds beschikt te laten bewaren? Een horecazaak met een hotspot voor draadloos internet hoort niets bij te houden ter bewaring. Elektronische betalingen kunnen evenmin worden bijgehouden. Het is bij wet immers verboden om kredietkaartgegevens op te slaan. Bestaande contracten tussen private partijen hieromtrent blijven geldig? Aanbieders van elektronische diensten, zoals email, moeten de nodige duidelijkheid krijgen. Wie is dan verantwoordelijk voor het bewaren van de gevraagde gegevens: de klant of de dienstenaanbieder?

De spreker waarschuwt er ten slotte voor dat dergelijke wetgeving zal helpen tegen sommige misdrijven en bij het oplossen van sommige onrustwekkende verdwijningen, maar grote georganiseerde misdaad beschikt over uitwegen om de effecten van deze wetgeving te kunnen ontwijken.

De heer Benoît Hellings (Ecolo-Groen) informeert de commissie dat een volgens een wetenschappelijke studie van de UCL in 2013, verschenen in het tijdschrift *Nature*, is gebleken dat met slechts vier types metadata die deze wet laat bijhouden tot 90 % van de telecomgebruikers te identificeren is. De persoonlijke levenssfeer is door dit wetsontwerp veel meer in het geding dan de regering durft toe te geven. De gegevens worden immers van alle gebruikers bijgehouden, niet louter van specifieke profielen die een mogelijk gevaar voor de

III. — DISCUSSION GÉNÉRALE

A. Questions et observations des membres

M. Peter Dedecker (N-VA) salue la modification que le projet de loi à l'examen apporte à la législation par rapport à ce qui a été fait au cours de la législature précédente. En 2013, le gouvernement a voulu régler cette question dans la précipitation, alors que la réglementation européenne datait déjà de 2006. Il est positif que les articles 8 à 13, qui modifient le Code d'instruction criminelle et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, soient renvoyés à la commission de la Justice. La teneur du projet de loi apporte une amélioration en ce qui concerne l'accès aux données conservées. Les divers délais sont à présent inscrits dans la loi, plutôt que dans un arrêté royal.

La double évaluation annoncée de la loi proposée, dont la nouvelle évaluation annuelle destinée à la Chambre des représentants, fera-t-elle une distinction selon l'ancienneté des données demandées et l'autorité qui les demande?

Cette nouvelle législation vise-t-elle aussi uniquement la conservation de données déjà disponibles? Un établissement horeca proposant un point d'accès wifi ne doit conserver aucune donnée. Les paiements électroniques ne peuvent pas non plus être conservés. La loi interdit en effet de conserver les données de cartes de crédit. Les contrats existants conclus en la matière entre parties privées restent-ils valables? La clarté doit être faite à l'intention des fournisseurs de services électroniques. Qui est en l'occurrence responsable de la conservation des données demandées: le client ou le fournisseur de services?

L'intervenant prévient enfin qu'une telle législation aidera à lutter contre certaines infractions et à résoudre certaines disparitions inquiétantes, mais que la grande criminalité organisée dispose d'alternatives pour échapper aux effets de cette législation.

M. Benoît Hellings (Ecolo-Groen) porte à la connaissance de la commission qu'une étude scientifique de l'UCL de 2013, parue dans la revue *Nature*, montre qu'il est possible d'identifier 90 % des utilisateurs des télécommunications grâce à quatre types seulement de métadonnées conservées en vertu de cette loi. Le projet de loi à l'examen met la vie privée beaucoup plus en péril que ce que le gouvernement ose l'admettre. Ce sont en effet les données de tous les utilisateurs qui sont conservées, pas seulement celles des profils

openbare veiligheid vormen. De spreker refereert in dit verband aan de eerdere vernietiging door het Hof van Justitie van de Europese Unie van de Europese richtlijn 2006/24/EG. De eerdere vernietigingen door het Hof van Justitie en het Grondwettelijk Hof zijn het gevolg geweest van een gebrek aan proportionaliteit.

Er is bovendien de internationale context, van het Amerikaanse inlichtingenprogramma PRISM en buitenlandse inlichtingendiensten die zich reeds eerder een toegang hebben verschaft tot data van bijvoorbeeld Belgacom. Wetgeving die dergelijke gegevens laat bijhouden moet steeds streven naar een minimum aan bij te houden informatie en dat voor een zo kort mogelijke tijd. Waarom maakt het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer geen deel uit van de bijlagen van het wetsontwerp?

Het wetsontwerp voorziet in een bewaartermijn van 12 maanden. Een inzage die tot zes maanden in de tijd teruggaat zou een goed principe zijn. Waarom een bewaartermijn die een jaar bedraagt? De heer Hellings citeert de opmerking van de Raad van State: “of niet zou kunnen worden overwogen om, zonder afbreuk te doen aan de nagestreefde legitieme doelstellingen, een kortere algemene bewaartermijn te bepalen en tegelijk een regeling in te voeren waarbij de Koning, mits voorzien wordt in bepaalde procedurele waarborgen, zou kunnen worden gemachtigd om in objectieve omstandigheden van een specifieke potentiële bedreiging die nauwkeurig moeten worden afgebakend, de bewaartermijn van de gegevens te verlengen (waarbij de wetgever evenwel een bovengrens vaststelt voor die verlenging van de termijn) en om, in voorkomend geval, gelet op de aard of de omvang van de bedreiging, meteen ook een bepaalde geografische zone af te bakenen.” (DOC 54 1567/001, p. 84-85)

Bij terrorismeonderzoeken bestaat bovendien nu reeds — naast het bewaren van elektronische gegevens — de mogelijkheid tot het toepassen van de bijzondere inlichtingenmethoden, waarbij er de controle is van de onderzoeksrechter, de procureur en het Comité I.

Het Grondwettelijk Hof heeft de artikelen 122 en 123 van de wet van 13 juni 2005, die het bewaren van gegevens voor commerciële doelen regelt, niet vernietigd. Waarom heeft de regering van het voorliggende wetsontwerp geen gebruik gemaakt om deze artikelen te wijzigen?

