DOC 53 **2921/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

27 juin 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 90*decies* du Code d'instruction criminelle

Pages

SOMMAIRE

LE GOUVERNEMENT DEMANDE L'URGENCE CONFORMÉMENT À L'ARTICLE 80 DE LA CONSTITUTION.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

27 juni 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 90*decies* van het Wetboek van Strafvordering

Blz.

INHOUD

DE SPOEDBEHANDELING WORDT DOOR DE REGERING GEVRAAGD OVEREENKOMSTIG ARTIKEL 80 VAN DE GRONDWET.

Le gouvernement a déposé ce projet de loi le 27 juin 2013.

Le "bon à tirer" a été reçu à la Chambre le 2 juillet 2013.

De regering heeft dit wetsontwerp op 27 juni 2013 ingediend.

De "goedkeuring tot drukken" werd op 2 juli 2013 door de Kamer ontvangen.

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
VB	:	*Vlaams Belang*
cdH	:	*centre démocrate Humaniste*
FDF	:	*Fédéralistes Démocrates Francophones*
LDD	:	*Lijst Dedecker*
MLD	:	*Mouvement pour la Liberté et la Démocratie*
INDEP-ONAFH	:	*Indépendant-Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkortingen bij de nummering van de publicaties:*	
DOC 53 0000/000:	*Document parlementaire de la 53e législature, suivi du n° de base et du n° consécutif*	*DOC 53 0000/000:*	*Parlementair document van de 53e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Questions et Réponses écrites*	*QRVA:*	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Version Provisoire du Compte Rendu intégral (couverture verte)*	*CRIV:*	*Voorlopige versie van het Integraal Verslag (groene kaft)*
CRABV:	*Compte Rendu Analytique (couverture bleue)*	*CRABV:*	*Beknopt Verslag (blauwe kaft)*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes) (PLEN: couverture blanche; COM: couverture saumon)*	*CRIV:*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen) (PLEN: witte kaft; COM: zalmkleurige kaft)*
PLEN:	*Séance plénière*	*PLEN:*	*Plenum*
COM:	*Réunion de commission*	*COM:*	*Commissievergadering*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT:*	*Moties tot besluit van interpellaties (beigekleurig papier)*

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

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

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

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Le projet de loi a pour objet de transposer partiellement la directive 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, dite directive "conservation des données" et l'article 15.1 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (dite "directive vie privée et communications électroniques").

Cette directive 2006/24/CE a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

La directive 2006/24/CE aurait dû être transposée en principe pour le 15 septembre 2007, à l'exception de ce qui concerne la conservation des données de communication concernant l'accès à Internet, la téléphonie par Internet et le courrier électronique par Internet, pour lesquels la date butoir de transposition était fixée au 15 mars 2009, la Belgique ayant utilisé la faculté prévue par la directive de demander un report.

Fin septembre 2012, la Commission européenne a mis la Belgique en demeure de transposer la directive et a attiré l'attention de la Belgique sur les sanctions pécuniaires que la Cour de justice pourrait lui infliger pour transposition incomplète de la directive. Il est donc exclu d'attendre encore plus longtemps et, à plus forte raison, d'attendre un amendement éventuel de la directive.

En vue de la transposition en droit belge de la directive 2006/24/CE, il est indispensable de revoir le libellé de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques qui, sur un certain nombre de points, contient des dispositions ne correspondant pas au prescrit européen.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

Het ontwerp van wet heeft als voorwerp de gedeeltelijke omzetting van 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, de zogenaamde "Dataretentierichtlijn" en artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (de zogenaamde "richtlijn betreffende privacy en elektronische communicatie").

Deze Richtlijn 2006/24/EG heeft tot doel de bepalingen van de lidstaten te harmoniseren in verband met de verplichtingen van de aanbieders van openbaar beschikbare elektronische-communicatiediensten of van openbare elektronische-communicatienetwerken wat betreft de bewaring van bepaalde gegevens die door die aanbieders zijn gegenereerd of verwerkt teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.

Richtlijn 2006/24/EG had in principe tegen 15 september 2007 omgezet moeten zijn, met uitzondering van wat betrekking heeft op de bewaring van communicatiegegevens in verband met internettoegang, internettelefonie en e-mail via het internet, waarvoor de streefdatum voor omzetting was vastgesteld op 15 maart 2009, omdat België heeft gebruikgemaakt van de in de richtlijn opgenomen mogelijkheid om uitstel te vragen.

Eind september 2012 heeft de Europese Commissie België in gebreke gesteld om de richtlijn om te zetten en de aandacht van België gevestigd op de geldboetes die het Hof van Justitie aan ons land zou kunnen opleggen wegens de onvolledige omzetting van de richtlijn. Er kan dus zeker niet langer gewacht worden en al zeker niet op een eventuele amendering van de richtlijn.

Met het oog op de omzetting in Belgisch recht van Richtlijn 2006/24/EG is een herziening noodzakelijk van de tekst van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie die hier en daar bepalingen bevat die niet stroken met de Europese bepalingen.

La transposition de la directive 2006/24/CE sera complétée en partie par une modification de l'article 126 de la loi du 13 juin 2005 précitée, et en partie par l'adoption d'un arrêté royal d'exécution de ce nouvel article 126, de telle sorte que la liste des données à conserver et les exigences auxquelles ces données doivent répondre seront fixées par le Roi.

Le projet de loi a été soumis à consultation publique du 27 mai 2008 au 16 juin 2008, puis deux fois pour avis (avis n° 24/2008 du 2 juillet 2008 et avis n° 20/2009 du 1er juillet 2009) à la Commission de la protection de la vie privée, ci-après la CPVP. La note transmise à la CPVP et contenant les éléments de réponse au premier avis n° 24/2008 est jointe en annexe de cet exposé des motifs.

Dans son avis n°20/2009 du 1er juillet 2009, la CPVP donne un avis favorable sur le projet de loi et sur le projet d'arrêté royal d'exécution de l'article 126 de la loi du 13 juin 2005 qui lui ont été communiqués le 23/04/2009, à condition qu'il soit tenu compte de certaines remarques (voir page 14 de l'avis). Il a été tenu compte de toutes ces remarques dans le présent projet et dans le projet d'arrêté royal d'exécution du nouvel article 126.

Le présent projet de loi ne prévoit pas de mécanisme de compensation des coûts des fournisseurs pour la récolte, l'enregistrement, la conservation et la destruction des données. Ces opérations sont donc à charge des fournisseurs.Les coûts de stockage ne représentent qu'une très petite partie de l'ensemble des coûts qu'exposent les fournisseurs dans le cadre de l'identification et de l'interception légale. De plus, grâce au progrès technologique, les coûts de l'équipement nécessaire pour le stockage diminueront sensiblement d'année en année.

Par contre, des indemnités par réquisition sur la base de l'article 46*bis* et de l'article 88*bis* du Code d'instruction criminelle figurent actuellement à l'annexe de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques. Cet arrêté royal vise la communication aux autorités judiciaires tant des données qui sont conservées en vertu du présent projet de loi et de l'arrêté d'exécution de l'article 126 que des données qui ne sont pas conservées en vertu de ces législations. Les indemnités susmentionnées visent à rembourser aux fournisseurs certains coûts relatifs à la recherche

De omzetting van Richtlijn 2006/24/EG zal deels aan de hand van een wijziging van artikel 126 van de voornoemde wet van 13 juni 2005 voltooid worden en deels door de aanneming van een koninklijk besluit ter uitvoering van dat nieuwe artikel 126, zodat de lijst van te bewaren gegevens en de vereisten waaraan deze gegevens moeten beantwoorden, zullen worden vastgelegd door de Koning.

Het ontwerp van wet werd voor openbare raadpleging voorgelegd van 27 mei 2008 tot 16 juni 2008, en vervolgens ook tweemaal voor advies (advies nr. 24/2008 van 2 juli 2008 en advies nr. 20/2009 van 1 juli 2009) aan de Commissie voor de bescherming van de persoonlijke levenssfeer, hierna de CBPL. In de bijlage bij deze memorie werd de nota opgenomen die aan de CBPL werd overgemaakt met de elementen van antwoord op het eerste advies nr. 24/2008.

In haar advies nr. 20/2009 van 1 juli 2009 geeft de CBPL een gunstig advies over het ontwerp van wet en het ontwerp van koninklijk besluit tot uitvoering van artikel 126 van de wet van 13 juni 2005 die haar werden toegestuurd op 23/04/2009, op voorwaarde dat rekening wordt gehouden met bepaalde opmerkingen (zie bladzijde 14 van het advies). Er werd met al deze opmerkingen rekening gehouden in dit ontwerp en in het ontwerp van koninklijk besluit tot uitvoering van het nieuwe artikel 126.

Dit ontwerp van wet voorziet niet in een compensatiemechanisme voor de kosten van de aanbieders voor de inzameling, registratie, bewaring en vernietiging van de gegevens. Deze verrichtingen zijn dus ten laste van de aanbieders. De kosten voor opslag vertegenwoordigen slechts een heel klein deel van alle kosten waaraan de aanbieders worden blootgesteld in het kader van de identificatie en de wettelijke onderschepping. Dankzij de technologische vooruitgang zullen de kosten voor de nodige apparatuur overigens beduidend dalen van jaar tot jaar.

Daarentegen worden momenteel in de bijlage bij het koninklijk besluit van 9 januari 2003 houdende de nadere regels voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie vergoedingen per vordering vermeld op grond van artikel 46*bis* en artikel 88*bis* van het Wetboek van Strafvordering wel vorderbare. Dat koninklijk besluit beoogt de mededeling aan de gerechtelijke autoriteiten van zowel de gegevens die worden bewaard krachtens het onderhavige ontwerp van wet en het besluit tot uitvoering van artikel 126 als de gegevens die niet worden bewaard krachtens deze wetgevingen. De voormelde vergoedingen zijn bedoeld als compensatie voor de

de données et à la communication de données aux autorités judiciaires.

