

# SÉNAT DE BELGIQUE

SESSION DE 2012-2013

18 JUILLET 2013

**Projet de loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du code d'instruction criminelle**

*Procédure d'évocation*

## RAPPORT

FAIT AU NOM DE LA COMMISSION  
DES FINANCES ET DES AFFAIRES  
ÉCONOMIQUES  
PAR  
**MME TALHAOUI ET**  
**M. MILLER**

# BELGISCHE SENAAT

ZITTING 2012-2013

18 JULI 2013

**Wetsontwerp houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering**

*Evocatieprocedure*

## VERSLAG

NAMENS DE COMMISSIE VOOR  
DE FINANCIËN EN VOOR  
DE ECONOMISCHE AANGELEGENHEDEN  
UITGEBRACHT DOOR  
**MEVROUW TALHAOUI EN**  
**DE HEER MILLER**

Composition de la commission / Samenstelling van de commissie :

**Président/Voorzitter :** Ludo Sannen.

**Membres/Leden :**

N-VA Frank Boogaerts, Patrick De Groote, Lieve Maes,  
Sabine Vermeulen.  
PS Marie Arena, Ahmed Laaouej, Louis Siquet.  
MR François Bellot, Richard Miller.  
CD&V Wouter Beke, Etienne Schouppe.  
sp.a Ludo Sannen, Fauzaya Talhaoui.  
Open Vld Rik Daems.  
Vlaams Belang Anke Van dermeersch.  
Écolo Jacky Morael.  
cdH Bertin Mampaka Mankamba.

**Suppléants/Plaatsvervangers :**

Bart De Nijn, Inge Faes, Lies Jans, Helga Stevens,  
Karl Vanlouwe.  
Paul Magnette, Philippe Mahoux, Fabienne Winckel, Olga Zrihen.  
Christine Defraigne, Gérard Deprez, Dominique Tilmans.  
Dirk Claes, Cindy Franssen, Johan Verstreken.  
Dalila Douffi, Fatma Pehlivian, Guy Swennen.  
Jean-Jacques De Gucht, Yoeri Vastersavendts.  
Yves Buysse, Filip Dewinter.  
Benoit Hellings, Cécile Thibaut.  
Francis Delpérée, Vanessa Matz.

*Voir:*

Documents du Sénat :

5-2222 - 2012/2013 :

N° 1 : Projet évoqué par le Sénat.

N° 2 : Amendements.

*Zie:*

Stukken van de Senaat :

5-2222 - 2012/2013

Nr. 1 : Ontwerp geëvoeerd door de Senaat.

Nr. 2 : Amendementen.

## I. INTRODUCTION

Le projet de loi qui fait l'objet du présent rapport et qui relève de la procédure bicamérale facultative a été déposé initialement à la Chambre des représentants le 27 juin 2013 (doc. Chambre, n° 51-2921/1).

Il a été adopté par la Chambre des représentants et transmis au Sénat qui l'a évoqué.

Il a été examiné en commission des Finances et des Affaires économiques le 18 juillet 2013.

## II. EXPOSÉ INTRODUCTIF DU SECRÉTAIRE D'ÉTAT A LA LUTTE CONTRE LA FRAUDE

Le secrétaire d'État renvoie à l'exposé des motifs du projet de loi (voir doc. Chambre, n° 53-2921/1, pp. 3 - 23).

Il tient par ailleurs à apporter encore quelques précisions :

- le projet de loi ne porte nullement sur la conservation du contenu des communications électroniques : il vise uniquement les données que les opérateurs conservent déjà actuellement;

- le délai de conservation de douze mois, tel que prévu dans le projet de loi, est conforme à celui qui existe déjà actuellement;

- l'obligation relative à la conservation de données en vue de la détection et de la répression d'infractions pénales n'est pas neuve non plus puisqu'elle figure déjà à l'article 126 de la loi relative aux communications électroniques et qu'elle fait déjà l'objet d'accords entre la justice et les opérateurs. Le projet de loi fixe des règles pour clarifier et mieux encadrer cette obligation;

- les appels malveillants vers les services d'urgence seront réprimés, mais c'est un point qui n'est pas neuf non plus;

- la loi fera l'objet d'un rapport d'évaluation qui sera transmis au Parlement.

## I. INLEIDING

Dit optioneel bicameraal wetsontwerp werd in de Kamer van volksvertegenwoordigers ingediend als een wetsontwerp op 27 juni 2013 (stuk Kamer, nr. 53-2921/1).

Het werd aangenomen door de Kamer van volksvertegenwoordigers en overgezonden aan de Senaat en door de Senaat geëvoceerd.

De commissie voor de Financiën en de Economische Aangelegenheden heeft het wetsontwerp besproken op 18 juli 2013.

## II. INLEIDENDE UITEENZETTING DOOR DE STAATSSECRETARIS VOOR FRAUDEBESTRIJDING

De staatssecretaris verwijst naar de memorie van toelichting bij het wetsontwerp. (zie stuk Kamer, nr. 53 2921/1, blz.3-23)

Voorts verduidelijkt hij nog de volgende punten :

- het wetsontwerp heeft op geen enkele wijze betrekking op het bewaren van de inhoud van de electronische communicatie : het betreft enkel de data die reeds op vandaag bijgehouden worden door de operatoren;

- de termijn van bewaring van twaalf maanden die wordt voorzien, is een bestendiging van de bestaande situatie;

- ook vandaag bestaat reeds de verplichting data te bewaren met het oog op het opsporen en beteugelen van strafbare feiten : zie huidig artikel 126 van de Telecomwet : er bestaan hierover reeds afspraken tussen justitie en de operatoren : de context waarin dit gebeurt, wordt met het wetsontwerp duidelijk omkaderd en verduidelijkt;

- er wordt een beteugeling voorzien van kwaadwillige oproepen naar nooddiensten, maar ook dat is niet volledig nieuw;

- er zal een evaluatieverslag van de wet aan het Parlement worden overgemaakt.

### **III. DISCUSSION**

#### **1. Discussion générale**

##### *Questions et observations des membres*

Mme Maes trouve que le projet de loi à l'examen accorde au Roi des pouvoirs très étendus, par exemple en ce qui concerne les définitions des données d'identification des utilisateurs finaux, les services de communication utilisés, les équipements terminaux utilisés, les données de trafic, etc. Il est dommage que l'élargissement du champ d'application ne soit pas soumis au Parlement pour approbation. C'est très regrettable.

En ce qui concerne l'article 5 du projet, l'intervenant fait remarquer que l'on donne au Roi la possibilité d'imposer un délai de conservation supérieur à vingt-quatre mois, alors qu'à d'autres endroits du projet, il est chaque fois question d'un délai de douze mois. Pourquoi un délai plus long est-il nécessaire ?

Sur le plan des principes, M. Hellings souscrit à la finalité officielle du projet visant à lutter contre la criminalité grave dans une société démocratique.

Cependant, le législateur ne peut gommer le contexte inquiétant dans lequel il s'insère. Sur tous les fronts, on assiste à une remise en cause du respect des droits fondamentaux à la vie privée, à la protection des données, à la confidentialité des communications, à la présomption d'innocence, à la liberté d'expression et à la liberté d'information. Au niveau international, on pense à PRISM mais aussi aux accords PNR adoptés malgré les mises en gardes de nombreuses institutions autorisées.

Le législateur doit entendre la voix de personnes et institutions autorisées.

Le Contrôleur européen de protection de la vie privée, à l'occasion de son évaluation de la directive, réalisée en 2011, confirme que la directive ne répond pas aux exigences fixées par le droit fondamental à la protection de la vie privée :

- absence de démonstration de la nécessité de conserver les données,

- possibilité de réglementer de manière moins intrusive,

- trop large marge de manœuvre laissée aux États membres en regard des finalités, des personnes pouvant accéder aux données et à quelles conditions.

### **III. BESPREKING**

#### **1. Algemene besprekking**

##### *Vragen en opmerkingen van de leden*

Mevrouw Maes is van oordeel dat voorliggend wetsontwerp zeer ruime bevoegdheden aan de Koning toekent, zoals bijvoorbeeld het bepalen van de definities van de gegevens ter identificatie van de eindgebruikers, de gebruikte communicatiediensten, de gebruikte eindapparatuur, verkeersgegevens en dergelijkem. Het is jammer dat de uitbreiding van het toepassingsgebied niet door het parlement wordt goedgekeurd. Dit is erg betreurenswaardig.

Wat artikel 5 van het ontwerp betreft, merkt spreekster op dat aan de Koning wordt overgelaten een bewaringstermijn op te leggen die langer is dan vierentwintig maand, terwijl elders in het ontwerp telkenmale sprake is van twaalf maanden. Waarom is deze langere termijn nodig ?

In principe verklaart de heer Hellings het eens te zijn met de officiële doelstelling van het ontwerp, met name de bestrijding van zware criminaliteit in een democratische samenleving.

De wetgever mag echter niet blind zijn voor de verontrustende context waarin dit plaatsgrijpt. Op alle fronten komen fundamentele rechten inzake privé-levenssfeer, databescherming, vertrouwelijkheid van communicatie, vermoeden van onschuld, vrijheid van meningsuiting en van informatie op losse schroeven te staan. Op internationaal vlak denkt men aan PRISM, maar ook aan de PNR-overeenkomsten die ondanks waarschuwingen van vele bevoegde instellingen werden goedgekeurd.

De wetgever moet luisteren naar de stem van bevoegde personen en instellingen.

De Europees Toezichthouder voor gegevensbescherming heeft in zijn evaluatie van de richtlijn in 2011 bevestigd dat de richtlijn niet beantwoordt aan de vereisten van het fundamenteel recht op bescherming van de privé-levenssfeer :

- de noodzaak om gegevens te bewaren is niet aangetoond,

- een minder intrusieve reglementering is Mogelijk,

- de lidstaten krijgen te veel speelruimte op het vlak van de doelstellingen, de personen die toegang kunnen krijgen tot de gegevens en de voorwaarden hiervoor.

Les cours constitutionnelles allemande (1), roumaine, bulgare et tchèque ont estimé que la rétention générale de données est inconstitutionnelle (2). À la suite de cela, la Commissaire Reding annonça vouloir s'assurer que le stockage de données soit compatible avec la Charte européenne des droits fondamentaux.

Pourquoi le ministre n'a-t-il pas pris la peine de consulter la Cour constitutionnelle belge ?