Hoe verhoudt dit wetsontwerp zich tot het gegarandeerde beroepsgeheim van advocaten en artsen? Met name de orde van de Franstalige balies is sterk gekant

spécifiques qui représentent un danger potentiel pour la sécurité publique. L'intervenant se réfère à cet égard à l'annulation de la directive européenne 2006/24/CE prononcée antérieurement par la Cour de justice de l'Union européenne. Les annulations antérieures prononcées par la Cour de justice et par la Cour constitutionnelle ont résulté d'un manque de proportionnalité.

Il y a en outre le contexte international, et notamment le programme de renseignements américain PRISM ainsi que des services de renseignement étrangers qui ont déjà accédé aux données de Belgacom, par exemple. La législation qui prévoit la conservation de telles données doit toujours tendre à réduire au maximum les informations à conserver, et ce, pour la durée la plus courte possible. Pourquoi l'avis de la Commission de la protection de la vie privée n'est-il pas repris dans les annexes du projet de loi à l'examen?

Le projet de loi à l'examen prévoit une période de conservation de 12 mois. Un droit de consultation qui remonte jusqu'à six mois dans le temps serait un bon principe. Pourquoi un délai de conservation d'un an? M. Hellings cite l'observation du Conseil d'État: *“la question se pose toutefois de savoir s'il ne serait pas envisageable, sans nuire aux objectifs légitimes poursuivis, de définir un délai général de conservation plus restreint, tout en mettant en place un système dans lequel moyennant certaines garanties procédurales, le Roi pourrait être habilité, dans des circonstances objectives de menace potentielle spécifique à définir avec précision, à étendre le délai de conservation des données (le législateur fixant toutefois une limite à cette extension de délai), tout en définissant, le cas échéant, compte tenu de la nature ou de l'étendue de la menace, une zone géographique déterminée.”* (DOC 54 1567/001, p. 84-85).

De plus, dans les enquêtes pour terrorisme, il est déjà possible à l'heure actuelle non seulement de conserver les données électroniques, mais aussi d'appliquer les méthodes particulières de recueil de données, sous le contrôle du juge d'instruction, du procureur et du Comité R.

Les articles 122 et 123 de la loi du 13 juin 2005, qui règlent la conservation des données à des fins commerciales, n'ont pas été annulés par la Cour constitutionnelle. Pourquoi le gouvernement n'a-t-il pas modifié ces articles dans le cadre du projet de loi à l'examen?

Comment concilier ce projet de loi avec le secret professionnel garanti des avocats et des médecins? Le projet de loi à l'examen, ainsi que ses implications

tegen het voorliggende wetsontwerp en de mogelijke implicaties voor het beroepsgeheim van de advocaten.

Welke termijn krijgt de Ombudsdienst voor Telecommunicatie om gegevens op te vragen? Gegevens moeten worden bewaard op het grondgebied van de Europese Unie, om rekening te houden met het arrest van 8 april 2014 van het Hof van Justitie van de Europese Unie. Is deze vereiste niet achterhaald door de technologische evolutie, bijvoorbeeld door het bijhouden van gegevens in de zogenaamde *cloud*?

De heer Hellings deelt de volgende vragen van de Raad van State, enerzijds of het “niet beter zou zijn de lijst van de strafbare feiten waarvoor de toegang toegestaan wordt, te beperken door van deze strafbare feiten een nauw keuriger opsomming te geven, zoals in artikel 90ter van het Wetboek van Strafvordering”? (DOC 54 1657/001, p. 94) Anderzijds, “of het niet beter zou zijn te bepalen dat de gegevens die krachtens het ontworpen artikel 126 bewaard worden, bewaard moeten worden in een databank die enkel bedoeld is voor die gegevens om het gevaar dat de desbetreffende gegevens niet verwijderd worden zoveel mogelijk in te perken”? (DOC 54 1567/001, p. 101)

De memorie van toelichting stelt meermaals dat het opvragen van dergelijke gegevens een gebruikelijke maatregel is geworden in gerechtelijke onderzoeken. Hoe vaak worden dergelijke verzoeken echter gedaan over gegevens die reeds zes maanden of langer oud zijn? Wellicht behoeft gerecht of politie doorgaans veel recentere gegevens? Onderzoek uit Duitsland, zowel op verzoek van de *Bundestag* als verricht door het *Max Planck Institute*, heeft uitgewezen dat het bijhouden van dergelijke gegevens geen impact heeft op het aantal opgeloste misdrijven. Alles zonder onderscheid 12 maanden laten bijhouden is bijgevolg buiten proportie.

Hoe zal de nodige samenwerking tussen het BIPT en de Commissie voor de bescherming van de persoonlijke levenssfeer worden geregeld? Beschikt het BIPT bovendien over de nodige mensen en middelen om de in het wetsontwerp geregelde rol te vervullen?

Wat zijn de gevolgen voor een gerechtelijk onderzoek indien een onderzoeksrechter op basis van een verkeerde kwalificatie van een misdrijf zekere bewijslast heeft weten te bemachtigen door middel van het opvragen van elektronische gegevens? Kan een procureur hiervan nog gebruik maken in zijn aanklacht?

Het wetsontwerp, ten slotte, zal niets kunnen ondernemen tegen sommige door terroristen en de georganiseerde criminaliteit gebruikte versleutelde elektronische

éventuelles au niveau du secret professionnel des avocats, sont fortement critiqués, en particulier par l'Ordre des barreaux francophones.

De quel délai le Service de médiation pour les télécommunications disposera-t-il pour réclamer la communication de données? Pour tenir compte de l'arrêt du 8 avril 2014 de la Cour de justice de l'Union européenne, les données doivent être conservées sur le territoire de l'Union européenne. Cette exigence n'est-elle pas dépassée par les évolutions technologiques et notamment par la conservation de données sur le “cloud”?