L'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité permet également aux fournisseurs de recevoir certaines indemnités. L'article 7 de cet arrêté royal prévoit en effet que "Pour l'application de l'article 18/18 de la loi du 30 novembre 1998, la collaboration des opérateurs d'un réseau de communications électroniques et des fournisseurs d'un service de communications électroniques est soumise aux tarifs définis par l'arrêté royal du 9 janvier 2003".

Selon le rapport de la Commission au Conseil et au Parlement européen (Rapport d'évaluation concernant la directive 2006/24/CE sur la conservation des données, n° COM (2011) 225 final), "la directive ne régit pas le remboursement des coûts supportés par les opérateurs du fait de l'obligation de conservation des données" (page 31 du rapport). Il s'agit donc d'une question qui doit être tranchée par les États membres. Selon ce même rapport, "tous les États membres prévoient une forme de remboursement lorsque les données sont demandées dans le cadre d'une procédure pénale devant un tribunal". En Belgique, les fournisseurs obtiennent une forme de remboursement sur base des tarifs en annexe de l'arrêté royal du 9 janvier 2003 précité.

L'avis 53.272/4 du Conseil d'État du 27 mai 2013 a été suivi, à l'exception de quelques points faisant l'objet de la justification suivante.

Le Consel d'État suggère une législation parallèle.

Le présent projet ne met pas en place les deux systèmes parallèles suggérés par le Conseil d'État, soit un système transposant la directive 2006/24/CE et un autre s'appuyant sur la directive 2002/58/CE, dès lors que cela compliquerait fortement la tâche des fournisseurs qui devraient combiner l'application de deux législations, sans doute parallèles mais pas nécessairement identiques. En pratique, les données sont conservées dans des bases de données. Cependant, avec deux systèmes parallèles, la base de données se rattachant à la directive 2002/58/CE devrait tout de même contenir certaines données se trouvant dans la base de données se rattachant à la directive 2006/24/CE, dès lors que certaines données ne peuvent être exploitées que lorsqu'elles sont reliées à d'autres données.

aanbieders van bepaalde kosten inzake de opzoeking van gegevens en mededeling van gegevens aan de gerechtelijke autoriteiten.

Het koninklijk besluit van 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie zorgt er ook voor dat de aanbieders bepaalde vergoedingen kunnen ontvangen. Artikel 7 van dat koninklijk besluit luidt inderdaad als volgt: "Voor de toepassing van artikel 18/18 van de wet van 30 november 1998 wordt de medewerking van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronische communicatiedienst vergoed volgens de tarieven bepaald in het koninklijk besluit van 9 januari 2003."

In het verslag van de Commissie aan de Raad en het Europees Parlement (Evaluatieverslag betreffende Richtlijn 2006/24/EG inzake gegevensbewaring, nr. COM (2011) 225 definitief), staat te lezen: "De vergoeding van de kosten die exploitanten moeten maken als gevolg van de verplichting om gegevens te bewaren, wordt niet door de richtlijn geregeld" (pagina 31 van het verslag). Deze kwestie moet dus worden geregeld door de lidstaten. Datzelfde verslag luidt verder: "Alle lidstaten kennen een of andere vorm van vergoeding indien de gegevens worden opgevraagd in het kader van een strafprocedure". In België ontvangen de aanbieders een vorm van vergoeding op basis van de tarieven in de bijlage bij het voormelde koninklijk besluit van 9 januari 2003.

Advies 53.272/4 van de Raad van State van 27 mei 2013 werd gevolgd, afgezien van een paar punten waarvan hierna de verantwoording volgt.

De Raad van State stelt een parallelle wetgeving voor.

Dit ontwerp stelt niet de twee parallelle systemen in die de Raad van State voorstelt, namelijk een systeem dat Richtlijn 2006/24/EG omzet en een ander dat steunt op Richtlijn 2002/58/EG, omdat dit de taak van de aanbieders heel wat complexer zou maken; deze laatsten zouden de toepassing moeten combineren van twee wetgevingen, die weliswaar gelijklopend zijn, maar niet noodzakelijk identiek. In de praktijk worden de gegevens bewaard in databanken. Met twee parallelle systemen zou de databank die verband houdt met Richtlijn 2002/58/EG echter toch bepaalde gegevens moeten bevatten die terug te vinden zijn in de databank die verband houdt met Richtlijn 2006/24/EG, aangezien sommige gegevens pas kunnen worden geëxploiteerd wanneer ze aan andere gegevens gekoppeld zijn.

Mettre en place deux systèmes parallèles impliquerait donc une duplication des données et nécessiterait dans la pratique que certaines données d'une base de données soient introduites dans l'autre.

Cependant, afin de tenir compte de l'observation du Conseil d'État, le tableau de transposition indique les dispositions qui transposent la directive 2002/58/CE et celles qui transposent la directive 2006/24/CE.

Pour ce qui concerne les données conservées qui sont transmises aux services d'urgence et au service de médiation, le Conseil d'État estime que le législateur devrait indiquer le bénéficiaire de ces données et les éléments essentiels des modalités de demande et de transmission de ces données.

Or, s'agissant des services d'urgence, la loi fédérale définit déjà les bénéficiaires des données ainsi que les éléments essentiels des modalités de demande et de transmission de ces données. L'article 107, § 1er, de la loi du 13 juin 2005 précitée définit ce qu'il faut entendre par services d'urgence. Selon l'article 107, § 2, de la même loi, c'est aux centrales de gestion de ces services d'urgence que les données conservées doivent être fournies. Ce même article définit également les données que les opérateurs doivent leur fournir, soit les données d'identification de l'appelant (voir définition à l'article 2, 57°, de la même loi) pour ce qui concerne les services d'urgence offrant de l'aide sur place et l'identification de la ligne appelante (voir article 2, 56°, de la même loi) pour ce qui concerne les services d'urgence offrant de l'aide à distance. Pour pouvoir fournir ces données aux services d'urgence, les opérateurs doivent puiser dans leur base de données des données conservées.

Enfin, en vertu de la législation, les services d'urgence ne doivent pas demander aux opérateurs les données susmentionnées mais ces dernières doivent leur être fournies automatiquement au moment où l'opérateur délivre l'appel d'urgence, c.-à-d. un appel vers un numéro d'urgence, à la centrale de gestion des appels d'urgence.

De même, s'agissant du service de médiation, des précisions similaires sont apportées par la législation fédérale. Outre les conditions de recevabilité applicables à toutes plaintes introduites auprès de ce service, l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques précise quand ce service doit investiguer une plainte d'utilisation malveillante d'un réseau ou d'un service de communications électroniques (à savoir quand les faits semblent établis et lorsque la demande se rapporte à des dates et heures précises). Pour le

Twee paralelle systemen instellen zou dus een verdubbeling van de gegevens impliceren en in de praktijk ertoe nopen dat bepaalde gegevens van de ene databank worden ingevoerd in de andere.

Om echter rekening te houden met de opmerking van de Raad van State vermeldt de omzettingstabel de bepalingen die Richtlijn 2002/58/EG omzetten en diegene die Richtlijn 2006/24/EG omzetten.

Wat betreft de bewaarde gegevens die worden overgezonden naar de nooddiensten en naar de ombudsdienst, is de Raad van State van oordeel dat de wetgever de begunstigde van die gegevens zou moeten vermelden alsook de essentiële elementen van de werkwijze voor de opvraging en overzending van die gegevens.

Welnu, wat de nooddiensten betreft, definieert de federale wet reeds de begunstigden van de gegevens, alsook de essentiële elementen van de werkwijze voor de opvraging en overzending van die gegevens. Artikel 107, § 1, van de voormelde wet van 13 juni 2005 definieert wat moet worden verstaan onder nooddiensten. Volgens artikel 107, § 2, van dezelfde wet, moeten de bewaarde gegevens worden verstrekt aan de beheerscentrales van die nooddiensten. Datzelfde artikel definieert ook de gegevens die de operatoren daaraan moeten verstrekken, namelijk de identificatiegegevens van de oproeper (zie definitie in artikel 2, 57°, van dezelfde wet) wat betreft de nooddiensten die ter plaatse hulp bieden en de identificatie van de oproepende lijn (zie artikel 2, 56° van dezelfde wet) wat betreft de nooddiensten die op een afstand hulp bieden. Om deze gegevens aan de nooddiensten te kunnen verstrekken, moeten de operatoren de bewaarde gegevens uit hun databank putten.

Krachtens de wetgeving ten slotte, moeten de nooddiensten de voormelde gegevens niet aan de operatoren vragen, maar moeten ze automatisch door deze laatsten worden verstrekt op het ogenblik dat de operator de noodoproep, t.t.z. een oproep naar een noodnummer, aflevert bij de beheerscentrale voor noodoproepen.

Wat de ombudsdienst betreft worden eveneens soortgelijke verduidelijkingen aangebracht door de federale wetgeving. Buiten de voorwaarden voor ontvankelijkheid die gelden voor alle klachten die bij deze dienst worden ingediend, preciseert artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven wanneer deze dienst een klacht over het kwaadwillige gebruik van een netwerk of dienst voor elektronische communicatie moet onderzoeken (namelijk wanneer de feiten lijken vast te staan en het verzoek betrekking heeft op precieze data

traitement de ces plaintes, le Service de médiation ne demandera à un opérateur que les données nécessaires pour évaluer le fondement de la plainte.