Y a-t-il eu une réponse à la question préjudiciale posée à la Cour de justice de l'UE par la Cour suprême irlandaise ?

Vu les enjeux en présence, le législateur ne peut se contenter de l'urgence décrétée par le ministre : on comprend le souci d'éviter l'amende de l'Union européenne, mais l'avis de la Commission pour la protection de la vie privée date du 2 juillet 2008. Pourquoi invoquer l'urgence maintenant ? Pourquoi soumettre ce projet à la commission de l'Infrastructure, en refusant l'avis de la commission de la Justice de la Chambre, puis filer vers la commission des Finances et des Affaires économiques lors du transfert du projet au Sénat ? En 2009, c'était le ministre de la Justice qui travaillait à ce projet de loi et il est proposé également par la ministre de la Justice aujourd'hui.

Quels sont les résultats de la consultation publique de 2008 ? Il serait utile de procéder à des auditions, notamment de la Ligue des droits de l'homme, Avocats.be, l'AJP et l'*Orde van Vlaamse Balies*, ainsi que de fournisseurs (ISPA).

Sur le fond, plusieurs remarques s'imposent.

— La collecte systématique, permettant l'accumulation massive de données permet le « *datamining* », soit la possibilité de pouvoir, grâce à un logiciel, prédire des comportements et déterminer des « profils criminels ». C'est d'autant plus grave lorsqu'on peut croiser plusieurs bases de données.

D'un système de collecte de données où l'on vérifie au cas par cas les soupçons que les services de sécurité

(1) Article 4/3/2010 Jean Lasar: Arrêt de la Cour constitutionnelle allemande : Les juges de Karlsruhe ont estimé abusif et incompatible avec la loi fondamentale le dispositif mis en place par le gouvernement fédéral obligeant les fournisseurs d'accès à Internet et les opérateurs téléphoniques, au nom de la lutte contre le terrorisme et la criminalité en ligne, à stocker systématiquement pendant six mois les données relatives aux appels téléphoniques et aux connexions Internet. Suite à cela, la Commissaire Redding annonçait vouloir s'assurer que le stockage de données soit compatible avec la Charte européenne des droits fondamentaux en vigueur depuis le mois de décembre 2010.

(2) Cf. CP 31 mai 2003 Ligue, avocats.be, AJP.

De grondwettelijke hoven van Duitsland (1), Roemenië, Bulgarije en Tsjechië hebben geoordeeld dat een algemene bewaring van gegevens ongrondwettelijk is (2). Als gevolg hiervan heeft Eurocommissaris Reding aangekondigd dat zij zich ervan wil vergewissen dat gegevensbewaring verenigbaar is met het Handvest van de grondrechten van de Europese Unie.

Waarom heeft de minister niet de moeite genomen het Belgisch Grondwettelijk Hof te raadplegen ?

Is er een antwoord gekomen op de prejudiciële vraag die het Ierse Hooggerechtshof heeft gesteld aan het Europees Hof van Justitie ?

Gelet op wat er op het spel staat, kan de wetgever geen genoegen nemen met de spoedbehandeling die de minister vraagt. Het is begrijpelijk dat men de Europese boete wil voorkomen, maar het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer dateert van 2 juli 2008. Waarom wordt de dringende noodzaak nu aangevoerd ? Waarom wordt het ontwerp aan de commissie voor de Infrastructuur voorgelegd, wordt het advies van de Kamercommissie voor Justitie geweigerd, en wordt het dan bij de overzending naar de Senaat aan de commissie voor de Financiën en de Economische Aangelegenheden voorgelegd ? In 2009 was het de minister van Justitie die aan dit ontwerp werkte, en ook nu wordt het door de minister van Justitie ingediend.

Welke zijn de resultaten van de openbare raadpleging van 2008 ? Het zou nuttig zijn hoorzittingen te houden, met name met de Liga voor de mensenrechten, de *Ordre des Barreaux francophone et germanophone*, de AJP, de Orde van Vlaamse Balies, en de providers (ISPA).

Wat de inhoud betreft, maakt spreker verschillende opmerkingen.

— Het systematisch verzamelen van een massale hoeveelheid gegevens maakt « *datamining* » mogelijk, met andere woorden het voorspellen van gedragingen door middel van een computerprogramma en het aanmaken van « *criminele profielen* ». Dit is nog erger wanneer men kan overgaan tot *datamatching*.

Van een systeem van gegevensvergaring waarmee men geval per geval verdenkingen van veiligheids-

(1) Artikel 4/3/2010 Jean Lasar : « *Arrêt de la Cour constitutionnelle allemande : Les juges de Karlsruhe ont estimé abusif et incompatible avec la loi fondamentale le dispositif mis en place par le gouvernement fédéral obligeant les fournisseurs d'accès à Internet et les opérateurs téléphoniques, au nom de la lutte contre le terrorisme et la criminalité en ligne, à stocker systématiquement pendant six mois les données relatives aux appels téléphoniques et aux connexions Internet. Suite à cela, la Commissaire Redding annonçait vouloir s'assurer que le stockage de données soit compatible avec la Charte européenne des droits fondamentaux en vigueur depuis le mois de décembre 2010.* »

(2) Cfr CP 31 mei 2003 Ligue, avocats.be, AJP.

peuvent avoir, on passe à un système où les données de tout le monde sont collectées, car parmi ce « tout le monde », il existe une série de coupables potentiels.

C'est une atteinte insupportable à la présomption d'innocence : les moyens utilisés sont totalement disproportionnés : ils impliquent la mise sous contrôle de la société dans son ensemble.

De plus, ce « *datamining* » est inefficace.

— Les données transférées ont un caractère extrêmement personnel, même sans contenu.

Une étude de l'UCL réalisée par M. Vincent Blondel (publiée par *Nature* en mars 2013) démontre qu'avec quatre données de localisation seulement, on peut déterminer l'identité de 95 % des individus (quinze mois d'étude, 1 500 000 clients de Belgacom testés), ceci sans autre données que celles-ci, croisées avec les autres données disponibles librement partout ailleurs.

— Le contenu pourra être conservé et utilisé : le contenu (1) n'est pas couvert par la directive (2). Mais le projet de loi prévoit, en son article 3, § 6 : « Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée. » Ceci ouvre la voie à des débordements.

— Chaque citoyen devra-t-il financer le coût de sa propre surveillance ?

Le projet entraînera un coût pour les opérateurs confrontés à l'obligation de conservation de données, or aucun système de compensation n'est prévu. Des indemnités de réquisitions sont certes prévues par l'arrêté royal du 9 janvier 2003 et l'arrêté royal du 12 octobre 2010, mais cela ne couvre pas la rétention et le stockage. L'intention du ministre est-elle que les opérateurs répercutent ces coûts sur le public ? Les individus paieraient donc eux-mêmes la mise en cause de leur vie privée. Les fournisseurs d'accès à l'internet ont-ils contribué à l'enquête publique ? Quelle est leur position à ce propos ? Il serait intéressant de les entendre lors d'une audition en commission.

Il semble (3) que cet archivage coûte à l'État français plus de 200 millions d'euros en remboursement des frais de conservation de ces données aux fournisseurs d'accès à l'Internet.

(1) Réponse du ministre de la Justice à une question orale en 2009 : Pour intercepter le contenu, il faut faire appel à l'article 90ter du Code d'instruction criminelle qui prévoit une protection particulière de la communication qui a trait au secret professionnel.

(2) Considérant 13 et article 1<sup>er</sup>, § 2, de la directive 2006/24.

(3) <http://www.netdeclick.net/blog/l-exploitation-des-donnees-privees-du-depute-vert-malte-spitz>.

diensten checkt, stapt men over naar een systeem waarmee de gegevens van iedereen worden verzameld, met het argument dat er onder die « iedereen » potentiële criminelen moeten zijn.

Dit is een onaanvaardbare schending van het vermoeden van onschuld. De gebruikte middelen zijn totaal disproportioneel : zij betekenen dat de hele maatschappij wordt gecontroleerd.

Bovendien is een dergelijke *datamining* inefficent.

— De overgedragen gegevens zijn van zeer persoonlijke aard, zelfs zonder inhoud.

Een studie van de UCL door de heer Vincent Blondel (in maart 2013 gepubliceerd in *Nature*) toont aan dat men met slechts vier plaatsgegevens de identiteit van 95 % van de mensen kan achterhalen (vijftien maanden onderzoek, 1 500 000 Belgacom-clanten getest) louter door deze gegevens te vergelijken met de andere gegevens die overal elders vrij verkrijgbaar zijn.

— De inhoud mag bewaard en gebruikt worden : de inhoud (1) wordt niet gedekt door de richtlijn (2). Het wetsontwerp bepaalt echter in artikel 3, § 6 : « Behoudens andersluidende wettelijke bepaling, mogen geen gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, bewaard worden. » Dat zet de deur open voor ontsporingen.

— Zal iedere burger de kosten van zijn eigen toezicht moeten financieren ?

Het ontwerp zal kosten met zich meebrengen voor de operatoren, die verplicht zullen worden gegevens te bewaren. Er is echter niets om dit te compenseren. Weliswaar voorzien de koninklijke besluiten van 9 januari 2003 en 12 oktober 2010 in een aantal vergoedingen, maar die betreffen niet de retentie en de opslag. Wil de minister dat de operatoren deze kosten op de klanten verhaalt ? Zij zouden dus zelf moeten betalen voor een inbreuk op hun privé-leven. Hebben de providers bijgedragen aan de openbare raadpleging ? Wat is hun standpunt hierover ? Het zou interessant zijn hen te horen tijdens een hoorzitting in de commissie.

De terugbetaling van de kosten voor de opslag van deze gegevens aan de *internetproviders* zou de Franse Staat bijvoorbeeld meer dan 200 miljoen euro kosten (3).

(1) Antwoord van de minister van Justitie op een mondelinge vraag in 2009 : « Om kennis te nemen van de inhoud, moet een beroep worden gedaan op artikel 90ter van het Wetboek van strafvordering dat voorziet in een bijzondere bescherming van de communicatie die onder het beroepsgeheim valt. »

(2) Considerans 13 en artikel 1, § 2, van richtlijn 2006/24.

(3) <http://www.netdeclick.net/blog/l-exploitation-des-donnees-privees-du-depute-vert-malte-spitz>.