M. Hellings partage certaines interrogations du Conseil d'État, qui se demande, d'une part, “*s'il ne conviendrait pas (...) d'établir une liste plus restreinte des infractions pour lesquelles l'accès est autorisé, en énumérant plus précisément celles-ci, à l'instar de l'article 90ter du Code d'instruction criminelle*” (DOC 54 1657/001, pp. 93 et 94) et, d'autre part, si “*afin de limiter de manière maximale les risques de non-destruction des données concernées (...), il ne serait pas adéquat de prévoir que les données conservées en vertu de l'article 126 en projet doivent l'être dans une base de données exclusivement consacrée à ces données.*” (DOC 54 1567/001, p. 101)

L'exposé des motifs indique à plusieurs reprises que la demande de ces données est devenue une mesure routinière dans les instructions judiciaires. Combien de demandes de cette nature portent-elles sur des données veilles de six mois ou plus? La police n'a-t-elle vraisemblablement pas ordinairement besoin de données beaucoup plus récentes? Des recherches menées en Allemagne, tant à la demande du *Bundestag* que de l'institut Max Planck, indiquent que la conservation de ces données n'a aucun impact sur le nombre d'affaires élucidées. Par conséquent, il est excessif de prévoir de tout conserver durant douze mois sans discernement.

Comment la coopération nécessaire entre l'IBPT et la Commission de la protection de la vie privée sera-t-elle organisée? L'IBPT dispose-t-il en outre du personnel et des moyens nécessaires pour accomplir les missions que lui confie le projet de loi?

Si un juge d'instruction parvient à se procurer certaines preuves en demandant des données électroniques sur la base d'une qualification erronée à l'égard d'une infraction, quelles en seront les conséquences sur le plan de l'instruction judiciaire? Le procureur pourrait-il encore utiliser ces éléments lors de l'accusation?

Enfin, le projet de loi à l'examen ne permettra pas de lutter contre certaines applications électroniques cryptées utilisées par les terroristes et dans le cadre de

toepassingen. Nochtans gebruiken deze toepassingen wel degelijk de telecominfrastructuur.

Mevrouw Fabienne Winckel (PS) herinnert aan de woorden van de minister, bij de vernietiging van het toenmalig artikel 126 door het Grondwettelijk Hof, dat niet al de Belgen als verdachten worden beschouwd. Gelden deze woorden nog steeds? Dergelijk onderwerp verdient een meer grondige behandeling, met bijvoorbeeld hoorzittingen over de draagwijdte van het arrest van het Hof van Justitie van de Europese Unie over de richtlijn 2006/24/EG. Hetzelfde Hof moet zich trouwens nog uitspreken over een relevante prejudiciële vraag van een Zweedse rechter. De regering had dus beter afge wacht met de indiening van deze reparatiewetgeving.

De Duitse wetgeving zal veel minder ver gaan dan de Belgische. Klantengegevens (telefoonnummers, IP-nummers, gesprekstijd) zullen er tien weken worden bijgehouden en plaatsgegevens slechts vier weken. Inzage zal gebeuren voor ernstige misdrijven en onder de controle van een rechter. Vroegere statistieken wezen uit dat tot 90 % van de in Europa opgevraagde gegevens geen zes maanden in de tijd teruggingen. Waarom zal de Belgische wetgeving een veel langere bewaartijd en ruimere inzage mogelijk maken? De memorie van toelichting stelt zelfs uitdrukkelijk: "Vooreerst zou het onredelijk zijn om het opvragen van de gegevens bedoeld in artikel 46bis, § 1, 1° en 2°, enkel mogelijk te maken voor zware misdrijven." (DOC 54 1567/001, p. 15)

Waarom blijft het wetsontwerp beperkt tot garanties met betrekking tot het beroepsgeheim van louter advocaten, artsen en journalisten? De advocaten stellen zelfs dat de ontworpen garanties niet eens voldoende zijn.

De redactie van het wetsontwerp houdt bovendien geen rekening met de hervormingen van het door de Kamer van volksvertegenwoordigers aangenomen wetsontwerp tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (DOC 54 1418/017). Het vorderen van de telecomsector voor het identificeren van de gebruikers van telecommunicatiediensten wordt immers niet langer gekwalificeerd als een zogenaamde specifieke methode. De BIM-commissie houdt er dus geen toezicht meer over.

Is een dergelijk ruime opslag van gegevens eigenlijk nodig? Private gegevens van alle burgers worden immers opgeslagen. Er is bovendien te weinig informatie voorhanden over het aantal keer dat dergelijke informatie wordt gebruikt en voor welke doeleinden. Waarom wordt de inzage van de gegevens niet beperkt tot de zware misdrijven? Hoe reageert de regering op de mogelijke

la criminalité organisée. Or, ces applications s'appuient bien sur les infrastructures de télécommunication.

Mme Fabienne Winckel (PS) rappelle que le ministre a déclaré, lors de l'annulation de l'ancien article 126 par la Cour constitutionnelle, que tous les Belges n'étaient pas suspects. Est-ce encore vrai? Cette question mérite un examen plus approfondi, par exemple dans le cadre d'auditions sur la portée de l'arrêt de la Cour de justice de l'Union européenne sur la directive 2006/24/CE. La Cour de justice doit d'ailleurs encore se prononcer sur une question préjudicielle pertinente posée par un juge suédois. Le gouvernement aurait donc mieux fait d'attendre le dépôt de cette loi de réparation.

La législation allemande ira bien moins loin en la matière que la législation belge. Elle stipulera que les données relatives aux clients (numéros de téléphone, numéros IP, durée d'appel) seront conservées dix semaines, contre seulement quatre semaines pour les données de localisation. La consultation des données sera autorisée pour les infractions graves et sera contrôlée par un juge. Selon des statistiques antérieures, jusqu'à 90 % des données demandées en Europe ont moins de 6 mois. Dès lors, pourquoi la législation belge prévoit-elle une durée de conservation bien plus longue et des possibilités de consultation bien plus étendues? L'exposé des motifs est explicite: "*Tout d'abord, il serait déraisonnable de rendre la demande des données visées à l'article 46bis, § 1^{er}, 1° et 2° possible seulement pour les infractions graves.*" (DOC 54 1567/001, p. 15)

Pourquoi le projet de loi s'est-il limité à des garanties quant au secret professionnel des avocats, des médecins et des journalistes? Les avocats indiquent que les garanties proposées ne suffisent même pas.