Le Conseil d'État se demande si la répression des appels malveillants (point b) de l'article 126, § 2, de la loi du 13 juin 2005 précitée) n'est déjà pas couverte par la recherche, l'instruction, et la poursuite des infractions pénales (point a) de l'article 126, § 2, de la loi du 13 juin 2005 précitée).

L'article 107, § 2, alinéa 5, de la même loi prévoit que les données d'identification par les centrales de gestion des appels d'urgence peuvent être utilisées par les systèmes qui sont mis place par les services d'urgence en question pour lutter contre les appels malveillants. Le but de ces systèmes est de dissuader les appelants d'effectuer de nouveaux appels malveillants. Ce n'est que lorsqu'un appelant effectue des appels malveillants de manière répétée et fréquente que les services d'urgence prendront des mesures allant jusqu'à une procédure judiciaire. Lancer une procédure judiciaire pour chaque appel malveillant entraînerait une surcharge de travail pour les instances judiciaires et manquerait à terme son but. Dans ce sens, la disposition du point b) du projet d'article 126, § 2, n'est que partiellement couverte par la disposition du point a) du projet d'article 126, § 2.

Le Service de médiation pour les télécommunications ne peut jamais communiquer au plaignant les données fournies par l'opérateur à sa demande, toutefois il renverra ce dernier à cet effet aux services judiciaires dans le but d'introduire une plainte formelle qui suivra alors les procédures judiciaires. La procédure de plaintes auprès du Service de médiation pour les télécommunications fait en sorte qu'un grand nombre de plaintes en matière de télécommunications peuvent être réglées à l'amiable, permettant ainsi de décharger les services judiciaires.

Le Conseil d'État se demande si le système mis en place pour calculer le point de départ du délai de conservation pour les données d'identification (article 126, § 3, alinéa 1er de la loi du 13 juin 2005 précitée) ne dépasse pas, dans certaines hypothèses, le délai maximum qui résulte des articles 5 et 6 de la directive 2006/24/CE.

À cet égard, les fournisseurs soumis à l'obligation de conservation de données doivent conserver les données d'identification aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit. Ainsi qu'illustré ci-après (voir point 3 ci-après, "Données à conserver"), dans la pratique, une communication est parfois encore possible après la fin de l'abonnement ou, lorsqu'un abonnement n'a pas été

en uren). Voor het behandelen van deze klachten zal de ombudsdienst slechts deze gegevens opvragen bij een operator die nodig zijn om de grond van de klacht te kunnen beoordelen.

De Raad van State vraagt zich af of de beteugeling van kwaadwillige oproepen (punt b) van artikel 126, § 2, van de voormelde wet van 13 juni 2005) niet reeds gedekt is door de opsporing, het onderzoek en de vervolging van de strafbare feiten (punt a) van artikel 126, § 2, van de voormelde wet van 13 juni 2005).

Artikel 107, § 2, vijfde lid, van dezelfde wet bepaalt dat de identificatiegegevens door de beheerscentrales van noodoproepen mogen worden gebruikt door systemen die door de betrokken nooddiensten worden in werking gesteld om kwaadwillige oproepen te bestrijden. Het doel van deze systemen bestaat erin om de oproepers af te raden om opnieuw kwaadwillige oproepen tot stand te brengen. Het is pas wanneer een oproeper bij herhaling en frequent kwaadwillige oproepen pleegt dat de nooddiensten zullen escaleren naar een gerechtelijke procedure. Voor elke kwaadwillige oproep een gerechtelijke procedure opstarten zou de gerechtelijke instanties overbelasten en zou op termijn zijn effect missen. In die zin is de bepaling onder b) van het ontwerp van artikel 126, § 2, slechts ten dele gedekt door de bepaling onder a) van het ontwerp van artikel 126, § 2.

De Ombudsdienst voor telecommunicatie mag nooit de door de operator als antwoord op zijn vraag geleverde gegevens aan de klager meedelen, doch zal deze daarvoor doorverwijzen naar de gerechtelijke diensten om een formele klacht in te dienen die dan de gerechtelijke procedures zal volgen. De klachtenprocedure bij de Ombudsdienst voor telecommunicatie zorgt er voor dat een heel aantal klachten in verband met telecommunicatie in der minne kunnen geregeld worden waardoor de gerechtelijke diensten ontlast worden.

De Raad van State vraagt zich af of het systeem dat wordt ingesteld voor de berekening van het beginpunt van de termijn voor de bewaring van de identificatiegegevens (artikel 126, § 3, eerste lid, van de voormelde wet van 13 juni 2005) in sommige hypotheses niet de maximumtermijn overschrijdt die voortvloeit uit de artikelen 5 en 6 van Richtlijn 2006/24/EG.

Daarbij moeten de aanbieders die verplicht zijn om gegevens te bewaren, de identificatiegegevens bewaren, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend. Zoals hieronder wordt geïllustreerd (zie punt 3 hierna, "Te bewaren gegevens") is in de praktijk communicatie soms nog mogelijk na het einde van het abonnement of wanneer er geen abonnement is

contracté, après la fin de la durée de validité du service. D'un point de vue théorique, si c'est encore possible plus de 12 mois après la fin de l'abonnement ou de la durée de validité du service, un délai de 24 mois, soit le délai maximum prévu par la directive directive 2006/24/CE, calculé à compter de la fin de l'abonnement ou de la durée de validité du service, pourrait être dépassé. Cependant, en pratique, une communication sera parfois encore possible quelques semaines après la fin de l'abonnement ou de la durée de validité du service, voire quelques mois, mais pas pendant une durée supérieure à 12 mois.

Le Conseil d'État estime que l'article 7, d), de la directive 2006/24/CE prévoit que les fournisseurs, à l'issue de l'expiration du délai de conservation, doivent détruire les données conservées à "l'exception des données auxquelles on a pu accéder et qui ont été préservées".

Des problèmes se poseraient cependant si les fournisseurs devaient continuer à converser les données transmises aux autorités au-delà de l'expiration du délai de conservation. En effet, la directive n'indique pas quand les fournisseurs doivent supprimer ces données. Cela supposerait donc que l'autorité concernée indique au fournisseur concerné, pour chaque donnée transmise, quand la donnée peut être détruite, ce qui risque de créer une charge administrative tant pour les autorités que pour les fournisseurs. Vu la longueur de certaines poursuites pénales, cela signifierait que ces fournisseurs devraient conserver ces données des années avant de pouvoir les détruire. En outre, la conservation prolongée des données par les fournisseurs indique qu'une procédure judiciaire est en cours, alors que les fournisseurs n'ont pas à connaître les suites réservées, par exemple, à une enquête pénale.

Il n'est pas indispensable que les fournisseurs conservent les données transmises aux autorités après l'expiration du délai de conservation. En effet, il revient à ces dernières de conserver ces données aussi longtemps que nécessaire.

Selon le Conseil d'État, afin d'assurer une transposition correcte de la directive 2006/24/CE, le projet doit prévoir que l'accès aux données conservées ne peut être effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice.

L'article 7, c, de la directive prévoit que les États membres doivent veiller à ce que les fournisseurs prennent les mesures techniques et organisationnelles appropriées afin de garantir que "l'accès aux données n'est effectué que par un personnel spécifiquement

genomen, na het einde van de geldigheidsduur van de dienst. Vanuit theoretisch oogpunt, indien dat nog mogelijk is meer dan 12 maanden na afloop van het abonnement of van de geldigheidsduur van de dienst, zou een termijn van 24 maanden kunnen worden overschreden, namelijk de maximale termijn die vastgesteld is in Richtlijn 2006/24/EG, berekend vanaf het einde van het abonnement of van de geldigheidsduur van de dienst. In de praktijk is communicatie echter soms nog mogelijk enkele weken en zelfs enkele maanden na afloop van het abonnement of van de geldigheidsduur van de dienst, maar niet gedurende een periode van meer dan 12 maanden.

De Raad van State is van oordeel dat artikel 7, d), van Richtlijn 2006/24/EG bepaalt dat de aanbieders, nadat de bewaringstermijn verstreken is, de bewaarde gegevens moeten vernietigen "met uitzondering van de geraadpleegde en vastgelegde gegevens".

Er zouden dan echter problemen rijzen indien de aanbieders de aan de autoriteiten overgezonden gegevens zouden blijven bewaren tot na afloop van de bewaringstermijn. De richtlijn geeft immers niet aan wanneer de aanbieders deze gegevens moeten vernietigen. Dit zou dus veronderstellen dat de betrokken autoriteit aan de betrokken aanbieder voor elk overgezonden gegeven laat weten wanneer het gegeven mag worden vernietigd, hetgeen een administratieve belasting dreigt te creëren, zowel voor de autoriteiten als voor de aanbieders. Wegens de lange duur van sommige strafrechtelijke vervolgingen zou dat betekenen dat deze aanbieders deze gegevens jarenlang zouden moeten bewaren, voordat ze die mogen vernietigen. Bovendien wijst de verlengde bewaring van gegevens door de aanbieders op een lopende gerechtelijke procedure, terwijl de aanbieders het gevolg dat bijvoorbeeld aan een strafrechtelijk onderzoek is gegeven, niet hoeven te weten.

Het is niet absoluut noodzakelijk dat de aanbieders de aan de autoriteiten overgezonden gegevens bewaren nadat de bewaringstermijn verstreken is. Het is immers de taak van deze laatste om die gegevens te bewaren zolang dat nodig is.

Om Richtlijn 2006/24/EG correct om te zetten, moet volgens de Raad van State het ontwerp voorschrijven dat de toegang tot de bewaarde gegevens enkel mogelijk is voor een of meer leden van de Coördinatiecel Justitie.