— La finalité de la rétention de données n'est pas limitée aux infractions graves.

La Commission européenne constate elle-même que l'absence de définition de la notion d'infraction grave dans les deux instruments en présence pose problème (1).

Le Conseil d'État juge que les buts poursuivis dépassent largement les finalités prévues par la directive 2006/24/CE sur la rétention des données pour des finalités pénales (p. 33, § 2).

Dans les développements, le projet de loi semble confirmer que le service de médiation peut demander des données en dehors de toute procédure pénale mais ne les transmettra au plaignant qu'en cas de procédure pénale.

L'arrêté royal prévoit que cela peut se faire aussi pour la poursuite de crimes et délits de droit commun.

#### — L'efficacité de cette loi est-elle démontrée ?

Le ministre dispose-t-il de chiffres l'attestant ? En 2011, l'Agence fédérale allemande pour la criminalité a publié une étude de la police montrant une augmentation des infractions criminelles enregistrées par la police entre 2007 (15 790) et 2009 (16 814). L'utilisation de la conservation des données a permis de solutionner seulement 83,5 % des faits contre 84,4 % en 2007, sans l'aide de la rétention des données... Comment le ministre explique-t-il cette information ? (2)

Le rapport d'évaluation dressé en avril 2011 par la Commission européenne sur la directive 2006/24/CE, indique que 90 % des données demandées en Europe ont moins de six mois.

Les « hot spots » ne seraient pas couverts par la loi. Elle risque donc bien d'organiser un réseau de lieux facilement accessible pour les auteurs de délits qu'elle cherche à contenir !

— La nécessaire confidentialité des échanges de certains corps de métiers est compromise.

La rétention générale des données met gravement en péril la nécessaire confidentialité des échanges de certains corps de métiers (les médecins, les avocats et toute personne soumise au secret professionnel) et le secret des sources des journalistes. Sans la garantie de respect de la vie privée, de nombreuses personnes pourraient hésiter, faute de garantie sur la confiden-

(1) Avis du CE, p. 33, § 1<sup>er</sup>. Directive 2002/58/CE pour les systèmes de conservation de données en vue de sauvegarder la sécurité, et directive 2006/24/CE pour garantir la disponibilité de ces données.

(2) Cfr CP 31 mai 2003 Ligue, avocats.be, AJP.

— Gegevensopslag is niet alleen bedoeld voor ernstige misdrijven.

De Europese Commissie stelt zelf vast dat het ontbreken van een definitie van het begrip zwaar misdrijf in de twee richtlijnen een probleem vormt (1).

De Raad van State oordeelt dat de doelstellingen ruimschoots die van richtlijn 2006/24/EG betreffende de bewaring van gegevens overschrijden (blz. 33, § 2).

In de toelichting lijkt het wetsontwerp te bevestigen dat de Ombudsdiest, buiten iedere strafrechtelijke procedure om, gegevens kan opvragen, maar dat zij die aan de klager alleen in geval van een strafrechtelijke procedure zal bezorgen.

Het koninklijk besluit bepaalt dat dit ook kan om gemeenrechtelijke misdaden en wanbedrijven te vervolgen.

— Is de doeltreffendheid van deze wet aangetoond ?

Beschikt de minister over cijfers die de doeltreffendheid aantonen ? In 2011 heeft het Duitse federale agentschap voor de criminaliteit een politiestudie gepubliceerd die aantoont dat het aantal geregistreerde misdrijven tussen 2007 (15 790) en 2009 (16 814) gestegen is. Het gebruik van gegevensopslag heeft slechts 83,5 % van de feiten helpen oplossen, tegenover 84,4 % in 2007, zonder de hulp van gegevensopslag. Hoe verklaart de minister dit ? (2)

Het evaluatieverslag dat de Europese Commissie in april 2011 over richtlijn 2006/24/EG gemaakt heeft, toont aan dat 90 % van de in Europa opgevraagde gegevens minder dan zes maand oud zijn.

« Hot spots » zouden niet door de wet gedekt zijn. Zo dreigt de wet een net van makkelijk toegankelijke plaatsen te organiseren voor de daders van misdrijven die zij probeert te beteugelen !

— De noodzakelijke vertrouwelijkheid van communicatie bij sommige beroepen staat op de helling.

De algemene bewaring van gegevens brengt ernstige schade toe aan de noodzakelijke vertrouwelijkheid van gegevensuitwisseling bij sommige beroepen (artsen, advocaten, eenieder die onderworpen is aan het beroepsgeheim) en het bronnengeheim van journalisten. Zonder waarborg dat de privé-levenssfeer in acht wordt genomen, zouden vele personen bij gebrek

(1) Advies Raad van State, p. 33, § 1. Richtlijn 2002/58/EG voor de bewaring van gegevens om de veiligheid te waarborgen, en Richtlijn 2006/24/EG om de beschikbaarheid van deze gegevens te waarborgen.

(2) Cf. CP 31 mei 2003 Ligue, avocats.be, AJP.

tialité des échanges, à prendre contact avec un avocat ou avec la presse par exemple, pour régler ou soulever un problème. Et l'argument selon lequel le contenu n'est pas conservé ni utilisé ne tient pas; avec les données collectées, on peut se faire une idée assez claire du profil d'un individu et de ses relations. Comment la loi prévoit-elle explicitement d'exclure la transmission de données concernant les médecins, les avocats ou les journalistes.

Qu'en est-il des institutions politiques, des conseils de ministres, de l'OTAN, des services secrets eux-mêmes ?

En ce qui concerne la durée de conservation, M. Hellings rappelle que le Conseil d'État relève que la durée de conservation prévue dépasse le prescrit de la directive.

Le Parlement est contraint de valider un texte qui, comme l'exposé des motifs le propose, doit s'entendre en complémentarité avec un arrêté royal. Pour quelles raisons n'a-t-il pas été rendu public ?

La Commission pour la protection de la vie privée a émis deux avis, dont seul le premier a été communiqué au Parlement, mais le ministre annonce avoir tenu compte de toutes les remarques. Quelles sont les remarques qui figuraient dans le second avis ?

Le ministre répond qu'il n'a pas choisi d'établir deux législations distinctes, comme suggéré par le Conseil d'État (pour la mise en œuvre de la directive 2002/58/CE pour les systèmes de conservation de données en vue de sauvegarder la sécurité, et la directive 2006/24/CE pour garantir la disponibilité de ces données) afin de faciliter la vie des fournisseurs d'accès. Quels sont les articles de ces directives qui doivent encore être transposés ?

Enfin, le ministre affirme avoir suivi l'avis du Conseil d'État — demandé en urgence. En réalité, il ne suit que le détail (tableau de correspondance), et ne tient pas compte des commentaires relatifs à la législation parallèle, à l'exigence de fixer dans la loi les modalités de demande et de transmission, au dépassement de délais dans certaines hypothèses ou à l'obligation de préciser clairement qui a accès aux données.

Le texte de l'article 5 du projet de loi est muet sur l'autorité et sur les modalités précises selon lesquelles les données seront demandées et transmises. S'agissant d'un régime de nature à porter atteinte au droit fondamental à la vie privée, il convient que le législateur fixe lui-même les éléments essentiels du régime de ces transmissions.

aan garanties inzake vertrouwelijkheid van de communicatie kunnen aarzelen contact op te nemen met bijvoorbeeld een advocaat of de pers om een probleem aan te kaarten of op te lossen. Het argument dat de inhoud niet wordt bewaard noch gebruikt, houdt geen stek: met de vergaarde gegevens kan men een vrij duidelijk beeld krijgen van iemands profiel en zijn contacten. Hoe zorgt de wet ervoor dat gegevens van artsen, advocaten of journalisten uitdrukkelijk niet worden vrijgegeven ?

Wat met politieke instellingen, de Ministerraad, de NAVO, de geheime diensten zelf ?

In verband met de bewaringstermijn, herinnert de heer Hellings eraan dat de Raad van State erop wijst dat de bewaringstermijn langer is dan wat de richtlijn voorschrijft.

Het Parlement is verplicht een tekst goed te keuren die, zoals de toelichting aangeeft, samen met een koninklijk besluit gelezen moet worden. Waarom werd dat besluit niet openbaar gemaakt ?

De Commissie voor de bescherming van de persoonlijke levenssfeer heeft twee adviezen uitgebracht, waarvan alleen het eerste aan het Parlement werd meegedeeld, maar de minister beweert dat hij rekening heeft gehouden met alle opmerkingen. Welke opmerkingen stonden in het tweede advies ?

De minister heeft geantwoord dat hij er niet voor gekozen heeft om twee verschillende wetgevingen op te stellen, zoals de Raad van State had voorgesteld (voor de tenuitvoerlegging van richtlijn 2002/58/EG voor de bewaring van gegevens om de veiligheid te waarborgen, en van richtlijn 2006/24/EG om de beschikbaarheid van deze gegevens te waarborgen) om het de providers makkelijker te maken. Welke artikelen van deze richtlijnen moeten nog omgezet worden ?

Ten slotte beweert de minister dat hij het — met hoogdringendheid gevraagde — advies van de Raad van State heeft gevolgd. In feite volgt hij alleen de details (overeenstemmingstabell) en houdt hij geen rekening met de opmerkingen betreffende de parallelle wetgeving, de vereiste om de nadere regels betreffende de aanvraag en de overdracht in de wet op te nemen, de overschrijding van de termijnen in sommige gevallen, of de verplichting om duidelijk aan te geven wie toegang heeft tot de gegevens.

De tekst van ontwerpartikel 5 zegt niets over de autoriteit en over de nadere regels voor het opvragen en de overdracht van gegevens. Aangezien deze regeling een schending kan inhouden van het fundamenteel recht op het privé-leven, is het belangrijk dat de wetgever zelf de krachtlijnen van deze overdracht bepaalt.

M. Daems renvoie aux remarques de l'ISPA, qui sont en tout cas pertinentes sur un point. Cette législation s'applique aux adresses Internet publiques. Grâce à certaines techniques, il est possible de créer des adresses publiques groupées via des adresses privées. Comment le projet de loi à l'examen règle-t-il cette question ? Ces adresses privées rendues publiques sous forme de groupes relèvent-elles aussi de la réglementation ou non ? Si ce n'est pas le cas, une personne dont les données ont été conservées sur la base d'adresses privées peut-elle accuser des opérateurs de rendre les adresses publiques, alors que la loi ne le permet pas ?