En outre, le projet de loi ne tient absolument pas compte des réformes résultant de l'adoption par la Chambre des représentants du projet de loi modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice, (DOC 54 1418/017). En effet, les réquisitions adressées au secteur des télécoms pour identifier les utilisateurs de services de télécommunications ne sont plus qualifiées de méthodes spécifiques et ne sont dès lors plus contrôlées par la Commission BIM.

Est-il vraiment nécessaire de stocker autant de données? En effet, les données privées de tous les citoyens sont stockées. En outre, trop peu d'informations sont disponibles quant au nombre de consultations de ces données et quant aux objectifs de ces consultations. Pourquoi la consultation des données n'est-elle pas limitée aux infractions graves? Quel est la réaction du

inbreuken op het beroepsgeheim, bijvoorbeeld van advocaten? Het wetsontwerp stelt geen voorafgaande controle door een onafhankelijk orgaan bij de vraag tot de inzage van gegevens in. Dit was nochtans een argument van het Hof van Justitie bij het arrest over de richtlijn 2006/24/EG. Meer nog, de controle achteraf door de BIM-commissie is ten gevolge het wetsontwerp tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie een lege doos geworden.

De heer Veli Yüksel (CD&V) reageert dat het nut en de wenselijkheid van dergelijke wetgeving niet kan worden ontkend. Hij verwijst bijvoorbeeld naar de mogelijke indicaties die politie en gerecht voor hun onderzoeken tegen grote criminaliteit en terrorisme uit opgevraagde elektronische informatie kunnen putten. Het is evenwel belangrijk te waken over de evenredigheid bij het bewaren en opvragen van dergelijke gegevens uit de persoonlijke levenssfeer. Vallen communicatiediensten van sociale media eveneens onder de bepalingen van deze wetgeving, of blijft het beperkt tot meer klassieke vormen van elektronische communicatie zoals sms-berichten? Wie draagt de kostprijs voor de opslag gedurende twaalf maanden door de operatoren en de opzoekingen in de bewaarde gegevens? Wat heeft de studie over de geraamde kostprijs door het BIPT uitgegeven? Zullen alle overheidsdiensten aan gelijkaardige voorzorgsmaatregelen worden onderworpen, teneinde onrechtmatige verzoeken tot inzage te verhinderen?

B. Antwoorden van de minister

Advies van de privacycommissie

Het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer over dit wetsontwerp (advies nr. 33/2015 van 9 september 2015) is op de website van de Commissie te vinden.

Hoogdringendheid

De hoogdringendheid wordt ingegeven door het feit dat de rechtszekerheid na de vernietiging van zowel de Europese richtlijn als de nationale regeling moet worden hersteld.

Toepassingsgebied

De wet zal van toepassing zijn op publiek toegankelijke aanbieders van e-maildiensten die op de Belgische markt actief zijn.

gouvernement concernant les violations potentielles du secret professionnel, dans le cas par exemple des avocats? Le projet de loi ne confère à aucun organisme indépendant la mission d'examiner préalablement les demandes de consultation des données, ce qui était pourtant un argument de la Cour de Justice dans son arrêt relatif à la directive 2006/24/EG. De plus, le contrôle réalisé *a posteriori* par la Commission BIM est devenu une coquille vide par suite de l'adoption du projet de loi modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice.

M. Veli Yüksel (CD&V) répond que l'utilité et l'opportunité de cette législation sont indéniables. Il évoque notamment les indications que la police et la justice peuvent puiser des informations électroniques qu'elles demandent dans le cadre des enquêtes menées en matière de grande criminalité et de terrorisme. Il importe toutefois de veiller à la proportionnalité lorsque l'on conserve et demande des données à caractère personnel. Les services de communication des médias sociaux sont-ils également soumis à l'application de cette législation ou cette dernière reste-t-elle limitée à des formes plus classiques de communications électroniques, comme les sms? Qui assume le coût afférent à la conservation de ces données pendant douze mois par les opérateurs et aux recherches dans les données conservées? Quelles sont les conclusions de l'étude menée par l'IBPT sur le coût estimé? Tous les services publics seront-ils soumis à des mesures de précaution équivalentes, de manière à empêcher les demandes de consultation illicites?

B. Réponses du ministre

Avis de la commission de la protection de la vie privée

L'avis de la commission de la protection de la vie privée concernant le projet de loi (avis n° 33/2015 du 9 septembre 2015) est disponible sur le site de la Commission.

Extrême urgence

L'extrême urgence est dictée par le fait que la sécurité juridique doit être rétablie après l'annulation tant de la directive européenne que de la réglementation nationale.

Champ d'application

La loi s'appliquera aux fournisseurs et aux services de messagerie électronique accessibles au public et opérant sur le marché belge.

Duitse regeling

Zowel de Duitse geschiedenis als de Duitse gastronomie zijn verschillend van die van vele andere Europese landen, waaronder België. Een andere regeling hoeft dus niet te verbazen.

Standpunt advocaten

De minister van Justitie is beter geplaatst om op deze vraag te antwoorden.

Beroepsgeheim

De minister van Justitie is beter geplaatst om op deze vraag te antwoorden.

Bijzondere opsporingsmethodes

De minister van Justitie is beter geplaatst om op deze vraag te antwoorden.

Toegang advocaten

De minister van Justitie is beter geplaatst om op deze vraag te antwoorden.

Misbruik voor lichtere misdrijven

De minister van Justitie is beter geplaatst om op deze vraag te antwoorden.

Statistieken duurtijd

Ze zullen jaarlijks bij koninklijk besluit op 1 maart ter beschikking worden gesteld. Het verdient aanbeveling deze splitsing — naargelang het gegevens van meer dan 3, 6 of 9 maanden oud betreft — in de statistieken tot uiting te laten komen.

Betalingsgegevens

Deze gegevens worden door derden bewaard, niet door operatoren.