Artikel 7, c, van de richtlijn bepaalt dat de lidstaten erop moeten toezien dat de aanbieders passende technische en organisatorische maatregelen nemen om te waarborgen dat "toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen".

autorisé". La directive ne définit cependant pas ce qu'il faut entendre précisément par "personnel spécifiquement autorisé". Il revient donc aux États membres de définir le contenu de cette expression. En pratique, il n'est pas réaliste de limiter l'accès aux données conservées aux seuls membres de la Cellule de coordination de la Justice. En effet, une aide du personnel technique est souvent indispensable pour qu'elle puisse répondre aux demandes des autorités. Ceci a d'ailleurs été reconnu dans l'article 2, § 4, de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, qui prévoit que "Pour l'exécution de sa mission de collaboration, la Cellule de coordination de la Justice peut, sous sa surveillance, se faire aider par des agents et des préposés de l'opérateur d'un réseau de communications électroniques ou fournisseur d'un service de communications électroniques concerné." Pour répondre au prescrit de la directive, ce personnel technique doit cependant être spécifiquement autorisé. En droit belge, c'est la Cellule coordination de la Justice qui doit donner cette autorisation.

COMMENTAIRE DES ARTICLES

CHAPITRE 1er

Objet

L'article 15.1 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (dite "directive vie privée et communications électroniques") permet aux États membres d'adopter des mesures réglementaires prévoyant la conservation de données pendant une durée limitée lorsque c'est justifié par un des motifs énumérés dans cet article. À cet égard, le considérant 12 de la directive 2006/24/CE prévoit que "l'article 15, paragraphe 1er, de la directive 2002/58/CE continue à s'appliquer aux données, y compris à celles relatives aux appels téléphoniques infructueux, dont la conservation n'est pas expressément requise par la présente directive et qui ne relèvent donc pas de son champ d'application, ainsi qu'à la conservation de données à d'autres fins que celles prévues par la présente directive, notamment à des fins judiciaires."

Dès lors que le présent projet de loi prévoit des finalités de conservation supplémentaires à celles prévues par la directive 2006/24/CE, il se base également sur l'article 15.1 de la directive 2002/58/CE.

De richtlijn definieert echter niet wat juist moet worden verstaan onder "speciaal daartoe bevoegde personen". Het komt dus aan de lidstaten toe om de inhoud van die woorden, vast te stellen. In de praktijk is het niet realistisch om de toegang tot de bewaarde gegevens enkel te beperken tot de leden van de Coördinatiecel Justitie. Er is immers vaak hulp nodig van het technische personeel om te kunnen voldoen aan de verzoeken van de autoriteiten. Dit wordt trouwens erkend in artikel 2, § 4, van het koninklijk besluit van 9 januari 2003 houdende de nadere regels voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, dat bepaalt: "Voor de uitvoering van de medewerking en onder zijn toezicht kan de Coördinatiecel Justitie gebruik maken van de hulp van personeelsleden en aangestelden van de betrokken operator van een elektronisch communicatienetwerk of verstrekker van een elektronische communicatiedienst." Om te voldoen aan wat de richtlijn voorschrijft, moet dat technische personeel evenwel speciaal bevoegd worden. In het Belgische recht moet die bevoegdheid worden verleend door de Coördinatiecel Justitie.

ARTIKELSGEWIJZE TOELICHTING

HOOFDSTUK 1

Doel

Artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (hierna "richtlijn betreffende privacy en elektronische communicatie") stelt de lidstaten in staat om bestuursrechtelijke bepalingen aan te nemen die voorzien in de bewaring van gegevens gedurende een beperkte periode, wanneer dat gerechtvaardigd is door een van de redenen die in dat artikel worden opgesomd. In dat opzicht luidt considerans 12 van Richtlijn 2006/24/EG als volgt: "Artikel 15, lid 1, van Richtlijn 2002/58/EG blijft van toepassing op gegevens, met inbegrip van gegevens met betrekking tot oproeppogingen zonder resultaat, die ingevolge de huidige richtlijn niet specifiek moeten worden bewaard en derhalve niet onder het toepassingsgebied daarvan, alsook voor bewaring van gegevens voor doelstellingen, inclusief van justitiële aard, andere dan die welke onder deze richtlijn vallen."

Omdat het onderhavige ontwerp van wet extra doeleinden vaststelt voor de bewaring buiten diegene waarin Richtlijn 2006/24/EG voorziet, is het eveneens gebaseerd op artikel 15.1 van Richtlijn 2002/58/EG.

CHAPITRE 2

Modification de la loi du 13 juin 2005 relative aux communications electroniques

Art. 2

Cet article comporte la référence obligatoire auxa directives transposées et n'appelle pas de commentaire.

Art. 3

Cet article remplace la définition de la notion d'"opérateur" à l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques.

La définition actuelle de la notion d'opérateur n'est pas acceptable dans la pratique car elle offre une échappatoire, en ce sens que les personnes qui n'introduiraient pas de notification à l'Institut belge des services postaux et des télécommunications (ci-après "IBPT") alors qu'elles ont l'obligation de le faire en vertu de l'article 9, § 1er, de la loi précitée, ne seraient pas soumises à la loi du 13 juin 2005 relative aux communications électroniques. Avec la nouvelle définition d'opérateur, les personnes qui auraient omis d'introduire une déclaration à l'IBPT comme opérateurs ne peuvent plus invoquer cette échappatoire: elles doivent respecter les obligations, même en l'absence de notification à l'IBPT.

Art. 4

La définition d'appel infructueux constitue une transposition d'un concept défini dans l'article 2.2, f), de la directive 2006/24/CE. Cette directive vise les appels téléphoniques infructueux, alors que le présent projet retient la notion d'appels infructueux. Le mot "téléphonique" est devenu superflu depuis la nouvelle définition de l'appel introduite dans la loi du 13 juin 2005 relative aux communications électroniques à l'occasion de la transposition du paquet télécoms européen de 2009. L'article 2, 22/1°, de la loi du 13 juin 2005 précitée, définit l'appel comme "une connexion établie au moyen d'un service de communications électroniques accessible au public permettant une communication vocale bidirectionnelle", de sorte qu'il va de soi qu'il s'agit d'une communication par téléphone. Un spam n'étant pas une communication vocale bidirectionnelle, il ne constitue donc pas un appel infructueux. Les spams ne doivent être conservés que lorsqu'ils sont parvenus dans la boite e-mail de l'utilisateur final, sous quelque rubrique que ce soit. Ceci incitera les opérateurs à améliorer les filtres anti-spams.

HOOFSTUK 2

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

Art. 2

Dit artikel bevat de verplichte verwijzing naar de omgezette richtlijnen en behoeft geen commentaar.

Art. 3

Dit artikel vervangt de definitie van het begrip "operator" in artikel 2, 11°, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

De huidige definitie van het begrip "operator" is niet aanvaardbaar in de praktijk omdat ze een achterpoortje openlaat, in die zin dat personen die geen kennisgeving zouden doen aan het Belgisch Instituut voor postdiensten en telecommunicatie (hierna het BIPT), terwijl ze daartoe verplicht zijn krachtens artikel 9, § 1, van de voormelde wet, niet zouden worden onderworpen aan de wet van 13 juni 2005 betreffende de elektronische communicatie. Met de nieuwe definitie van operator kunnen personen die zouden hebben verzuimd aan het BIPT een aangifte te doen als operator, niet langer van dat achterpoortje gebruikmaken: zij moeten de verplichtingen vervullen, zelfs zonder kennisgeving aan het BIPT te hebben gedaan.

Art. 4

De definitie van oproeppoging zonder resultaat vormt een omzetting van een begrip dat gedefinieerd is in artikel 2.2, f), van Richtlijn 2006/24/EG. Deze richtlijn is gericht op telefoonoproepen zonder resultaat, terwijl het onderhavige besluit het heeft over oproeppogingen zonder resultaat. Het woord "telefoon" is overbodig geworden sedert de nieuwe definitie van oproep die ingevoerd is in de wet van 13 juni 2005 betreffende de elektronische communicatie bij de omzetting van het Europese telecompakket uit 2009. Artikel 2, 22/1°, van de WEC, definieert een oproep als "door middel van een openbaar beschikbare elektronische-communicatiedienst tot stand gebrachte verbinding die tweewegspraakcommunicatie mogelijk maakt", zodat het vanzelfsprekend is dat het om een telefoongesprek gaat. Omdat een spambericht geen bidirectioneel spraakbericht is, vormt dit dus geen oproeppoging zonder resultaat. Spamberichten moeten maar worden bewaard als ze terechtgekomen zijn in de mailbox van de eindgebruiker, onder gelijk welke rubriek. Dit zal de operatoren ertoe aansporen om de antispamfilters te verbeteren.

Art. 5

Cet article remplace l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.

Le nouveau paragraphe 1er de l'article 126 fait le lien avec la législation générale en matière de protection de la vie privée, indique les catégories d'entreprises tenues de conserver des données et indique les catégories de données à conserver.

1) *Lien avec la législation générale en matière de protection de la vie privée*

Une refonte de l'article 126 de la loi du 13 juin 2005 est susceptible de fournir une base légale adéquate à la mise en place d'instruments contribuant aux moyens d'investigation mis à la disposition des bénéficiaires de la conservation des données.

Toutefois, ceci ne peut se faire au détriment d'une protection efficace de la vie privée des personnes dont les données sont conservées par les fournisseurs de réseaux et de services de communications électroniques.

Ainsi, on notera que l'article 126 nouveau s'applique sans préjudice des dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ce que l'ancienne mouture de l'article 126 ne mentionnait pas.