Mme Piryns fustige la manière dont l'examen de plusieurs projets de loi importants doit être expédié à la Chambre des représentants et au Sénat. Cette manière de procéder est particulièrement problématique pour le projet de loi qui nous occupe, dans la mesure où il concerne la transposition d'une directive européenne qui a déjà été adoptée il y a sept ans. Le gouvernement a pris tout son temps, et il faut aujourd'hui examiner le projet de loi à la hâte, si bien qu'il n'est plus possible d'organiser des auditions ni de mener un débat sérieux sur le sujet. Il s'agit pourtant, en l'occurrence, d'une législation fondamentale. L'argument selon lequel notre pays risque une amende si la transposition n'est pas effectuée dans les délais ne tient pas, dès lors que le gouvernement est personnellement responsable de cette non-transposition.

En outre, il ressort du débat mené dans d'autres États membres de l'Union européenne qu'il faudrait en fait s'opposer à cette directive. Tant en Allemagne qu'en Roumanie, par exemple, on se pose de sérieuses questions quant à la compatibilité de cette directive avec les libertés constitutionnelles nationales. Il est fâcheux que le gouvernement belge ne s'interroge pas à cet égard. Tout cela est indigne d'une démocratie.

Sur le fond, l'intervenante adhère aux arguments formulés par M. Hellings. Enregistrer ainsi toutes les données de tout un chacun et conserver pendant au moins un an l'identité des destinataires de sms ou de courriels constitue une grave atteinte à la vie privée. Alors que certains ne se posent à première vue aucune question à ce sujet, il en ira sans doute autrement lorsqu'ils s'avéreront que des tiers peuvent consulter sans problème les données personnelles et même déterminer l'endroit où l'on se trouvait au moment de l'envoi, ce qui veut dire qu'il est possible de vérifier où l'on se trouvait durant une année entière !

C'est pourquoi Mme Piryns s'oppose au projet de loi à l'examen, d'autant plus que son champ d'application est défini de manière très large. La directive européenne laisse aux États membres la latitude de conserver les données pour une durée comprise entre six mois et deux ans. Le gouvernement belge opte

De heer Daems verwijst naar de opmerkingen van ISPA, die zeker op één punt terecht zijn. Deze wetgeving is van toepassing op publieke internet-adressen. Door het gebruik van sommige technieken kan men via private adressen gebundeld publieke adressen maken. Hoe is deze aangelegenheid geregel in voorliggend wetsontwerp ? Vallen die private adressen die gebundeld publiek worden gemaakt ook onder de regeling of niet ? Indien dit niet het geval is, kan iemand wiens data werden bijgehouden op basis van private adressen operatoren ervan beschuldigen de adressen publiek te maken, waar dit wettelijk gesproken niet mag.

Mevrouw Piryns hekelt de wijze waarop enkele belangrijke wetsontwerpen snel door de Kamer van volksvertegenwoordigers en de Senaat moeten worden besproken. Zeker voor onderhavig wetsontwerp is dit problematisch vermits het de omzetting betreft van een Europese richtlijn die reeds 7 jaar geleden werd aangenomen. De regering heeft hier zo lang mee gewacht en nu moet het wetsontwerp snel worden behandeld, zodat er geen ruimte is voor hoorzittingen noch voor een ernstig debat. Het gaat nochtans om fundamentele wetgeving. Het argument, dat ons land in geval van niet-tijdige omzetting een boete riskeert, snijdt geen hout vermits het de fout van de regering zelf is dat de richtlijn nog steeds niet is omgezet.

Bovendien blijkt uit het debat dat in andere landen van de Europese Unie werd gevoerd dat men zich eigenlijk zou moeten verzetten tegen deze richtlijn. Zowel in Duitsland als Roemenië werden immers reeds ernstige vragen gesteld over de verenigbaarheid ervan met hun grondwettelijke vrijheden. Het is betreurenswaardig dat de Belgische regering zich hier geen vragen bij stelt. Dit alles is een democratie onwaardig.

Ten gronde, sluit spreekster zich aan bij de argumenten die door de heer Hellings naar voor werden gebracht. Het is een enorme inbreuk op de private levenssfeer om zomaar alle gegevens van eenieder op te slaan en zeker gedurende een jaar bij te houden wie men sms't of mailt. Waar sommigen zich hierover op het eerste gezicht geen vragen stellen, zal dit wellicht wel het geval zijn wanneer blijkt dat anderen de persoonlijke gegevens zomaar kunnen raadplegen en zelfs kunnen vaststellen waar men zich bevond op het moment van de verzending. Dit betekent dat kan worden nagegaan waar men zich bevond gedurende een volledig jaar !

Daarom verzet mevrouw Piryns zich tegen voorliggend wetsontwerp, temeer omdat het toepassingsgebied ervan zeer ruim werd gedefinieerd. De Europese richtlijn geeft de lidstaten de ruimte om de gegevens bij te houden voor een periode tussen een half jaar en twee jaar. De Belgische regering kiest er

d'emblée, sans justification, pour un délai de conservation d'un an. L'intervenante suppose que ce délai a été choisi afin de laisser le temps à la justice belge, relativement lente, de demander les données nécessaires. Il aurait mieux valu s'employer à améliorer l'efficacité de la justice. Qui plus est, le délai d'un an peut être porté à vingt-quatre mois, et ce sans une intervention du Parlement !

Bref, le gouvernement pourrait non seulement s'opposer à la directive européenne et se joindre aux protestations d'autres pays, mais il pourrait aussi, en transposant la directive en droit belge, aller moins loin dans la violation de la vie privée.

#### *Réponses du secrétaire d'État*

M. John Crombez, secrétaire d'État à la Lutte contre la fraude sociale et fiscale, indique que l'arrêté royal pris en exécution de l'article 5, § 3, alinéa 3, du projet à l'examen, a été soumis pour consultation aux membres de la Chambre des représentants et il souhaite qu'il en aille de même en ce qui concerne les sénateurs.

Conformément à la réglementation en vigueur, le durée de conservation des données ne peut être inférieure à douze mois ni supérieure à trente-six mois. La directive européenne prévoit aujourd'hui de ramener ce délai maximum à vingt-quatre mois, ainsi que dispose aussi l'article 5 du projet de loi à l'examen. Le projet ne va donc pas plus loin que la directive, dont il reprend toutefois le délai maximum de vingt-quatre mois, soit un délai inférieur à celui de trente-six mois en vigueur aujourd'hui.

Le secrétaire d'État déclare ensuite que le projet de loi ne fait pas de distinction entre les adresses Internet publiques et les adresses Internet privées.

Par ailleurs, M. Crombez estime que certains mènent un faux débat. Il a pourtant été clair dès le départ dans la formulation des objectifs. Il rappelle que, par comparaison avec la législation actuelle, qui préconise un délai maximum de trente-six mois, le projet de loi à l'examen prévoit un délai de douze mois, pouvant éventuellement être prolongé jusqu'à vingt-quatre mois. Ce délai vaut aussi pour les données existantes dont disposent aujourd'hui les opérateurs.

Si les cours constitutionnelles allemande et roumaine s'interrogent sur la compatibilité de la directive européenne avec les droits et libertés fondamentaux, il s'agit avant tout d'une préoccupation européenne. Le fait que cette discussion ait lieu entre certains États

meteen voor om de gegevens voor één jaar bij te houden, zonder dat dit wordt verantwoord. Spreekster gaat ervan uit dat deze termijn werd genomen om de Belgische justitie, die eerder traag werkt, de tijd te geven de gegevens op te vragen. Beter wäre het de justitie sneller te laten werken. Bovendien kan de termijn van één jaar worden verlengd tot vierentwintig maanden, en dit zonder een tussenkomst van het Parlement !

Kortom : de regering zou zich niet alleen kunnen verzetten tegen de Europese richtlijn en zich aansluiten bij het protest uit andere landen, maar zou bij de omzetting ervan in Belgisch recht ook minder ver kunnen gaan in de schending van de private levenssfeer.

#### *Antwoorden van de staatssecretaris*

De heer John Crombez, staatssecretaris voor de Bestrijding van de sociale en de fiscale fraude, wijst erop dat het koninklijk besluit dat wordt genomen ter uitvoering van artikel 5, § 3, derde lid, van voorliggend ontwerp, ter inzage werd verstrekt aan de leden van de Kamer van volksvertegenwoordigers en wenst dat dit ook zou gebeuren voor de senatoren.

Volgens de thans geldende regelgeving worden de gegevens gedurende minimum twaalf en maximum zesendertig maanden bewaard. De Europese richtlijn bepaalt nu dat deze maximumtermijn wordt ingekort tot vierentwintig maanden en dit is wat ook artikel 5 van voorliggend wetsontwerp bepaalt. Het ontwerp gaat dus niet verder dan de draagwijdte van de richtlijn, maar neemt wel de maximumtermijn van vierentwintig maanden over. Dit is evenwel minder dan de termijn van zesendertig maanden die vandaag geldt.

De staatssecretaris geeft vervolgens aan dat het wetsontwerp geen onderscheid maakt tussen publieke en private internetadressen.

Verder is de heer Crombez van oordeel dat sommigen op een onbehoorlijke manier het debat voeren. Nochtans is hij van meet af aan duidelijk geweest in de formulering van de doelstellingen. Hij herhaalt dat, in vergelijking tot de huidige stand van de wetgeving die een maximumtermijn van zesendertig maanden vooropstelt, onderhavig wetsontwerp een termijn twaalf maanden, eventueel te verlengen tot vierentwintig maanden, omvat. Deze termijn geldt ook voor de reeds bestaande gegevens die vandaag in het bezit zijn van de operatoren.

Wanneer de grondwettelijke hoven van Duitsland en Roemenië zich vragen stellen over de verenigbaarheid van de Europese richtlijn met de fundamentele rechten en vrijheden, is dit in de eerste plaats een bezorgdheid voor de Europese Unie. Het feit dat deze

membres et l'Union européenne ne dispense pas les autres États membres de l'obligation de transposer la directive en droit interne. Du reste, l'intervenant rappelle que la Suède, qui n'a pas transposé la directive, s'est vu infliger une amende de 3 millions d'euros. La façon dont le gouvernement belge procède à cette transposition ne change d'ailleurs rien, ou si peu, à la situation qui prévaut sur le terrain.