Hoster advocatenkantoor

Vanaf het ogenblik dat de e-maildienst niet publiek toegankelijk is, valt hij niet onder de bewaarverplichting.

Geëncrypteerde berichten

Versleuteling is een basisrecht. Het gaat dus in de eerste plaats om niet-geëncrypteerde gegevens. PS4 is nota bene niet geëncrypteerd.

Dispositif allemand

Tant l'histoire de l'Allemagne que sa gastronomie diffèrent de celles de nombreux autres pays européens, dont la Belgique. Il ne faut donc pas s'étonner qu'un autre dispositif y soit appliqué.

Point de vue des avocats

Le ministre de la Justice est mieux placé pour répondre à cette question.

Secret professionnel

Le ministre de la Justice est mieux placé pour répondre à cette question.

Méthodes particulières de recherche

Le ministre de la Justice est mieux placé pour répondre à cette question.

Accès des avocats

Le ministre de la Justice est mieux placé pour répondre à cette question.

Abus pour infractions mineures

Le ministre de la Justice est mieux placé pour répondre à cette question.

Statistiques sur la durée

Elles seront annuellement mises à disposition, le 1^{er} mars, par arrêté royal. Il est recommandé de faire ressortir cette distinction — selon que les données sont vieilles de plus de 3, 6 ou 9 mois — dans les statistiques.

Données relatives aux paiements

Ces données sont conservées par des tiers, pas par les opérateurs.

Hébergeur bureau d'avocats

Dès lors que le service de courrier électronique n'est pas accessible au public, l'obligation de conservation ne lui est pas applicable.

Messages cryptés

Le cryptage est un droit fondamental. Ce sont donc en premier lieu les messages non cryptés qui sont concernés. La Playstation 4 n'est pas cryptée, *nota bene*.

Verzamelen/toegang hebben

Voorliggende artikelen van het wetsontwerp hebben het alleen over wie wat gedurende hoe lang moet bewaren en niet over wie tot welke gegevens toegang heeft.

Raad van State

De Raad verkiest kortere termijnen die verlengbaar zijn, maar een dergelijke regel kan niet veralgemeend worden, dus worden precieze termijnen opgelegd.

Drie categorieën

Deze categorieën — waarvoor de bewaarplicht 12 maanden bedraagt — werden na lange raadplegingen vastgelegd. Ze slaan op de identificerings- en lokalisatiegegevens alsook op hun raadpleegbaarheid naargelang van de zwaarte van het misdrijf.

Artikelen 122 & 123

Deze gegevens — voor commerciële doeleinden en marketing — kunnen slechts bewaard worden voor zover hun bewaring noodzakelijk is. Dit kan niet in een precies aantal maanden worden uitgedrukt.

Ombudsdienst

Deze dienst moet soms telefonisch stalkinggedrag of abnormale oproepen over een langere periode kunnen onderzoeken die echter niet langer dan 12 maanden kan bedragen.

Lokalisatie cloud

De server van een cloud moet lokaliseerbaar in Europa zijn. Het BIPT controleert dit.

Lijst misdrijven

Hiervoor wordt naar het Wetboek van strafvordering verwezen, waar wordt gedifferentieerd naargelang van de zwaarte van het misdrijf.

Protocol Privacycommissie/BIPT

De wet voorziet in de noodzaak een samenwerkingsprotocol af te sluiten.

Chatdiensten

De Europese privacyrichtlijn is dermate ruim dat deze diensten er mogelijk onder vallen. Indien een

Collecte/accès

Les articles du projet de loi à l'examen portent uniquement sur "qui doit conserver quoi et combien de temps?" et pas sur "qui a accès à quelles données?".

Conseil d'État

Le Conseil d'État opte pour des périodes plus courtes qui peuvent être prolongées, mais une telle règle ne peut pas être généralisée, le texte fixe donc des délais précis.

Trois catégories

Ces catégories — pour lesquelles l'obligation de conservation est de 12 mois — ont été déterminées au terme de longues consultations. Elles concernent les données d'identification et de localisation ainsi que leur consultabilité en fonction de la gravité de l'infraction.

Articles 122 & 123

Ces données — à des fins commerciales et de marketing — ne peuvent être conservées qu'aussi longtemps que leur conservation est nécessaire. Il n'est pas possible de déterminer cette durée en un nombre de mois précis.

Service de médiation

Ce service doit parfois pouvoir enquêter sur des cas de harcèlement téléphonique ou des appels anormaux sur une période plus longue mais qui ne peut toutefois pas dépasser 12 mois.

Localisation *Cloud*

Le serveur d'un *Cloud* doit être localisable en Europe. L'IBPT en assure le contrôle.

Liste des infractions

À cet effet, il est renvoyé au Code d'instruction criminelle, une différenciation étant faite selon la gravité de l'infraction.

Protocole commission de la protection de la vie privée/IBPT

La loi prévoit la nécessité de conclure un protocole de collaboration.

Services de chat

La directive européenne relative à la protection de la vie privée est tellement étendue que ces services

regeling zich al opdringt, moet ze op Europees vlak tot stand komen.

Universele verdenking

Hier is absoluut geen sprake van massabewaking waarbij eenieder verdacht zou zijn. Het betreft integendeel uiterst gericht onderzoek.

Controle

Het BIPT en de onderzoeksrechters zullen waken over de correcte toepassing van de wet.

Evaluatie

Iedere noodzakelijke wijziging van de wet zal blijken na de evaluatie die binnen twee jaar moet worden gemaakt.

Kostprijs

De gegevens worden door de operatoren sowieso bewaard. De wet legt hen een termijn op alsook de verplichting de gegevens na die termijn te vernietigen, tenzij ze voor commerciële doeleinden en marketing noodzakelijk zijn. In dat geval kunnen alleen de identificeringsgegevens worden bewaard.