Dès lors, les fournisseurs sont explicitement tenus de respecter l'ensemble des dispositions de la loi du 8 décembre 1992 et de son arrêté d'exécution du 13 février 2001, en ce qui concerne notamment la qualité des données (exactitude, mise à jour, conservation sous une forme permettant l'identification des personnes concernées, *etc*.), les obligations du responsable de traitement (confidentialité, mesures techniques et organisationnelles, sous-traitance, *etc*.), et les droits de la personne concernée. Cette dernière conserve bien entendu ses droits: elle devra être informée par les fournisseurs de la conservation de ses données pendant une période maximale de 12 mois, elle pourra accéder à ses données et pourra, le cas échéant, les faire rectifier, le tout sans préjudice d'une plainte devant la CPVP ou d'une requête devant le Président du Tribunal de Première Instance. Il va de soi que la personne concernée ne peut accéder qu'à ses données personnelles et pas aux données des autres personnes.

Art. 5

Dit artikel vervangt artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

De nieuwe paragraaf 1 van artikel 126 legt het verband met de algemene wetgeving inzake de bescherming van de persoonlijke levenssfeer, duidt de categorieën van ondernemingen aan die verplicht zijn tot gegevensbewaring alsook de categorieën van gegevens die moeten worden bewaard.

1) *Verband met de algemene wetgeving inzake de bescherming van de persoonlijke levenssfeer*

Een herziening van artikel 126 van de wet van 13 juni 2005 kan een geschikte wettelijke basis leveren voor het invoeren van instrumenten die bijdragen tot de onderzoeksmiddelen die ter beschikking worden gesteld van de begunstigden van de gegevensbewaring.

Dit mag echter geen afbreuk doen aan een doeltreffende bescherming van de persoonlijke levenssfeer van personen van wie de gegevens worden bewaard door de aanbieders van elektronische-communicatienetwerken en diensten.

Zo wordt opgemerkt dat het nieuwe artikel 126 van toepassing is onverminderd de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, wat het oude artikel 126 niet vermeldde.

Daarom zijn de aanbieders uitdrukkelijk verplicht alle bepalingen van de wet van 8 december 1992 en het bijbehorende uitvoeringsbesluit van 13 februari 2001 na te leven, meer bepaald wat betreft de kwaliteit van de gegevens (nauwkeurigheid, bijwerking, bewaring op een manier die het mogelijk maakt de betrokken personen te identificeren, enz.), de verplichtingen van de persoon die verantwoordelijk is voor de verwerking (vertrouwelijkheid, technische en organisatorische maatregelen, uitbesteding, enz.), en de rechten van de betrokken persoon. Deze laatste behoudt uiteraard zijn rechten: de aanbieders dienen deze persoon op de hoogte te brengen van de bewaring van zijn gegevens gedurende maximaal 12 maanden, de persoon dient zijn gegevens te kunnen inzien en, indien nodig, deze te laten rechtzetten, dit alles onverminderd een klacht bij de CBPL of een verzoek aan de voorzitter van de rechtbank van eerste aanleg. Het spreekt vanzelf dat de betrokken persoon slechts zijn persoonlijke gegevens kan inkijken en niet de gegevens van andere personen.

2) *Les entreprises tenues de conserver des données*

La directive 2006/24/CE établit le cadre général de la conservation des données relatives aux communications électroniques. Seules cinq catégories de services de communications électroniques accessibles au public sont visées à l'article 5 de la directive: la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, la messagerie électronique (e-mail) et la téléphonie via l'internet.

Ces catégories sont également explicitement énumérées au projet de l'article 126, afin qu'il soit clair quels fournisseurs sont soumis à l'obligation de conservation des données.

Le paragraphe 1er vise différents services de téléphonie et non des services téléphoniques. Cette différence de terminologie s'explique par le fait que l'article 2, c), de la directive 2006/24/CE donne une définition de "service téléphonique" qui ne correspond pas à la définition de "service téléphonique accessible au public" au sens de l'article 2, 22°, de la loi du 13 juin 2005 relative aux communications électroniques. Une terminologie différente (service de téléphonie et non service téléphonique) est ainsi utilisée dans l'article 126 pour éviter un conflit avec la définition de "service téléphonique accessible au public" à l'article 2, 22° précité.

Le paragraphe 1er vise certaines catégories de fournisseurs de services dont certains sont opérateurs au sens de la loi du 13 juin 2005 relative aux communications électroniques, et d'autres, non, afin d'assurer une transposition correcte de la directive 2006/24/CE. Ainsi, par exemple, le courrier électronique par l'internet est visé à plusieurs endroits au sein de l'article 5 de la directive. Pour assurer une transposition correcte de cet article de la directive, le paragraphe 1er de l'article 126 inclut également les fournisseurs au public de service de courrier électronique par internet. Or le courrier électronique par l'internet n'entre pas dans le champ d'application de la définition du service de communications électroniques (art. 2, 5° de la loi du 13 juin 2005) car ce service ne consiste pas à transmettre des signaux mais à fournir, à l'aide de réseaux et services de communications électroniques, du contenu transmis. En incluant les fournisseurs au public de service de courrier électronique par l'internet, le paragraphe 1er de l'article 126 inclut donc des fournisseurs de service qui ne sont pas opérateurs au sens de la loi du 13 juin 2005 relative aux communications électroniques.

Le paragraphe 1er vise également les fournisseurs de réseaux publics de communications électroniques tout comme l'article 3, §§ 1er et 2, de la directive 2006/24/CE.

2) *De ondernemingen die verplicht zijn tot gegevensbewaring*

Richtlijn 2006/24/EG legt het algemene kader voor de gegevensbewaring betreffende elektronische communicatie vast. Slechts vijf categorieën van openbaar beschikbare elektronische-communicatiediensten worden beoogd door artikel 5 van de richtlijn: vaste telefonie, mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie.

Deze categorieën worden ook uitdrukkelijk in het ontwerp van artikel 126 opgesomd, zodat duidelijk is welke aanbieders onderworpen zijn aan de verplichting tot bewaring van de gegevens.

Paragraaf 1 beoogt verschillende telefoniediensten en niet telefoondiensten. Dit verschil in terminologie wordt verklaard door het feit dat artikel 2, c) van Richtlijn 2006/24/EG een definitie geeft van "telefoondienst" die niet overeenstemt met de definitie van een "openbare telefoondienst" zoals bepaald in artikel 2, 22°, van de wet van 13 juni 2005 betreffende de elektronische communicatie. Aldus wordt in artikel 126 een verschillende terminologie (telefoniedienst en niet telefoondienst) gebruikt om een conflict met de definitie van "openbare telefoondienst" in het voormelde artikel 2, 22° te vermijden.

De eerste paragraaf beoogt bepaalde categorieën van dienstenaanbieders, waarvan sommigen operator zijn in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, en anderen niet, om te zorgen voor een correcte omzetting van Richtlijn 2006/24/EG. Zo wordt de e-maildienst over het internet bijvoorbeeld beoogd op verschillende plaatsen binnen artikel 5 van de richtlijn. Om dit artikel van de richtlijn correct om te zetten, omvat paragraaf 1 van artikel 126 ook de aanbieders van aan het publiek aangeboden e-maildiensten over het internet. Nu valt de e-maildienst over het internet niet binnen het toepassingsgebied van de definitie van de elektronische-communicatiedienst (art. 2, 5°, van de wet van 13 juni 2005) omdat deze dienst niet bestaat uit het overbrengen van signalen maar uit de levering met behulp van elektronische-communicatienetwerken en -diensten van de overgebrachte inhoud. Door de aanbieders van aan het publiek aangeboden e-maildiensten over het internet mee te rekenen, dekt paragraaf 1 van artikel 126 dus ook dienstenaanbieders die geen operatoren zijn in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Paragraaf 1 beoogt tevens de aanbieders van openbare elektronische-communicatienetwerken, net zoals artikel 3, §§ 1 en 2, van Richtlijn 2006/24/EG dat doet.

Les fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6 de la loi du 13 juin 2005 relative aux communications électroniques ne sont par contre pas inclus dans le champ d'application du nouvel article 126. En effet, l'article 9, § 7, de la loi du 13 juin 2005 prévoit que ces fournisseurs et revendeurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et de la répression d'infractions pénales, et en vue de la répression d'appels malveillants vers les services d'urgence ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organisatrice des services de renseignement et de sécurité, et ce, dans des conditions qui doivent encore être fixées par arrêté royal.

Le projet de loi n'applique pas de règles différentes pour des fournisseurs de petite taille. En effet, la directive ne fait pas de distinction entre les fournisseurs selon leur taille et une telle distinction risquerait de créer des difficultés pratiques (difficulté de fixer un seuil et risque qu'un fournisseur passe à un moment donné en dessous ou au-dessus du seuil). De plus, il est difficile de concevoir que les bénéficiaires de la conservation de données reçoivent moins de données du fait que le fournisseur concerné est un petit fournisseur.

3) *Les données à conserver*

L'article 1.2. de la directive 2006/24/CE prévoit qu'elle s'applique "aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré".

La directive établit la liste des données à conserver en les regroupant par catégories selon qu'il s'agit de données nécessaires à: l'identification de la source d'une communication, l'identification de la destination d'une communication, la détermination des caractéristiques temporelles d'une communication, la détermination du type de communication, ainsi que du matériel utilisé, et la localisation du matériel utilisé.

Le projet de loi regroupe ces catégories de données sous les dénominateurs d'une part "données de trafic et de localisation" et d'autre part "données d'identification d'utilisateurs finals", "données d'identification de l'équipement terminal qui est présumé avoir été utilisé" et "données d'identification du service de communications électroniques utilisé". Les deux dernières catégories de données ont pour but ultime de permettre l'identification de l'utilisateur final.