On recourt déjà souvent, aujourd'hui, à l'« exploration de données » dans des matières très concrètes qui l'exigent. Cela ne signifie pas pour autant qu'on puisse utiliser comme ça toutes les données de toutes les personnes, à tout moment et sans limites. Bien au contraire : l'exploration de données est chaque fois mise en balance avec la vie privée de la personne, dans le respect de la législation et des directives en la matière. Il a en outre été dûment tenu compte, lors de la rédaction du projet de loi à l'examen, du deuxième avis de la Commission de la protection de la vie privée.

Il existe déjà, à l'heure actuelle, toute une réglementation sur l'« exploration de données » et le respect de la vie privée; une concertation approfondie a d'ailleurs été menée à ce sujet, notamment au sein des comités sectoriels concernés. Ainsi par exemple, il existe des directives qui concernent les magasins. Il faut aujourd'hui réglementer le secteur des télécommunications et prévoir un cadre légal pour une situation qui est en fait existante, et cela poserait des problèmes insurmontables ? En outre, un cadre légal définit maintenant les rapports entre le secteur, la police et la justice, ce qui est tout de même particulièrement important ! Le cadre légal proposé marque une avancée par rapport à la situation actuelle.

Le secrétaire d'État renvoie ensuite explicitement à l'avis rendu par la Commission de la protection de la vie privée au sujet du projet de loi à l'examen. Il ne voit pas d'objection à ce qu'une discussion fondamentale ait lieu, mais il faut alors aussi accorder au point de vue de cette Commission l'importance qu'il mérite. Ce que dit cette Commission est bien différent de ce que d'aucuns veulent faire croire aujourd'hui. Le gouvernement a pratiquement tenu compte de toutes les observations de la Commission de la protection de la vie privée et les a intégrées dans le projet de loi.

M. Crombez rappelle les conclusions de la « *Federal Computer Crime Unit* », qui ont été présentées récemment. Il ne s'agit pas de petite criminalité mais, au contraire, de blanchiment d'argent, de terrorisme, etc. Il est apparu qu'une durée de conservation des données de six mois permet à la FCCU de résoudre 26 % des affaires. Après une durée d'un an, ce pourcentage atteint même 61 % ! Ces chiffres parlent d'eux-mêmes et prouvent encore une fois la nécessité d'une lutte efficace contre la criminalité organisée.

discussie wordt gevoerd tussen sommige lidstaten en de Europese Unie, ontslaat de andere lidstaten niet van de verplichting de richtlijn om te zetten in intern recht. Spreker herinnert er overigens aan dat Zweden, die de richtlijn niet heeft omgezet, een boete van 3 miljoen euro werd opgelegd. De wijze waarop de Belgische regering de richtlijn omzet, verandert overigens vrijwel niets aan de bestaande situatie op het terrein.

Vandaag reeds wordt veel beroep gedaan op « *datamining* », voor zeer concrete aangelegenheden waarvoor dit noodzakelijk is. Dit betekent evenwel geenszins dat men zomaar op een onbegrenste manier een beroep doet op alle gegevens van elke persoon op elk ogenblik. Het tegendeel is eerder waar : telkens wordt een afweging gemaakt met de private levenssfeer van elkeen en houdt men rekening met de wetgeving en richtlijnen terzake. Bovendien werd bij het uitschrijven van het wetsontwerp terdege rekening gehouden met het tweede advies van de Privacycommissie.

Er bestaat vandaag reeds heel wat regelgeving inzake « *datamining* » en het respect voor de privacy; hierover wordt bovendien grondig overleg gepleegd, onder meer in de betrokken sectoriële comités. Zo zijn er bijvoorbeeld richtlijnen voor de winkels. Vandaag gaat het om de telecomsector en wordt in feite een bestaande situatie wettelijk omkaderd en dit zou dan onoverkomelijke problemen veroorzaken ? Bovendien wordt nu een wettelijk kader gecreëerd voor de verhoudingen tussen de sector en de politie en de justitie, wat toch zeer belangrijk is ! De voorgestelde wettelijke omkadering betekent een vooruitgang ten aanzien van de huidige situatie.

De staatssecretaris verwijst voorts nadrukkelijk naar het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer over onderhavig wetsontwerp. Hij is het ermee eens dat een fundamentele discussie wordt gevoerd, maar in dat geval moet men ook voldoende belang hechten aan de zienswijze van deze Commissie. Deze Commissie zegt heel wat anders dan wat sommigen vandaag willen doen geloven. De regering heeft rekening gehouden met vrijwel alle opmerkingen van de Privacycommissie en heeft deze geïntegreerd in het wetsontwerp.

De heer Crombez herinnert aan de bevindingen van de « *Federal Computer Crime Unit* » die recent werden voorgesteld. Het gaat hier niet om kleine criminaliteit, maar integendeel om witwassen van geld, terrorisme en dergelijke. Het is gebleken dat de FCCU, door gedurende zes maanden data bij te houden, in staat is om 26 % van de gevallen op te lossen. Na verloop van één jaar loopt dit percentage zelfs op tot 61 % ! Deze cijfers spreken voor zich en bewijzen nogmaals de noodzaak van een efficiënt optreden tegen de georganiseerde criminaliteit.

Certes, l'examen parlementaire du projet de loi est réalisé en un laps de temps très court, mais il ne faut tout de même pas perdre de vue que les débats préparatoires sur le projet de loi ont duré plusieurs années et que ces débats sont aussi déjà menés en toute transparence depuis 2008 et leur publication par l'IBPT.

Dès 2009 et 2010, le Parlement a organisé des auditions avec le concours du ministre de la Justice de l'époque. Le débat a aussi été alimenté par les résultats de la concertation qui a eu lieu avec les acteurs et les organes consultatifs concernés. Après toute cette procédure de concertation, le ministre compétent en la matière a donc pris ses responsabilités en soumettant un projet de loi à l'approbation du Parlement.

En réponse aux remarques formulées, le secrétaire d'État tient encore à préciser ce qui suit :

— données privées versus données à caractère personnel :

Aucune distinction n'est faite entre données privées et données publiques;

— demande de données :

Tant le procureur du Roi que le juge d'instruction, chacun pour ce qui concerne ses compétences propres, doivent respecter les principes de proportionnalité, de subsidiarité et de nécessité lorsqu'ils requièrent la collaboration des fournisseurs de réseaux ou de services pour la communication de données conservées. À cet égard, il ne faut pas perdre de vue que, de par l'accès aux données conservées qui leur est donné, les autorités judiciaires peuvent aussi bien inculper une personne que l'innocenter;

— vie privée :

Il est faux de croire que plus le délai de conservation des données à caractère personnel est court, mieux la vie privée est protégée. Ce n'est qu'en déterminant avec précision quelles données peuvent être consultées, par qui et selon quelles modalités que l'on protégera efficacement la vie privée. Il va sans dire que l'utilisation des données précitées s'inscrit avant tout dans le cadre de la recherche de coupables, mais elle permet aussi, dans certains cas, d'innocenter des personnes. À l'heure actuelle déjà, la Justice peut porter atteinte à la vie privée, par exemple lorsqu'elle ordonne une perquisition;

— cadre réglementaire actuel :

Le projet de loi à l'examen n'élargit pas le champ d'application, mais en donne une définition plus précise. La Justice a déjà la possibilité aujourd'hui de réclamer aux opérateurs toutes les données que ceux-ci conservent pour quelque raison que ce soit. L'objectif est donc non pas d'obliger les opérateurs à

Waar de parlementaire behandeling van het wetsontwerp op een korte tijdsperiode wordt gevoerd, mag men toch niet uit het oog verliezen dat de voorbereidende debatten over het wetsontwerp verscheidene jaren hebben geduurde en dat deze debatten, sedert 2008, na de openbaarmaking door het BIPT, ook reeds in alle openheid worden gevoerd.

Reeds in 2009 en 2010 werden er in het Parlement hoorzittingen georganiseerd met medewerking van de toenmalige minister van Justitie. Het debat werd ook verder gevoerd door de resultaten van het overleg dat met de betrokken actoren en adviesorganen heeft plaatsgehad. Na heel deze overlegprocedure heeft de terzake bevoegde minister dan zijn verantwoordelijkheid opgenomen en een wetsontwerp ter goedkeuring in het Parlement neergelegd.

Voorts heeft de staatssecretaris nog de volgende antwoorden op de gemaakte opmerkingen :

— private versus persoonlijke gegevens :

Er wordt geen onderscheid gemaakt tussen private en publieke gegevens;

— opvraging gegevens :

Zowel de procureur des Konings als de onderzoeksrechter, elk voor hun eigen bevoegdheden, moeten de beginselen van evenredigheid, subsidiariteit en noodzakelijkheid in acht nemen wanneer ze de medewerking van de netwerk- of dienstenaanbieders eisen om bewaarde gegevens mee te delen. Daarbij mag niet uit het oog worden verloren dat de toegang tot deze bewaarde gegevens de gerechtelijke autoriteiten in staat kan stellen om een persoon zowel te beschuldigen als vrij te spreken;

— privacy :

Het is een misvatting te denken dat de privacy beter wordt beschermd naarmate de bewaartijd van de persoonlijke gegevens korter is. De bescherming van de privacy is alleen gediend met de nauwkeurige omschrijving van wie wat kan raadplegen en hoe dit dient te gebeuren. Het gebruik van voornoemde gegevens kadert uiteraard vooral in de zoektocht naar schuldigen maar kan soms ook het bewijs van onschuld leveren. Vandaag reeds kan de justitie een inbreuk op de privacy plegen, bijvoorbeeld wanneer ze een huiszoeking beveelt;

— huidig reglementair kader :

Het voorliggend ontwerp breidt het toepassingsgebied niet uit, maar omschrijft het nauwkeuriger. Alle gegevens die de operatoren om welke reden ook bewaren, kunnen thans door de justitie reeds worden opgevraagd. Het gaat er dus niet om de operatoren tot het creëren van nieuwe databanken te verplichten, wel

créer de nouvelles banques de données, mais bien à leur imposer un délai minimum de conservation lorsqu'ils disposent déjà d'une telle banque de données;

— délai de conservation de douze mois :

L'article 6 de la directive 2006/24/CE prévoit un délai minimum de conservation des données de six mois et un délai maximum de conservation des données de vingt-quatre mois. Le délai de conservation de douze mois qui a été retenu s'inscrit dans cette fourchette. La Commission de la protection de la vie privée avait, dans son avis n° 20/2009, proposé un délai de conservation de douze mois, qui est le délai retenu par les autorités. Vu l'importance cruciale des données d'identification, d'enregistrement et de localisation en matière de communications électroniques dans la lutte contre la criminalité, mais compte tenu néanmoins des coûts liés à la conservation, le gouvernement ne veut pas aller aussi loin que la directive en imposant un délai maximum de vingt-quatre mois, mais a fait le choix d'opter pour un délai de douze mois. Il y a de nombreux cas où l'utilisation de certaines données téléphoniques du passé a permis de faire avancer des enquêtes pénales.