C. Replieken

De heer Benoit Hellings (Ecolo-Groen) betreurt dat geen debat mogelijk is met de minister van Justitie waar de minister nochtans vaak naar verwijst. De gegevens voor commerciële doeleinden en marketing mogen de wettelijke bewaartijden van artikel 126 overschrijden omdat ze worden bewaard krachtens de artikelen 122 en 123, maar het past ook hier de duurtijd exact vast te leggen en niet in het ongewisse te laten. De voorwaarde dat hun bewaring “noodzakelijk” moet zijn, is veel te vaag en kan tot misbruiken leiden. Hierin moet zowel het advies van de Privacycommissie als het standpunt van de staatssecretaris voor Privacy worden gevolgd: “Zo weinig mogelijk gegevens mogen toegankelijk zijn voor zo weinig mogelijk personen.” Voorliggend wetsontwerp voldoet alleen aan de laatste voorwaarde, niet aan de eerste. Ook mag niet uit het oog worden verloren dat de gedurende twaalf maanden bewaarde gegevens gehackt kunnen worden en dus in handen kunnen geraken van malafide personen en instellingen. De kostprijs van de bewaarverplichting kan niet beperkt zijn als men weet dat de operator er een aangestelde moet voor vrijmaken. Heeft het BIPT wel de nodige middelen — in aantallen

relèvent peut-être de son champ d’application. Si une réglementation devait s’imposer, elle devrait être élaborée au niveau européen.

Suspicion universelle

Il n’est absolument pas question d’une surveillance de masse qui supposerait que chacun est suspect. Il s’agit au contraire d’une investigation extrêmement ciblée.

Contrôle

L’IBPT et les juges d’instruction veilleront à l’application correcte de la loi.

Évaluation

La nécessité de modifier la loi apparaîtra à la lumière de l’évaluation qui doit avoir lieu dans deux ans.

Coût

Les données sont de toute façon conservées par les opérateurs. La loi leur impose un délai ainsi que l’obligation de détruire les données au terme de ce délai, sauf si elles sont nécessaires à des fins commerciales ou de marketing. Dans ce cas, seules les données d’identification peuvent être conservées.

C. Répliques

M. Benoit Hellings (Ecolo-Groen) déplore qu’aucun débat ne soit possible avec le ministre de la Justice, auquel le ministre fait pourtant régulièrement référence. Le délai de conservation des données à des fins commerciales et de *marketing* peut excéder les délais légaux prévus par l’article 126, car ces données sont conservées en vertu des articles 122 et 123. Il s’indique toutefois également de fixer un délai de conservation précis en la matière. La condition selon laquelle la conservation de ces données doit être “nécessaire” est bien trop vague et susceptible d’entraîner des abus. Il convient à cet égard de suivre à la fois l’avis de la Commission de la protection de la vie privée et la position du secrétaire d’État à la Protection de la vie privée, qui considèrent qu’un nombre de données aussi limité que possible doivent être accessibles à un nombre de personnes aussi limité que possible. Le projet de loi à l’examen remplit uniquement la seconde condition, et non la première. Il ne faut pas non plus perdre de vue que les données conservées durant douze mois risquent d’être piratées et donc de tomber entre les mains de personnes et d’institutions malintentionnées. Le coût

extra personeelsleden — om deze nieuwe opdracht uit te voeren? De minister beweert dat het voorliggend ontwerp hoogdringend is omwille van de rechtszekerheid die na een aantal vernietigingen hersteld moet worden. Is dan geen nieuwe Europese richtlijn in voorbereiding? Schiet het ontwerp niet zijn doel voorbij als men weet dat gehaaide criminelen en terroristen communiceren via Viber, Thor en Telegramm, die niet onder het toepassingsveld van de reparatiewet zullen vallen. Ook geëncrypteerde berichten vallen er niet onder. Tot slot: wat is de reële impact van gegevens van meer dan zes maanden op het percentage misdrijven dat dankzij deze gegevens wordt opgehelderd?

De heer Peter Dedecker (N-VA) wenst te weten wie als operator wordt beschouwd want voor het BIPT is iedere gemeente die wifi aanbiedt, een operator. Zullen deze gemeentes ook onder het toepassingsveld van de wet vallen?

Mevrouw Fabienne Winckel (PS) herinnert eraan dat België weliswaar Duitsland niet is maar wel geconfronteerd wordt met dezelfde risico's. Een gemeenschappelijke vergadering met de commissie voor de Justitie en een hoorzitting met de staatssecretaris voor Privacy had op dit vlak voor meer duidelijkheid gezorgd. De evaluatie die binnen twee jaar zal plaatshebben is onvoldoende.

D. Bijkomende antwoorden van de minister

Regeling buurlanden

De Duitse Bondsdag heeft korte raadpleegtermijnen wettelijk verankerd maar is een uitzondering. In Frankrijk, Nederland en Denemarken is de raadpleegtermijn conform aan het Europees gemiddelde, hetzij twaalf maanden.

Middelen BIPT

Het BIPT heeft thans reeds de middelen om controle uit te oefenen want het voert thans reeds controles uit.

Kostprijs

De kostprijs voor het bewaren van de gegevens is vrij beperkt. Bovendien is de toegang betalend. De consument betaalt een marginaal bedrag. Ten slotte betaalt de

de l'obligation de conservation n'est pas limité, car l'opérateur est contraint de désigner un préposé pour assumer cette tâche. L'IBPT dispose-t-il des moyens nécessaires — en termes de personnel supplémentaire — pour s'acquitter de cette nouvelle mission? Le ministre invoque l'urgence du projet de loi à l'examen, en excitant de la nécessité de rétablir la sécurité juridique, qui a été mise à mal après une série d'annulations. L'intervenant demande si l'Union européenne n'est pas en train de préparer une nouvelle directive européenne en la matière. Le projet de loi à l'examen ne manque-t-il pas son objectif lorsqu'on sait que les criminels et terroristes aguerris communiquent par le biais de *Viber*, *Thor* et *Telegramm*, qui ne seront pas inclus dans le champ d'application de la loi de réparation? Les messages cryptés ne relèvent pas non plus du champ d'application de cette loi. L'intervenant conclut son intervention en demandant quel est l'impact réel des données remontant à plus de six mois sur le pourcentage d'infractions élucidées grâce à ce type de données.