De aanbieders en doorverkopers bedoeld in artikel 9, §§ 5 en 6, van de wet van 13 juni 2005 betreffende de elektronische communicatie vallen daarentegen niet onder het toepassingsgebied van het nieuwe artikel 126. Artikel 9, § 7, van de wet van 13 juni 2005 bepaalt immers dat deze aanbieders en doorverkopers verkeersgegevens en identificatiegegevens van eindgebruikers registreren en bewaren ten behoeve van de opsporing en de beteugeling van strafbare feiten en met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten alsook om de inlichtingsopdrachten te vervullen waarin de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten voorziet, volgens voorwaarden die nog moeten worden vastgelegd bij koninklijk besluit.

Het ontwerp van wet past geen verschillende regels toe voor kleine aanbieders. De richtlijn maakt immers geen onderscheid tussen de aanbieders volgens hun omvang en een dergelijk onderscheid zou tot praktische moeilijkheden kunnen leiden (moeilijkheid om een drempel vast te leggen en risico dat een provider op een gegeven ogenblik onder of boven de drempel gaat). Bovendien is het moeilijk voorstelbaar dat de begunstigden van de gegevensbewaring minder gegevens ontvangen doordat de betrokken aanbieder een kleine aanbieder is.

3) *De te bewaren gegevens*

Artikel 1.2 van Richtlijn 2006/24/EG bepaalt dat ze van toepassing is op "verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren".

De richtlijn stelt de lijst op van de te bewaren gegevens, onderverdeeld in categorieën naargelang het gegevens betreft die nodig zijn voor: de identificatie van de bron van een communicatie, identificatie van de bestemming van een communicatie, de bepaling van de tijdsgebonden karakteristieken van een communicatie, de bepaling van het type communicatie, alsook van de gebruikte apparatuur en de locatie van de gebruikte apparatuur.

Het ontwerp van wet groepeert deze categorieën van gegevens onder de noemers "verkeers- en locatiegegevens" enerzijds en "gegevens voor identificatie van de eindgebruikers", "gegevens ter identificatie van de vermoedelijk gebruikte eindapparatuur" en "gegevens ter identificatie van de gebruikte elektronische-communicatiedienst" anderzijds. De twee laatste categorieën van gegevens hebben tot ultieme doel de identificatie van de eindgebruiker mogelijk te maken.

Les données d'identification de l'équipement terminal qui est présumé avoir été utilisé correspondent "aux données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel" et aux "données nécessaires pour localiser le matériel de communication mobile" (voir l'article 5.1, e) et f) de la directive).

Le paragraphe 1er précise que les données ne doivent être conservées par les fournisseurs en question que pour autant que ces données soient générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés. Dans les cas où ces données ne sont pas générées ou traitées par ces fournisseurs, il n'y a pas d'obligation de les conserver. Ce principe est contenu à l'article 3.1 de la directive et explicité aux considérants 13 et 23.

La technologie de la communication et les protocoles techniques qui règlent cette communication électronique se développent rapidement, en particulier en ce qui concerne les formes de la téléphonie via l'internet. Pour que le cadre légal soit un instrument efficace dans la lutte contre la criminalité, il est nécessaire que ce cadre puisse suivre l'évolution de ces protocoles techniques.

Un arrêté royal permet une mise à jour rapide du cadre légal. En outre, cette méthode de travail ne s'écarte pas de la volonté et de la méthode de travail du législateur, qui en 2000 a déjà fixé les principes et qui a prescrit que les données à conserver et les modalités de cette conservation seraient reprises dans un arrêté royal. Ce principe était déjà clairement formulé à l'article 14 de la loi du 28 novembre 2000 relative à la criminalité informatique. Il a été confirmé à l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, qui a remplacé l'article précédent.

Le nouveau paragraphe 2 de l'article 126 indique les catégories de services publics pouvant bénéficier des données conservées.

La finalité relative à la poursuite et à la répression d'infractions pénales est remplacée dans le nouvel article 126, § 2, alinéa 1er, a), par "la recherche, la détection et la poursuite" d'infractions pénales.

La présente loi ne porte pas préjudice aux législations particulières. On pense ainsi par exemple à la possibilité pour l'administration fiscale d'accèder à certaines informations des opérateurs et aux exceptions prévues à l'article 125 de la loi du 13 juin 2005 relative aux communications électroniques.

De identificatiegegevens van de vermoedelijk gebruikte eindapparatuur stemmen overeen met de "gegevens die nodig zijn om de communicatieapparatuur of de vermoedelijke communicatieapparatuur van de gebruikers te identificeren" en met de "gegevens die nodig zijn om de locatie van de mobiele communicatieapparatuur te bepalen" (zie artikel 5.1, e) en f) van de richtlijn).

Paragraaf 1 preciseert dat de gegevens enkel moeten worden bewaard door de betrokken aanbieders voor zover deze gegevens door hen werden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten. Wanneer dergelijke gegevens niet worden gegenereerd of verwerkt door deze aanbieders, is er geen verplichting ze te bewaren. Dat principe is vervat in artikel 3.1 van de richtlijn en wordt toegelicht in de consideransen 13 en 23.

De communicatietechnologie en de technische protocollen die deze elektronische communicatie regelen evolueren snel, voornamelijk wat betreft de vormen van internettelefonie. Opdat het wettelijk kader een effectief instrument voor de bestrijding van criminaliteit zou zijn, is het noodzakelijk dat dit kader de evolutie van deze technische protocollen kan volgen.

Een koninklijk besluit maakt dan ook een snelle update van het wettelijke kader mogelijk. Deze werkwijze wijkt bovendien niet af van de wil en de werkwijze van de wetgever die al in 2000 de principes vastlegde en voorschreef dat de te bewaren gegevens en de nadere regels van deze bewaring opgenomen zouden worden in een koninklijk besluit. Dit principe was al duidelijk beschreven in artikel 14 van de wet inzake informaticacriminaliteit van 28 november 2000. Het werd nog eens bevestigd in artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, dat in de plaats kwam van het vorige artikel.

De nieuwe paragraaf 2 van artikel 126 duidt de categorieën van overheidsdiensten aan die recht hebben op de bewaarde gegevens.

Het doeleinde "opsporing en beteugeling van strafbare feiten" wordt in het nieuwe artikel 126, § 2, eerste lid, a), vervangen door "het onderzoek, de opsporing en de vervolging" van strafbare feiten.

Deze wet doet geen afbreuk aan de bijzondere wetgevingen. We denken bijvoorbeeld aan de mogelijkheid voor de fiscale overheid om inzage te krijgen in bepaalde informatie van de operatoren en aan de uitzonderingen waarin artikel 125 van de wet van 13 juni 2005 betreffende de elektronische communicatie voorziet.

Les modalités pratiques d'accès des services publics concernés aux données conservées par les fournisseurs ne sont pas réglées dans le présent projet de loi ni dans son arrêté d'exécution mais dans d'autres législations. On citera à cet égard par exemple l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité.

Par ailleurs, tant le procureur du Roi que le juge d'instruction, chacun pour leurs 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 des données conservées. A cet égard, il convient de souligner que le fait de pouvoir avoir accès à ces données conservées peut tout autant permettre aux autorités judiciaires d'inculper la personne que de l'innocenter.

Le nouveau paragraphe 3 de l'article 126 fixe le délai de conservation des données ainsi que les principes pour déterminer le point de départ de ce délai.

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 retenu s'inscrit dans cette fourchette.

La CPVP avait, dans son avis n° 20/2009, proposé un délai de conservation de douze mois, qui est le délai retenu par le gouvernement.

Dans la pratique, le délai de conservation de 12 mois est le délai actuel pour ce qui concerne les services téléphoniques accessibles au public. En effet, l'article 126, § 2, de la loi du 13 juin 2005 relative aux communications électroniques, tel qu'il existe actuellement, prévoit que "les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut." Cet arrêté royal n'ayant pas été adopté, les fournisseurs de services téléphoniques accessibles au public sont donc tenus de conserver les données concernées pendant au moins 12 mois.

De praktische werkwijze voor toegang tot de door de aanbieders bewaarde gegevens voor de overheidsdiensten, wordt niet geregeld in dit ontwerp van wet noch in het bijbehorende uitvoeringsbesluit maar in andere wetgevingen. Zie ook in dit kader bijvoorbeeld het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en het koninklijk besluit van 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie.

Zowel de procureur des Konings als de onderzoeksrechter, elk voor hun eigen bevoegdheden, moeten trouwens 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.

De nieuwe paragraaf 3 van artikel 126 bepaalt de bewaringstermijn van de data alsook de principes om het beginpunt van deze termijn te bepalen.

Artikel 6 van Richtlijn 2006/24/EG voorziet zo 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 CBPL had in haar advies nr. 20/2009 een bewaringstermijn van twaalf maanden voorgesteld, wat de termijn is die de overheid in aanmerking neemt.

In de praktijk is de bewaringstermijn van 12 maanden de huidige termijn voor de openbare telefoniediensten. Artikel 126, § 2, van de wet van 13 juni 2005 betreffende de elektronische communicatie, in zijn huidige vorm luidt immers: "De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut." Aangezien dat koninklijk besluit niet is aangenomen, zijn de aanbieders van openbare telefoniediensten dus verplicht om de gegevens in kwestie gedurende ten minste 12 maanden te bewaren.