Il convient également de renvoyer au rapport d'évaluation de la directive européenne de la Commission européenne du 18 avril 2011 (COM 2011 225 final) qui énonce notamment : « Ces données [les données conservées] fournissent des preuves et des indices précieux pour prévenir et poursuivre les infractions et garantir une justice pénale. Leur utilisation a abouti à des condamnations pour des infractions pénales qui, si les données n'avaient pas été conservées, seraient restées impunies. Elle a également permis l'acquittement de personnes innocentes (Rapport d'évaluation, pp. 34- 35). »;

— possibilité de prolongation du délai de conservation de douze mois :

Le délai de conservation proposé de douze mois ne peut être prolongé par arrêté royal qu'après évaluation par le Parlement.

### *Répliques*

M. Hellings dit n'avoir encore reçu aucune réponse à sa question relative aux « *hot spots* ». Quel sera l'impact des nouvelles dispositions sur le contrôle des « *hot spots* » ? Les criminels ne manqueront pas d'en faire usage. L'intervenant se demande aussi comment le problème des cartes prépayées sera réglé.

hun een mininumbewaartermijn op te leggen wanneer zij reeds over dergelijke databank beschikken;

— bewaartermijn van twaalf maanden :

Artikel 6 van richtlijn 2006/24/EG voorziet in een minimale bewaringstermijn van de gegevens van zes maanden en in een maximale bewaringstermijn van de gegevens van vierentwintig maanden. De in aanmerking genomen bewaringstermijn van twaalf maanden valt binnen die uitersten. De Privacy-commissie had in haar advies nr. 20/2009 een bewaringstermijn van twaalf maanden voorgesteld, wat de termijn is die de overheid in aanmerking neemt. Gezien het cruciale belang voor de criminaliteitsbestrijding om te beschikken over identificatie-, registratie- en locatiegegevens inzake elektronische communicatie enerzijds en toch rekening houdend met de kosten die de bewaring met zich brengt anderzijds, wil de regering niet zo ver gaan als de maximumtermijn van vierentwintig maanden van de richtlijn maar opteert zij voor een termijn van twaalf maanden. Talrijk zijn de voorbeelden in strafrechtelijke onderzoeken waar een doorbraak nog kon geforceerd worden omdat men bepaalde telefoniegegevens uit het verleden nog kon bekomen.

Er moet ook verwezen worden naar het evaluatie-rapport van de Europese richtlijn van de Europese Commissie van 18 april 2011 (COM2011 225 definitief) dat onder meer stelt : « Deze gegevens [de bewaarde gegevens] leveren waardevolle aanwijzingen en bewijzen op die ertoe leiden dat strafbare feiten kunnen worden voorkomen en vervolgd en dat het strafrecht zijn beloop kan hebben. Dankzij de bewaarde gegevens zijn veroordelingen uitgesproken voor strafbare feiten die zonder deze gegevens misschien nooit zouden zijn opgelost. Ook zijn onschuldige personen vrijgesproken op basis van bewaarde gegevens (Evaluatierapport, p. 34-35). »;

— mogelijke verlenging van de bewaartermijn van twaalf maanden :

Een verlenging van de vooropgestelde bewaartermijn van twaalf maanden kan bij koninklijk besluit slechts geschieden na een evaluatie door het Parlement.

### *Replieken*

De heer Hellings stelt nog geen antwoord te hebben gekregen met betrekking tot zijn vraag over de *hot spots*. Hoe zullen de nieuwe bepalingen een effect hebben op de controle van de *hot spots*. Juist hiervan zullen de criminelen gebruik maken. Spreker vraagt zich ook af hoe men de vooraf betaalde kaarten aanpakt.

En ce qui concerne le calendrier de transposition de la directive, l'intervenant indique que son groupe n'aurait rien à se reprocher si l'Europe devait infliger une amende à notre pays, étant donné qu'il n'a cessé depuis des années d'interpeler le ministre compétent au sujet de cette directive. Le gouvernement est responsable d'avoir laissé traîner les choses.

Cette directive est problématique dans de nombreux États européens et la Belgique pouvait se baser sur le travail fait dans les autres pays pour la transposer d'une façon respectueuse des droits humains.

La Cour constitutionnelle allemande de Karlsruhe a jugé, après la transposition allemande contenant une obligation de rétention de données de six mois, que le dispositif mis en place par le gouvernement fédéral obligeant les fournisseurs d'accès à Internet et les opérateurs téléphoniques, au nom de la lutte contre le terrorisme et la criminalité en ligne, à stocker systématiquement pendant six mois les données relatives aux appels téléphoniques et connections internet, ne correspond pas à la Charte européennes des droits fondamentaux.

L'intervenant soutient l'objectif suivi de lutter contre la fraude en général et il est évident que la fraude passe par la voie électronique. La vision sur le *datamining* avancée par le secrétaire d'État est celle de la FCCU. Mais la question de la proportionnalité se pose, car il est évident qu'il faut vérifier ce que font certaines personnes lorsque le doute existe et la législation en la matière existe déjà pour permettre à la Sureté de l'État et à la police de faire ce qui est nécessaire et de mettre sur écoute des criminels qu'on soupçonne. Cette possibilité n'est pas mise en cause, mais bien celle du *datamining*. Dans ce cas, l'on présume un comportement criminel sur la base de statistiques et non plus de soupçons. Les services concernés doivent pouvoir accéder à certaines données, mais bien dans un cadre balisé qui existe déjà. La proportionnalité pose la question de savoir si nous sommes prêts à remettre en cause la liberté fondamentale de la vie privée par rapport à la menace que représentent fraude et terrorisme.

Ce qui est proposé par le projet de loi est d'augmenter à la fois la durée de détention des données et le nombre de personnes qui y ont accès. En augmentant la période de six à douze mois, la potentialité des données récoltées est doublée. L'intervenant estime aussi que le nombre de personnes qui auront accès est beaucoup trop large et la loi devrait déterminer clairement qui peut accéder à ces données.

Il y a eu différents cas de bases de données (SNCB,...) qui se sont retrouvées accidentellement sur Internet et cela prouve bien que plus des données électroniques sont sauvegardées, plus nombreuses sont

In verband met de timing van de omzetting van de richtlijn, stelt de spreker dat zijn fractie niets kan verweten worden, moest er een Europese boete komen voor ons land aangezien ze de bevoegde minister jaren geleden al over deze richtlijn hebben aangesproken. Het is de verantwoordelijkheid van de regering die de zaak heeft laten aanslepen.

Deze richtlijn wordt in heel wat Europese staten als een probleem ervaren en België kon zich laten inspireren door de aanpak van andere landen om ze om te zetten met eerbiediging van de mensenrechten.

Het Duits Grondwettelijk Hof van Karlsruhe oordeelde na de Duitse omzetting met een verplichting om de gegevens zes maanden te bewaren, dat de regeling die de bondsregering had ingesteld, waarbij de aanbieders van internetdiensten en de telefoonoperatoren verplicht werden de data in verband met de telefoonoproepen en de internetverbindingen in naam van de strijd tegen terrorisme en misdaad gedurende zes maanden systematisch te bewaren, niet overeenstemt met het Europees Handvest van de grondrechten van de Europese Unie.

Spreker steunt de doelstelling de fraude in het algemeen te bestrijden en het is evident dat fraude langs elektronische weg plaatsvindt. De visie op *datamining* die de staatssecretaris naar voor schuift is die van de FCCU. Hier rijst evenwel het proportionaliteitsprobleem, want het is duidelijk dat men moet controleren wat bepaalde personen doen wanneer er twijfel bestaat en de wetgeving ter zake reeds bestaat om de Veiligheid van de Staat en de politie in de gelegenheid te stellen het nodige te doen en misdadigers die men verdenkt af te luisteren. Die mogelijkheid wordt niet betwist, maar de mogelijkheid van *datamining* wel. In dat geval gaat men er op basis van statistieken en niet van verdenking vanuit dat er misdadig gedrag is. De betreffende diensten moeten toegang krijgen tot bepaalde gegevens, maar dan binnen reeds bestaande kijftlijnen. De proportionaliteit doet de vraag rijzen of we bereid zijn de fundamentele vrijheid van de persoonlijke levenssfeer op losse schroeven te zetten in het licht van de dreiging van fraude en terrorisme.

In het wetsontwerp stelt men voor zowel de bewaartijd voor de data als het aantal personen die er toegang toe hebben, te verhogen. Door de periode te verhogen van zes tot twaalf maanden, worden de gebruiksmogelijkheden van de verzamelde gegevens verdubbeld. Spreker vindt ook dat het aantal personen dat toegang krijgt veel te groot is en dat de wet duidelijk moet bepalen wie toegang tot die gegevens kan krijgen.

Meer dan eens zijn databanken (NMBS, ...) per ongeluk op het internet beland, wat bewijst dat hoe meer digitale gegevens bewaard worden en hoe meer personen er toegang toe hebben, hoe groter het gevaar

les personnes qui y ont accès et plus grand est le danger que ces données ne soient dévoilées au grand jour. Il faut réduire ce risque. C'est un des objectifs des amendements déposés par l'intervenant.

## 2. Discussion des amendements

Article 5

### *Amendement n° 1*

M. Hellings dépose l'amendement n° 1 (doc. Sénat, n° 5-2222/2), qui vise à remplacer les mots « les fournisseurs au public » par les mots « les opérateurs » et les mots « fournisseurs de réseaux publics » par les mots « opérateurs de réseaux publics ».

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État explique qu'il s'agit d'une incompréhension du texte. Les fournisseurs et revenus de réseaux ou de services visés à l'article 9, §§ 5 et 6, de la loi du 13 juin 2005 relative aux communications électroniques (par exemple le wifi offert par un café ou un hôtel) sont exclus du champ d'application du nouvel article 126 de la même loi, comme demandé par la Commission vie privée. Cela ressort du texte de cet article et les travaux préparatoires le confirment explicitement.