M. Peter Dedecker (N-VA) demande qui est considéré comme opérateur, car pour l'IBPT, chaque commune qui offre le wifi est un opérateur. Ces communes relèveront-elles également du champ d'application de la loi?

Mme Fabienne Winckel (PS) rappelle que la Belgique n'est certes pas l'Allemagne, mais qu'elle n'en est pas moins exposée aux mêmes risques. Une réunion commune avec la commission de la Justice et une audition du secrétaire d'État en charge de la Protection de la vie privée aurait permis de clarifier la situation. L'évaluation qui aura lieu dans les deux ans est insuffisante.

D. Réponses supplémentaires du ministre

Réglementation dans les pays voisins

Le *Bundestag* a ancré dans la loi des délais de consultation courts, mais il fait figure d'exception à cet égard. En France, aux Pays-Bas et au Danemark, le délai de consultation est conforme à la moyenne européenne, soit douze mois.

Moyens de l'IBPT

L'IBPT dispose d'ores et déjà de moyens nécessaires pour exercer un contrôle, et il les met à profit.

Coût

Le coût de la conservation des données est relativement limité. En outre, l'accès est payant. Le consommateur paie un montant marginal. En somme, la société

gemeenschap ook voor de politie, zelfs indien er geen beroep op wordt gedaan.

Universele verdenking

Het vermoeden van onschuld verhindert niet dat burgers gecontroleerd worden op hun identiteit of op hun verplaatsingen. ANPR-camera's lezen thans de nummerplaten van alle voorbijrijdende auto's.

Europese richtlijn

Er is geen nieuwe Europese richtlijn over dit onderwerp in zicht.

Wifi gemeentes

De aanbieders van publieke wifi — zoals gemeentes — worden niet als operatoren beschouwd en dienen zich dus ook niet te houden aan enige bewaarverplichting.

IV. — ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN

Art. 1 tot 3

Deze artikelen worden achtereenvolgens zonder verdere bespreking eenparig aangenomen.

Art. 4

Amendement nr. 1

De heer Benoît Hellings (Ecolo-Groen) c.s. dient amendement nr. 1 (DOC 54 1567/4) in teneinde de toegang tot gegevens door de Ombudsdienst te beperken tot zes maanden. Anders heeft de Ombudsdienst de facto een ruimere bevoegdheid dan de politiediensten.

De minister stelt dat alleen de identificeringsgegevens toegankelijk zijn voor de Ombudsdienst en de praktijk wil dat abnormale oproepen over een langere periode onderzocht moeten kunnen worden.

Amendement nr. 2

De heer Benoît Hellings (Ecolo-Groen) c.s. dient amendement nr. 2 (DOC 54 1567/4) in teneinde operatoren te verplichte er één enkele gegevensbank op na te houden waarin zowel de metagegevens voor commerciële doeleinden en marketing als die voor onderzoek door de wettelijk toegelaten instanties zouden worden ondergebracht. Anders beschikken operatoren eigenlijk

finance aussi les services de police, même lorsqu'elle ne doit pas y faire appel.

Suspicion universelle

La présomption d'innocence n'empêche pas de contrôler l'identité ou les déplacements de citoyens. Les caméras ANPR lisent actuellement les numéros de plaque de toutes les automobiles qui passent.

Directive européenne

Aucune nouvelle directive européenne n'est prévue dans ce domaine.

Wifi des communes

Les fournisseurs de wifi public – comme les communes – ne sont pas considérés comme des opérateurs et ne sont donc soumis à aucune obligation de conservation.

IV. — DISCUSSION DES ARTICLES ET VOTES

Articles 1-3

Ces articles ne donnent lieu à aucune observation et sont successivement adoptés à l'unanimité.

Article 4

Amendement n° 1

M. Benoît Hellings (Ecolo-Groen) et consorts présentent un amendement (n° 1 – Doc 54 1567/4), qui tend à limiter à six mois l'accès du Service de médiation aux données, sans quoi celui-ci dispose de facto d'une compétence plus large que les services de police.

Le ministre indique que seules les données d'identification sont accessibles au Service de médiation, et la pratique veut que les appels anormaux puissent être examinés pendant une période plus longue.

Amendement n° 2

M. Benoît Hellings (Ecolo-Groen) et consorts présentent un amendement (n° 2 – 54 1567/4), qui tend à obliger les opérateurs à ne tenir qu'une seule banque de données rassemblant tant les métadonnées à des fins commerciales et de marketing que les données qui doivent être examinées par les instances habilitées par la loi, sans quoi les opérateurs disposent en fait d'une

over een kopie, die niet na maximaal twaalf maanden vernietigd moet worden.

De minister stelt dat de Raad van State geen standpunt inneemt. Het BIPT heeft deze werkhypothese — dat het bestaan van twee verschillende gegevensbanken de correcte toepassing van de wet zou ondergraven — geanalyseerd. Het heeft geconcludeerd dat de twee gegevensbanken absoluut niet identiek zijn en dus van geen significante invloed op de toepassing van de wet.

Amendement nr. 3

De heer Benoît Hellings (Ecolo-Groen) c.s. dient amendement nr. 3 (DOC 54 1567/4) in teneinde het BIPT de bevoegdheid te geven te controleren dat alle gegevens in welke gegevensbank ook na 12 maanden worden vernietigd om enig misbruik te voorkomen.

De minister onderstreept dat de operator ze slechts mag bewaren als het nodig is, maar over die noodzaak zelf beslist.

Amendement nr. 4

Mevrouw Sabien Lahaye-Battheu (Open Vld) c.s. dient amendement nr. 4 in (DOC 54 1567/4) teneinde een correctie door te voeren ingevolge de goedkeuring van de Potpourri II (wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten).

De minister stemt in met deze correctie.

De amendementen nrs. 1, 2 en 3 worden achtereenvolgens verworpen met 10 stemmen tegen 1 en 1 onthouding.

Amendement nr. 4 wordt aangenomen met 11 stemmen en 1 onthouding.

Het aldus gewijzigde artikel wordt aangenomen met 10 tegen 2 stemmen.