On notera également que l'article 6 de la directive 2006/24/CE ne limite pas le champ d'application des durées minimum et maximum de conservation au service téléphonique accessible au public. La référence à ce service, prévue dans l'ancienne version de l'article 126, est dès lors supprimée, et le délai de conservation s'applique donc pour tous les fournisseurs de services et de réseaux énumérés dans le premier alinéa du nouvel article 126.

Étant donné que, pour lutter contre la criminalité, il est d'une importance cruciale de disposer de données d'identification, d'enregistrement et de localisation en matière de communications électroniques et, d'autre part, conscient néanmoins des coûts liés à la conservation, le gouvernement ne veut pas aller aussi loin que le délai maximum de 24 mois prévu par la directive, mais opte en faveur d'un délai de 12 mois. En matière d'enquêtes pénales, les exemples sont légions où une percée a encore pu être forcée grâce à l'obtention de données téléphoniques du passé.

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 précise 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, p. 35).

Cette évaluation montre cependant aussi qu'un des objectifs de la directive, à savoir l'harmonisation de la législation des États membres sur ce plan, motif sur lequel semble se baser la CPVP pour opter en faveur d'un délai de conservation de 12 mois (cf. numéro 22, avis CPVP) n'a pas été atteint et que la directive sera peut être à nouveau modifiée à terme. Il convient également de souligner que cette évaluation n'a fait apparaître aucune infraction grave à la vie privée.

De plus, il s'avère également que, pour pouvoir répondre aux obligations internationales ainsi qu'aux demandes d'entraide judiciaire émanant d'autres États (UE), il est crucial que la Belgique dispose de ces données de communication et ce dans le cadre d'une coopération européenne renforcée en vue de la lutte contre la criminalité (transfrontalière). Il ne suffit pas, en effet, de créer des organes de maintien (tels qu'Europol et Eurojust) et de placer, en termes de résultats, la barre

We merken eveneens op dat artikel 6 van Richtlijn 2006/24/EG het toepassingsgebied van de minimale en de maximale bewaringstermijn niet beperkt tot de openbaar beschikbare telefoniedienst. De verwijzing naar deze dienst uit de oude versie van artikel 126 vervalt bijgevolg, en de bewaringstermijn geldt dus voor alle diensten- en netwerkaanbieders die opgesomd worden in het eerste lid van het nieuwe artikel 126.

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 24 maanden van in de richtlijn maar opteert zij voor een termijn van 12 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 evaluatierapport 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)".

Uit die evaluatie blijkt echter ook dat één van de doelstellingen van de richtlijn, met name de harmonisatie van de wetgeving van de lidstaten op dat vlak, reden waarop de CBPL zich lijkt te steunen om te opteren voor een bewaringstermijn van 12 maanden (cf. randnummer 22, advies CBPL), niet is gehaald en dat de richtlijn misschien op termijn opnieuw zal gewijzigd worden. Eveneens moet benadrukt worden dat uit die evaluatie geen ernstige inbreuken op de privacy zijn gebleken.

Bovendien blijkt ook dat om aan de internationale verplichtingen te kunnen voldoen en om te kunnen voldoen aan rechtshulpverzoeken van andere (EU-) staten het cruciaal is dat België over deze communicatiegegevens beschikt en dit alles in het kader van een versterkte Europese samenwerking ter bestrijding van de (grensoverschrijdende) criminaliteit. Het volstaat inderdaad niet alleen handhavingsorganen te creëren (zoals Europol en Eurojust) en de lat in termen van

haute sur ce plan. Ces organes doivent également être dotés des outils nécessaires permettant de prendre à charge cette lourde tâche.

Vu la complexité de nombreux dossiers, un délai de conservation supérieur à un an est souhaitable du point de vue des services publics bénéficiaires des données conservées. Tout d'abord, il est renvoyé à cet égard aux exemples au point 10 de la réponse à l'avis n°24/2008 du 2 juillet 2008 de la CPVP.

Ensuite, il est établi que le processus communicationnel se déplace de plus en plus vers l'internet. Pour identifier les utilisateurs d'internet, il faut le plus souvent procéder à plusieurs réquisitions successives auprès de différents opérateurs (parfois aussi à l'étranger). 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 12 mois, les opérateurs avaient pu fournir une réponse dans 61 % des cas. Si ce délai était relevé à 18 mois, il pourra être répondu à 78 % des questions posées. Dans 14 % des cas, la demande envers les opérateurs concerne des données générées ou traitées plus de 18 mois avant la demande et dans 8 % des cas, la date d'utilisation de l'adresse IP n'a pas été spécifiée sur la demande, ce qui rend impossible de donner un âge à cette donnée. Il s'agit, en l'occurrence, de dossiers de terrorisme, de traite d'êtres humains, de pédopornographie ou de demandes d'entraide judiciaire traitées par le parquet fédéral. Pour les autorités judiciaires, un délai de conservation de 18 mois est préférable par rapport à un délai de conservation de 12 mois.

Cependant, vu les remarques du secteur des communications électroniques et de la CPVP, le délai de conservation est à l'heure actuelle fixé à douze mois.

Le rapport d'évaluation qui doit être soumis deux ans après l'entrée en vigueur de l'arrêté royal d'exécution de l'article 126 (cf. article 126, § 7) permettra de démontrer si le délai de conservation doit être revu vers le haut ou vers le bas, comme l'indique à juste titre la CPVP (cf. numéro 22).

Pour ce qui concerne le point de départ du délai de conservation, le paragraphe 3 de l'article 126 fait la distinction suivante.

resultaten op dat vlak hoog te leggen. Zij moeten ook de tools krijgen om die zware taak op te nemen.

Gezien de complexiteit van heel wat dossiers is een bewaringstermijn van 1 jaar wenselijk vanuit het standpunt van de overheidsdiensten die de begunstigden zijn van de bewaarde gegevens. Er wordt in de eerste plaats verwezen naar de voorbeelden in punt 10 van het antwoord op advies nr. 24/2008 van 2 juli 2008 van de CBPL.

Vervolgens staat vast dat, meer en meer, het communicatiegebeuren verschuift naar het internet. Het identificeren van de internetgebruiker noodzaakt meestal de uitvoering van meerdere opeenvolgende vorderingen bij verschillende operatoren (soms ook in het buitenland). 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 12 maanden de operatoren in 61 % van de gevallen een antwoord hadden kunnen verstrekken. Indien deze termijn zou worden opgetrokken naar 18 maanden, dan kunnen 78 % van de gestelde vragen beantwoord worden. In 14 % van de gevallen betreft de aan de operatoren gerichte aanvraag gegevens die meer dan 18 maanden voor de aanvraag werden gegenereerd of verwerkt en in 8 % van de gevallen is de datum van gebruik van het IP-adres niet op de aanvraag gespecificeerd, waardoor het onmogelijk is om op dat gegeven een ouderdom te plakken. Het gaat hier over dossiers van terrorisme, mensenhandel, kinderpornografie of rechtshulpverzoeken behandeld door het federaal parket. Voor de gerechtelijke autoriteiten is een bewaringstermijn van 18 maanden verkieslijk tegenover een bewaringstermijn van 12 maanden.

Gezien de opmerkingen van de elektronische-communicatiesector en de CBPL wordt de bewaringstermijn vandaag evenwel vastgelegd op twaalf maanden.

Het evaluatieverslag dat moet worden voorgelegd twee jaar na de inwerkingtreding van het koninklijk besluit tot uitvoering van artikel 126 (cf. artikel 126, § 7) zal kunnen aantonen of de bewaringstermijn dient te worden gewijzigd naar boven of naar beneden, zoals de CBPL terecht aangeeft (cf. randnummer 22).

Wat betreft het startpunt voor de bewaringstermijn, maakt paragraaf 3 van artikel 126 het volgende onderscheid.

Les données de trafic et de localisation sont conservées pendant douze mois à partir de la date de la communication.

Par contre, les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé (ci-après les données d'identification) sont conservées dès la souscription au service, que ce soit dans le cadre d'un abonnement ou non, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.

Dans la pratique, une communication est parfois encore possible après la fin de l'abonnement ou, lorsqu'un abonnement n'a pas été contracté, après la fin de la durée de validité du service, ainsi que les exemples suivants l'illustrent:

— il existe des formules d'abonnement où l'abonné ne peut plus établir de communications sortantes lui-même à la fin de l'abonnement, mais où il peut encore recevoir des communications entrantes pendant trois mois;
— pour les cartes prépayées pour la téléphonie mobile, où l'utilisateur peut encore être appelé pendant trois mois après que son propre crédit d'appel ait été utilisé.

Le point de départ du délai de conservation est fonction du type de données à conserver. Or, ces données à conserver sont fixées précisément dans l'arrêté royal d'exécution de l'article 126. Par conséquent, alors que les principes en la matière sont fixés dans le paragraphe 3 de l'article 126, c'est l'arrêté royal précité qui précise quel point de départ du délai de conservation s'applique à quelle donnée.

L'article 126, paragraphe 3, alinéa 1er, qui vise les données d'identification, ne reprend pas le libellé de l'article 6 de la directive qui prévoit que le point de départ pour le calcul du délai de conservation est la "date de la communication". En effet, ce libellé est adéquat pour les données de trafic et de localisation dès lors que ces données sont particulières à chaque communication et doivent être conservées pour chaque communication. Par contre, ce libellé est difficile à appliquer aux données d'identification qui ne constituent pas en tant que telles des communications et qui peuvent exister indépendamment de toute communication.

Si la date de la communication était également prise comme point de départ pour le calcul du délai de conservation pour les données d'identification, alors:

De verkeers- en locatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie.