### *Amendement n° 2*

M. Hellings dépose l'amendement n° 2 (doc. Sénat, n° 5-2222/2), qui vise à supprimer, au § 1<sup>er</sup> de l'article 126 proposé, l'alinéa 2.

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État renvoie à la réponse qu'il a formulée au sujet de l'amendement n° 1 et prie la commission de ne pas adopter cet amendement.

### *Amendement n° 3*

M. Hellings dépose l'amendement n° 3 (doc. Sénat, n° 5-2222/2), qui vise à supprimer les mots « sauf disposition légale contraire » dans l'article 126, § 1<sup>er</sup>, alinéa 6, proposé.

M. Hellings renvoie à sa justification écrite, mais ajoute que cet amendement vise à faire en sorte qu'il

is dat die gegevens openbaar worden gemaakt. Men moet dat risico beperken. Dat is een van de doelstellingen van de amendementen die spreker heeft ingediend.

## 2. Bespreking van de amendementen

Artikel 5

### *Amendement nr. 1*

De heer Hellings dient amendement nr. 1 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt de woorden « de aanbieders van aan het publiek aangeboden » te vervangen door de woorden « de operatoren » en de woorden « de aanbieders van de onderliggende » te vervangen door de woorden « de operatoren van de onderliggende ».

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris legt uit dat men de tekst niet begrepen heeft. De leveranciers en de doorverkopers van netwerken of van diensten bedoeld in artikel 9, §§ 5 en 6, van de wet van 13 juni 2005 betreffende de elektronische communicatie (bijvoorbeeld de wifi die een café of een hotel aanbiedt), worden van het toepassingsgebied van het nieuwe artikel 126 van dezelfde wet uitgesloten, zoals de privacycommissie dat gevraagd heeft. Dat blijkt uit de tekst van dat artikel en wordt uitdrukkelijk bevestigd in de parlementaire voorbereiding.

### *Amendement nr. 2*

De heer Hellings dient amendement nr. 2 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in § 1 van het voorgestelde artikel 126 het tweede lid te doen vervallen.

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris verwijst naar zijn antwoord op het amendement nr. 1 en verzoekt de commissie het amendement niet te steunen.

### *Amendement nr. 3*

De heer Hellings dient amendement nr. 3 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in § 1, zesde lid, van het voorgestelde artikel 126 de woorden « behoudens andersluidende wettelijke bepaling » te vervangen door het woord « er ».

De heer Hellings verwijst naar zijn schriftelijke toelichting, maar voegt toe dat dit amendement ervoor

soit explicitement exclu que le contenu de la communication électronique soit sauvegardé. Le secrétaire d'État a en effet expliqué que tel était bien l'objectif poursuivi.

Le secrétaire d'État répond que l'article 5.2 de la directive « conservation des données » prévoit qu'« aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive ». La conservation du contenu est donc possible si une autre directive que la directive « conservation des données » permet ou impose de conserver le convenu.

Les mots « sans disposition légale contraire » visent les dispositions légales éventuelles qui seraient adoptées pour transposer une autre directive que la directive « conservation des données » qui imposerait ou permettrait de conserver le contenu.

Si le législateur décidait plus tard de conserver le contenu des communications, ce ne serait donc possible que si permis par une autre directive que la directive « conservation des données ».

Il n'a jamais été question d'imposer aux opérateurs de conserver le contenu.

Il demande à la commission de ne pas soutenir l'amendement.

#### *Amendement n° 4*

M. Hellings dépose l'amendement n° 4 (doc. Sénat, n° 5-2222/2), qui vise à remplacer le § 2, alinéa 1<sup>er</sup>, *a*, de l'article 126 proposé, par ce qui suit : « de la recherche, de l'instruction et de la poursuite du crime organisé et des infractions terroristes, selon la procédure visée aux articles 46bis et 88bis du Code d'instruction criminelle. »

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État explique qu'il revient aux États membres de décider ce qu'il faut entendre par « infractions graves ». Il est estimé que les infractions graves ne sont pas limitées au crime organisé ou aux infractions terroristes.

Par ailleurs, la Commission de la vie privée a marqué son accord avec le texte.

#### *Amendement n° 12*

M. Hellings dépose l'amendement n° 12 (doc. Sénat, n° 5-2222/2), qui vise à supprimer le point *d* dans l'article 126, § 2, alinéa 1<sup>er</sup>, proposé.

wil zorgen dat uitdrukkelijk wordt uitgesloten dat de inhoud van de elektronische communicatie zou worden opgeslagen. De staatssecretaris verklaarde immers dat dit wel degelijk de bedoeling is.

De staatssecretaris antwoordt dat artikel 5.2 van de « dataretentierichtlijn » bepaalt : « Gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, mogen krachtens deze richtlijn niet worden bewaard ». Bewaring van inhoud is dus mogelijk indien een andere richtlijn dan de « dataretentierichtlijn » het bewaren van de inhoud toestaat of verplicht maakt.

« Behoudens andersluidende wettelijke bepaling » behelst de wettelijke bepalingen die kunnen worden aangenomen om een andere richtlijn dan de « dataretentierichtlijn » om te zetten, die het bewaren van de inhoud oplegt of toestaat.

Mocht de wetgever later beslissen de inhoud van de communicatie te bewaren, dan is dat dus slechts mogelijk indien een andere richtlijn dan de « dataretentierichtlijn » het toestaat.

Er is nooit sprake van geweest de operatoren ertoe te verplichten de inhoud te bewaren.

Hij verzoekt de commissie het amendement niet te steunen.

#### *Amendement nr. 4*

De heer Hellings dient amendement nr. 4 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt § 2, eerste lid, *a*, van het voorgestelde artikel 126, te vervangen als volgt : « de opsporing, het onderzoek en de vervolging van de georganiseerde misdaad en van de terroristische misdrijven, volgens de procedure bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering. »

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris legt uit dat het aan de lidstaten is om te bepalen wat moet worden verstaan onder « ernstige criminaliteit ». Men neemt aan dat ernstige criminaliteit niet beperkt blijft tot de georganiseerde misdaad of terroristische misdrijven.

Overigens heeft de Commissie voor de bescherming van de persoonlijke levenssfeer met de tekst ingestemd.

#### *Amendement nr. 12*

De heer Hellings dient amendement nr. 12 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in het voorgestelde artikel 126, § 2, eerste lid, het punt *d* te schrappen.

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État explique que cette disposition figure déjà dans l'article 126 de la loi relative aux communications électroniques et reprend le texte de la directive.

Il demande à la commission de ne pas soutenir l'amendement.

#### *Amendement n° 5*

M. Hellings dépose l'amendement n° 5 (doc. Sénat, n° 5-2222/2), qui vise à remplacer, dans l'article 126, § 2, alinéa 2, proposé, les mots « sur simple demande aux autorités chargées des missions visées aux points a) à d) » par les mots « sur demande du Procureur du Roi et du juge d'instruction selon les modalités prévues aux articles 46bis et 88bis du Code d'instruction criminelle, sur demande écrite du chef de service des services d'urgences visée à l'article 107 dans le cadre du § 2, alinéa 1<sup>er</sup>, b), du chef de service du Service de médiation dans le cadre du § 2, alinéa 1<sup>er</sup>, c), ainsi que du chef de service des renseignements civils et militaires dans le cadre du § 2, alinéa 1<sup>er</sup>, d) ».

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État répond que le nouvel article 126 n'a pas pour objet de régler en détail la transmission des données conservées aux autorités. Les règles concernant ces modalités contenues dans d'autres législations, par exemple dans le Code d'instruction criminelle, restent entièrement d'application. Si on devait estimer que les règles de transmission des données conservées des opérateurs vers les autorités ne sont pas adéquates, ce sont ces autres législations qu'il conviendrait de modifier, pas le nouvel article 126.

#### *Amendement n° 6*

M. Hellings dépose l'amendement n° 6 (doc. Sénat, n° 5-2222/2), qui vise à remplacer, dans l'article 126, § 3, alinéa 1<sup>er</sup>, proposé, le mot « douze » par le mot « six ».

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État explique que la Commission de la vie privée, dans son avis 20/2009 du 1<sup>er</sup> juillet 2009 a donné un avis favorable sur l'avant-projet de loi, à la

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris verduidelijkt dat deze bepaling vandaag reeds in artikel 126 van de wet elektronische communicatie staat en een overname van de richtlijn betreft.

De staatssecretaris verzoekt de commissie het amendement niet te aanvaarden.

#### *Amendement nr. 5*

De heer Hellings dient amendement nr. 5 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in het voorgestelde artikel 126, § 2, tweede lid, de woorden « op eenvoudig verzoek aan de autoriteiten belast met de opdrachten bedoeld in de punten a) tot d) kunnen worden meegedeeld en uitsluitend aan deze laatsten » te vervangen door de woorden « op verzoek van de procureur des Konings en de onderzoeksrechter op de wijze als bepaald in de artikelen 46bis en 88bis van het Wetboek van strafvordering, of op schriftelijk verzoek van het diensthoofd van de nooddiensten bedoeld in artikel 107 in het kader van § 2, eerste lid, b), van het diensthoofd van de Ombudsman in het kader van § 2, eerste lid, c), alsook van het diensthoofd van de burgerlijke en militaire inlichtingendiensten in het kader van § 2, eerste lid, d) ».

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris antwoordt dat het nieuwe artikel 126 niet strekt om de overdracht van de bewaarde gegevens aan de overheid in detail te regelen. De regels met betrekking tot die modaliteiten die in andere wetten staan, bijvoorbeeld in het Wetboek van strafvordering, blijven volledig van toepassing. Mocht men oordelen dat de regels van overdracht van de bewaarde gegevens van de operatoren aan de overheid niet goed zijn, dan moet men die andere wetten veranderen, niet het nieuwe artikel 126.

#### *Amendement nr. 6*

De heer Hellings dient amendement nr. 6 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in § 3, eerste lid, van het voorgestelde artikel 126, het woord « twaalf » te vervangen door het woord « zes ».

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris legt uit dat de Commissie voor de bescherming van de persoonlijke levenssfeer in haar advies 20/2009 van 1 juli 2009 een gunstig advies

condition que le délai de conservation soit de douze mois.