Art. 5

De heer Benoît Hellings (Ecolo-Groen) stelt dat de coördinatiecel bij iedere operator toegang zal hebben tot alle gegevens, zowel die bewaard krachtens artikelen 122 en 123 als die welke bewaard worden krachtens artikel 126. Hoe kan de toegang dan ontzegd worden tot personen en instanties die daartoe niet wettelijk zijn gemachtigd? Ook wordt wel gesteld dat de metagegevens weliswaar geen inhoudelijke elementen mogen

copie, qui ne doit pas être détruite après un délai maximum de douze mois.

Le ministre note que le Conseil d'État ne prend pas position. L'IBPT a analysé cette hypothèse de travail — selon laquelle l'existence de deux banques de données hypothéquerait l'application correcte de la loi. Il a conclu que les deux banques de données n'étaient absolument pas identiques et qu'elles n'avaient par conséquent pas d'influence significative sur l'application de la loi.

Amendement n° 3

M. Benoît Hellings (Ecolo-Groen) et consorts présentent un amendement (n° 3 – Doc 54 1567/4), qui tend à habiliter l'IBPT à vérifier que toutes les données, quelle que soit la banque de données, sont détruites après 12 mois, pour éviter tout abus.

Le ministre souligne que l'opérateur ne peut conserver les données que si c'est nécessaire, mais qu'il décide lui-même de cette nécessité.

Amendement n° 4

Mme Sabien-Lahaye-Battheu (Open Vld) et consorts présentent un amendement (n° 4 – Doc 54 1567/4), qui tend à apporter une correction à la suite de l'adoption de la loi pot-pourri II (modification de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité).

Le ministre souscrit à cette correction.

Les amendements n°s 1, 2 et 3 sont successivement rejetés par 10 voix contre une et une abstention.

L'amendement n° 4 est adopté par 11 voix et une abstention.

L'article, ainsi modifié, est adopté par 10 voix contre 2.

Article 5

M. Benoît Hellings (Ecolo-Groen) précise que la cellule de coordination aura accès, chez chaque opérateur, à toutes les données, tant celles qui sont conservées en vertu des articles 122 et 123 que celles qui le sont en vertu de l'article 126. Comment peut-on alors refuser l'accès aux personnes et aux instances qui n'y sont pas habilitées par la loi? Il est également précisé que les métadonnées ne peuvent comporter aucun élément de

bevatten, maar aangezien naar artikel 90ter van het Wetboek van strafvordering wordt verwezen zou dit in combinatie kunnen gebeuren met af luisteren en dus toch slaan op de inhoud. Welke sociale bescherming geniet een aangestelde die zijn directie wijst op een inbreuk van de wet? Tot wie moet een dergelijk persoon zich richten wanneer hij constateert dat zijn eigen werkgever de wet schendt?

De minister antwoordt dat de verwijzing naar artikel 90ter van het Wetboek van strafvordering alleen bedoeld is om de termijnen te bepalen die naargelang van de zwaarte van het misdrijf van kracht zullen zijn. Naar de aard van de gegevens wordt absoluut niet verwezen, alleen naar de termijnen. Justitie kan altijd alle gegevens raadplegen. Voorts zal de arbeidsrechtbank beslissen welke sanctie moet worden opgelegd aan een werkgever die de wet niet loyaal uitvoert en daar door zijn aangestelde op gewezen is. Deze aangestelde kan zich, indien hij van zijn eigen hiërarchie geen respons krijgt, in eerste instantie richten tot het BIPT.

Dit artikel wordt ongewijzigd aangenomen met 10 stemmen tegen 1 en 1 onthouding.

Art. 6

Dit artikel wordt zonder verdere bespreking aangenomen met 10 stemmen tegen 1 en 1 onthouding.

Art. 7

Dit artikel wordt zonder verdere bespreking aangenomen met 11 stemmen tegen 1.

V. — VERZOEK TOT TWEEDE LEZING

De heer Benoît Hellings (Ecolo-Groen) vraagt toepassing van artikel 83 van het kamerreglement, dat in zijn eerste lid stelt: “Na de stemming over de artikelen van een wetsontwerp (...) gaat de commissie, op voorstel van een commissielid (...) over tot een tweede lezing.”

De rapporteur,

Peter DEDECKER

De voorzitter,

Karine LALIEUX

contenu, mais dès lors qu’il est renvoyé à l’article 90ter du Code d’instruction criminelle, leur consultation pourrait être combinée à des écoutes téléphoniques et donc bien porter sur le contenu. De quelle protection sociale bénéficie un préposé qui signale à son employeur une infraction à la loi? À qui cette personne doit-elle s’adresser si elle constate que son propre employeur enfreint la loi?

Le *ministre* répond que le renvoi à l’article 90ter du Code d’instruction criminelle vise uniquement à fixer les délais qui seront en vigueur en fonction de la gravité de l’infraction. On ne renvoie absolument pas à la nature des données, uniquement aux délais. La Justice peut toujours consulter l’intégralité des données. En outre, le tribunal du travail décidera quelle sanction devra être infligée à un employeur qui n’applique pas loyalement la loi et dont l’attention a été attirée sur ce point pas son préposé. Ce dernier peut s’adresser en premier lieu à l’IBPT s’il n’obtient pas de réponse de la part de sa propre hiérarchie.

Cet article est adopté sans modification par 10 voix contre une et une abstention.

Article 6

Cet article ne donne lieu à aucune observation et est adopté par 10 voix contre une et une abstention.

Article 7

Cet article ne donne lieu à aucune observation et est adopté par 11 voix contre une.

V. — DEMANDE DE DEUXIÈME LECTURE

M. Benoît Hellings (Ecolo-Groen) demande l’application de l’article 83 du Règlement de la Chambre, dont l’alinéa 1^{er} prévoit que: “Après le vote sur les articles d’un projet (...) de loi, la commission procède à une deuxième lecture si un de ses membres le demande(...).”

Le rapporteur,

Peter DEDECKER

La présidente,

Karine LALIEUX