Concernant les statistiques, on peut lire ce qui suit dans les travaux préparatoires : « Dans des dossiers du parquet fédéral, la FCCU (*Federal Computer Crime Unit*) de la police fédérale recherche des suspects qui utilisent l'Internet. Les chiffres de la FCCU relatifs à l'identification des adresses IP en 2007-2012 nous apprennent qu'avec un délai de conservation de douze mois, les opérateurs avaient pu fournir une réponse dans 61 % des cas. Si ce délai était relevé à dix-huit mois, il pourra être répondu à 78 % des questions posées. »

#### *Amendement n° 7*

M. Hellings dépose l'amendement n° 7 (doc. Sénat, n° 5-2222/2), qui vise à remplacer, dans l'article 126, § 3, alinéa 2, proposé, le mot « douze » par le mot « six ».

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État renvoie à la réponse qu'il a donnée à propos de l'amendement n° 6.

#### *Amendement n° 8*

M. Hellings dépose l'amendement n° 8 (doc. Sénat, n° 5-2222/2), qui vise à compléter l'article 126, § 3, alinéa 2, par ce qui suit : « Il en va de même des données de trafic. »

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État répond que le § 3 prévoit déjà que « les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication ». Il n'est pas nécessaire d'ajouter qu'il en va de même pour les données de trafic.

#### *Amendement n° 9*

M. Hellings dépose l'amendement n° 9 (doc. Sénat, n° 5-2222/2) visant à supprimer le § 4 de l'article 126 proposé.

Il renvoie à sa justification écrite.

Le secrétaire d'Etat explique que le premier alinéa du paragraphe 4 donne au Roi la possibilité de fixer un

heeft gegeven voor het voorontwerp van wet, op voorwaarde dat de bewaartijd twaalf maanden werd.

Wat de statistieken betreft, kan men in de parlementaire voorbereiding het volgende lezen : « In dossiers van het federaal parket spoort de FCCU (*Federal Computer Crime Unit*) van de federale politie verdachten op die gebruikmaken van het internet. Uit de FCCU-cijfers in verband met de identificatie van IP-adressen in 2007-2012 leren we dat met een bewaringstermijn van twaalf maanden de operatoren in 61 % van de gevallen een antwoord hadden kunnen verstrekken. Indien deze termijn zou worden opgetrokken naar achttien maanden, dan kunnen 78 % van de gestelde vragen beantwoord worden. »

#### *Amendement nr. 7*

De heer Hellings dient amendement nr. 7 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in § 3, tweede lid van het voorgestelde artikel 126, het woord « twaalf » te vervangen door het woord « zes ».

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris verwijst naar zijn antwoord op het amendement nr. 6.

#### *Amendement nr. 8*

De heer Hellings dient amendement nr. 8 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in § 3 van het voorgestelde artikel 126, het tweede lid aan te vullen als volgt : « Dit geldt ook voor de verkeersgegevens. »

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris antwoordt dat in § 3 reeds staat dat « De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie ». Het is niet nodig eraan toe te voegen dat hetzelfde voor de verkeersgegevens geldt.

#### *Amendement nr. 9*

De heer Hellings dient amendement nr. 9 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in het voorgestelde artikel 126, § 4, te doen vervallen.

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris legt uit dat het eerste lid van paragraaf 4 de Koning de mogelijkheid geeft om voor

délai supérieur à douze mois, sans dépasser dix-huit mois, pour certaines catégories de données. Cette possibilité donnée au Roi ne peut cependant être exercée qu'après que le ministre et le ministre de la Justice ont fait leur rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 1<sup>er</sup>, alinéa 3 (voir paragraphe 7). Le parlement pourrait prendre une résolution après ce rapport en estimant que le délai de douze mois est suffisant. Il est difficilement imaginable qu'un ministre passe outre à cette résolution et propose un délai de dix-huit mois. Pour ce qui concerne l'alinéa 2 du § 4, la Commission de la vie privée a donné un avis favorable pour autant que des exemples de circonstances exceptionnelles soient données dans les travaux préparatoires, ce qui a été fait.

#### *Amendement n° 10*

M. Hellings dépose l'amendement n° 10 (doc. Sénat, n° 5-2222/2), visant, dans l'article 126 proposé, à remplacer le § 4 par la disposition suivante : « En cas de conflit armé interne ou international impliquant la Belgique, le délai de rétention de données est allongé à douze mois. »

M. Hellings renvoie à sa justification écrite.

Le secrétaire d'État renvoie à sa réponse à l'amendement n° 9 et demande à la commission de ne pas adopter cet amendement.

#### *Amendement n° 11*

M. Hellings dépose l'amendement n° 11 (doc. Sénat, n° 5-2222/2), qui vise à remplacer le § 7 de l'article 126 proposé par ce qui suit : « Le ministre de la Justice fait rapport annuellement au Parlement sur le nombre d'informations et d'instructions pour lesquelles des données ont été demandées et obtenues, le nombre de magistrats qui en ont fait la demande, le type d'infractions pour lesquelles elles ont été demandées, les résultats qui ont été obtenus et, le cas échéant, les infractions à la vie privée qui auraient été constatées. »

M. Hellings renvoie à sa justification écrite.

bepaalde categorieën van gegevens een termijn van meer dan twaalf maanden vast te stellen, zonder dat die termijn meer dan achttien maanden bedraagt. Die mogelijkheid die aan de Koning wordt gegeven, kan echter slechts worden uitgeoefend nadat de minister en de minister van Justitie hun evaluatieverslag hebben uitgebracht aan de Kamer van volksvertegenwoordigers, twee jaar na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, derde lid (zie paragraaf 7). Na dat verslag kan het parlement een resolutie aannemen waarin staat dat de termijn van twaalf maanden volstaat. Men kan zich moeilijk voorstellen dat een minister die resolutie wegwijs en een termijn van achttien maanden voorstelt. Wat het tweede lid van § 4 betreft, heeft de Commissie voor de bescherming van de persoonlijke levenssfeer een gunstig advies gegeven, op voorwaarde dat er in de parlementaire voorbereiding voorbeelden van uitzonderlijke omstandigheden werden gegeven, wat ook gebeurd is.

#### *Amendement nr. 10*

De heer Hellings dient amendement nr. 10 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt in het voorgestelde artikel 126, § 4 te vervangen als volgt : « In geval van een binnenlands of internationaal gewapend conflict waarbij België is betrokken, wordt de bewaringstermijn verlengd tot twaalf maanden. »

De heer Hellings verwijst naar zijn schriftelijke toelichting.

De staatssecretaris verwijst naar zijn antwoord op het amendement nr. 9 en verzoekt de commissie het amendement niet te aanvaarden.

#### *Amendement nr. 11*

De heer Hellings dient amendement nr. 11 in (stuk Senaat, nr. 5-2222/2), dat ertoe strekt § 7 van het voorgestelde artikel 126 te vervangen als volgt : « De minister van Justitie brengt jaarlijks bij het Parlement verslag uit over het aantal inlichtingen en onderzoeken waarvoor gegevens werden gevraagd en verkregen, over het aantal magistraten dat gegevens heeft gevraagd, over het soort misdrijf waarvoor ze werden gevraagd, over de behaalde resultaten en, in voor komend geval, de vastgestelde schendingen van de persoonlijke levenssfeer. »

De heer Hellings verwijst naar zijn schriftelijke toelichting.

Le secrétaire d'État réplique qu'il lui semble utile de garder le rapport d'évaluation approfondi deux ans après l'entrée en vigueur des dispositions. Le § 7 a d'ailleurs été introduit à la demande la Commission vie privée.

Le paragraphe 6 prévoit déjà la fourniture des statistiques annuellement à la Chambre des représentants. Un débat peut avoir lieu à la Chambre après la remise de ces statistiques

#### IV. VOTES

Les amendements n<sup>os</sup> 1 à 4 sont rejetés par 10 voix contre 1.

L'amendement n<sup>o</sup> 5 est rejeté par 9 voix contre 2.

Les amendements n<sup>os</sup> 6 à 10 sont rejetés par 10 voix contre 1.

Les amendements n<sup>os</sup> 11 et 12 sont rejetés par 9 voix contre 2.

L'ensemble du projet amendé est adopté par 9 voix contre 2.

\*  
\* \*

Confiance a été faite aux rapporteurs pour la présentation d'un rapport oral en séance plénière.

*Les rapporteurs,*  
Fauzaya TALHAOUI.  
Richard MILLER.

*Le président,*  
Ludo SANNEN.

\*  
\* \*

**Le texte adopté par la commission  
est identique au texte du projet  
transmis par la Chambre  
des représentants  
(voir le doc. Chambre, n<sup>o</sup> 53-2921/6 — 2012/2013).**

De staatssecretaris antwoordt dat het hem nuttig voorkomt het grondig evaluatieverslag twee jaar na de inwerkingtreding van de bepalingen, te behouden. Paragraaf 7 werd overigens op verzoek van de Commissie voor de bescherming van de persoonlijke levensfeer toegevoegd.

Paragraaf 6 voorziet er nu reeds in dat de statistieken jaarlijks aan de Kamer van volksvertegenwoordigers worden verstrekt. Na het overzenden van die statistieken, kan in de Kamer een debat worden gehouden.

#### IV. STEMMINGEN

De amendementen nrs. 1 tot 4 worden verworpen met 10 stemmen tegen 1 stem.

Het amendement nr. 5 wordt verworpen met 9 tegen 2 stemmen.

De amendementen nrs. 6 tot 10 worden verworpen met 10 stemmen tegen 1 stem.

De amendementen nrs. 11 en 12 worden verworpen met 9 tegen 2 stemmen.

Het wetsontwerp in zijn geheel wordt aangenomen met 9 tegen 2 stemmen.

\*  
\* \*

Vertrouwen werd geschenken aan de rapporteurs voor het uitbrengen van een mondeling verslag in de plenaire vergadering.

*De rapporteurs,*  
Fauzaya TALHAOUI.  
Richard MILLER.

*De voorzitter;*  
Ludo SANNEN.

\*  
\* \*

**De door de commissie aangenomen tekst  
is dezelfde als de tekst van het door  
de Kamer van volksvertegenwoordigers  
overgezonden wetsontwerp  
(zie stuk Kamer, nr. 53 2921/6 — 2012/2013).**