De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur (hierna "identificatiegegevens") worden daarentegen bewaard vanaf de inschrijving op de dienst, ongeacht of dit in het kader van een abonnement is of niet, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

In de praktijk is communicatie soms nog mogelijk na afloop van het abonnement of, wanneer geen abonnement werd genomen, na afloop van de geldigheidsduur van de dienst, zoals blijkt uit de volgende voorbeelden:

— er bestaan abonnementsformules waarbij de abonnee zelf geen uitgaande communicatie meer tot stand kan brengen op het einde van het abonnement, maar hij wel nog inkomende communicatie kan ontvangen gedurende drie maanden;
— voorafbetaalde kaarten voor mobiele telefonie, waarbij de gebruiker nog gedurende drie maanden kan worden gebeld nadat zijn eigen belkrediet is opgebruikt.

Het beginpunt voor de bewaringstermijn hangt af van het te bewaren type van gegevens. Deze te bewaren gegevens worden overigens nauwkeurig vastgelegd in het koninklijk besluit tot uitvoering van artikel 126. Bijgevolg, terwijl de principes ter zake worden bepaald in paragraaf 3 van artikel 126, is het het voorgaande koninklijk besluit dat het beginpunt bepaalt voor de bewaringstermijn voor elk gegeven.

Artikel 126, paragraaf 3, eerste lid, dat de identificatiegegevens beoogt, gebruikt niet de formulering van artikel 6 van de richtlijn, dat bepaalt dat het startpunt voor de berekening van de bewaringstermijn de "datum van de communicatie" is. Die formulering is inderdaad gepast voor de verkeers- en locatiegegevens omdat die gegevens specifiek zijn voor elke communicatie en moeten worden bewaard voor elke communicatie. Die formulering kan daarentegen maar moeilijk worden toegepast op de identificatiegegevens die niet aldus communicatie vormen en die los van alle communicatie kunnen bestaan.

Indien de communicatiedatum ook als startpunt zou worden genomen voor de berekening van de bewaringstermijn voor de identificatiegegevens, dan:

— les fournisseurs n'auraient pas l'obligation de conserver ces données entre la date de la souscription au service et la première communication;

— les fournisseurs n'auraient pas l'obligation de conserver ces données en l'absence de communication, alors qu'il est possible que des appels infructueux soient adressés à un utilisateur final, qui sont une indication d'un lien avec d'autres parties;

— les fournisseurs devraient conserver ces données d'identification pour chaque communication, de la première jusqu'à la dernière communication, ce qui augmenterait le volume des données à conserver.

Dès lors, l'article 126, paragraphe 3, alinéa 1er, reprend le principe posé par la directive (délai de conservation de douze mois à compter de la dernière communication) mais se limite à imposer aux fournisseurs de conserver une seule fois les données d'identification au début de la souscription au service.

Le paragraphe 4 de l'article 126 prévoit différentes hypothèses dans lesquelles le délai de conservation de 12 mois pourrait être dépassé.

Tout d'abord, le premier alinéa du paragraphe 4 donne au Roi la possibilité de fixer un délai supérieur à douze mois, sans dépasser 18 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 aient fait leur rapport d'évaluation à la Chambre des Représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, alinéa 3 (voir paragraphe 7). Ainsi, par exemple, un délai de conservation plus long que douze mois pourrait être prévu pour l'identification des adresses IP si cela s'avèrait nécessaire. On notera que 5 États membres ont défini différentes durées de conservation selon les catégories de données (Rapport d'évaluation concernant la directive sur la conservation des données, p. 16).

Ensuite, le paragraphe 4, alinéa 2, de l'article 126 donne au Roi la possibilité de fixer temporairement un délai supérieur au maximum légal en cas de circonstances exceptionnelles. Ces circonstances exceptionnelles sont énumérées à l'article 4, § 1er, de la loi du 13 juin 2005 relative aux communications électroniques: "lorsque la sécurité publique, la santé publique, l'ordre public ou la défense du Royaume l'exigent". On peut à titre d'exemple penser aux situations de guerre ou aux attentats terroristes ou à une vague de criminalité violente. En tout cas, il faut que les circonstances soient très sérieuses. L'évaluation de la Commission européenne a cependant montré qu'à ce jour aucun État membre n'a utilisé la possibilité prévue par la directive.

— zouden de aanbieders niet verplicht zijn om deze gegevens te bewaren tussen de datum van inschrijving op de dienst en de eerste communicatie;

— zouden de aanbieders niet verplicht zijn om deze gegevens te bewaren indien er geen communicatie plaatsvindt, terwijl het mogelijk is dat mislukte oproepen worden gedaan naar een eindgebruiker, die een indicatie zijn van een link met andere partijen;

— zouden de aanbieders deze identificatiegegevens moeten bewaren voor elke communicatie, van de eerste tot de laatste communicatie, wat het volume van te bewaren gegevens zou vergroten.

Artikel 126, paragraaf 3, eerste lid, neemt dan ook het principe over van de richtlijn (bewaringstermijn van twaalf maanden vanaf de laatste communicatie) maar beperkt zich ertoe de aanbieders te verplichten om één enkele keer de identificatiegegevens te bewaren aan het begin van de inschrijving op de dienst.

Paragraaf 4 van artikel 126 voorziet in verschillende hypothesen waarbij de bewaringstermijn van 12 maanden zou kunnen worden overschreden.

Allereerst biedt het eerste lid van paragraaf 4 de Koning de mogelijkheid om een termijn van langer dan twaalf maanden te bepalen, maar niet langer dan 18 maanden, voor bepaalde gegevenscategorieën. Deze aan de Koning geboden mogelijkheid mag evenwel enkel worden benut nadat de minister en de minister van Justitie hun evaluatieverslag hebben voorgelegd aan de Kamer van volksvertegenwoordigers, twee jaar na de inwerkingtreding van het koninklijk besluit beoogd in paragraaf 1, derde lid (zie paragraaf 7). Een bewaringstermijn van meer dan twaalf maanden zou aldus mogelijk zijn voor de identificatie van IP-adressen indien dat nodig zou blijken. We merken op dat 5 lidstaten verschillende bewaringstermijnen hebben vastgelegd afhankelijk van de gegevenscategorieën (Evaluatieverslag betreffende de richtlijn inzake gegevensbewaring, blz. 16).

Paragraaf 4, tweede lid van artikel 126 geeft de Koning vervolgens de mogelijkheid om tijdelijk een langere termijn dan het wettelijke maximum te bepalen in uitzonderlijke omstandigheden. Deze uitzonderlijke omstandigheden worden opgesomd in artikel 4, § 1, van de wet van 13 juni 2005 betreffende de elektronische communicatie: wanneer de openbare veiligheid, de volksgezondheid, de openbare orde of de verdediging van het Rijk dit eisen". Men kan bijvoorbeeld denken aan oorlogssituaties of terroristische aanslagen of een golf van gewelddadige criminaliteit. In ieder geval moeten de omstandigheden zwaarwegend genoeg zijn. Uit de evaluatie van de Europese Commissie is echter gebleken dat tot op heden geen enkele lidstaat van deze in de Richtlijn geboden mogelijkheid gebruikt heeft gemaakt.

Finalement, une procédure de notification à la Commission européenne est prévue au paragraphe 4, alinéa 3, de l'article 126, conformément à l'article 12 de la directive. En effet, cet article 12 prévoit que lorsqu'un État membre a l'intention de prolonger le délai au-delà du délai maximum de 24 mois prévu par la directive, il doit notifier cette prolongation à la Commission européenne. Comme déjà dit, ce cas ne s'est pas encore présenté au niveau de l'UE.

Le paragraphe 5 fixe un certain nombre de conditions de conservation destinées à garantir la sécurité des données et à assurer leur traitement adéquat par du personnel spécifiquement autorisé (article 7 de la directive).

En ce qui concerne les mesures techniques et organisationnelles appropriées afin de protéger les données conservées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, il peut être renvoyé aux mesures de référence établies par la CPVP, qui peuvent s'appliquer à la protection du traitement de données à caractère personnel.

L'article 126, § 5, alinéa 1er, 4°, prévoit qu'après l'expiration du délai de conservation, les données conservées sont détruites sans délai.

On rappelera également que le paragraphe 1er de l'article 126 prévoit expressément qu'il est pris "Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel". Il est renvoyé aux commentaires de cette disposition ci-dessus.

Les paragraphes 6 et 7 de l'article 126 reprennent une demande de la CPVP et prévoient une double évaluation de la loi. D'une part, deux ans après l'entrée en vigueur du futur arrêté royal exécutant l'article 126, une vaste évaluation unique devra être menée; à cet égard, les ministres responsables feront rapport à la Chambre des représentants sur l'application de la loi, et, éventuellement des recommandations de contenu pourront être formulées concernant les délais de conservation, le contenu des données conservées, l'application pratique, *etc*. Le cas échéant, cette évaluation pourrait conduire à des initiatives appropriées. D'autre part, le projet de loi prévoit également un rapport annuel à la Chambre des Représentants. Il s'agit en l'occurrence plutôt d'un rapport statistique, comme cela est déjà prévu pour certaines mesures d'instruction à l'article 90*decies* du Code d'instruction criminelle.

Tot slot voorziet paragraaf 4, derde lid, van artikel 126, conform artikel 12 van de richtlijn, in een procedure voor kennisgeving aan de Europese Commissie. Dat artikel 12 bepaalt immers dat als een lidstaat de intentie heeft om de bewaringstermijn langer te maken dan de in de richtlijn vastgestelde maximumtermijn van 24 maanden, hij deze verlenging moet meedelen aan de Europese Commissie. Zoals gezegd heeft het geval zich nog niet voorgedaan in de EU.

Paragraaf 5 stelt een aantal voorwaarden inzake bewaring vast die bedoeld zijn om de veiligheid van de gegevens te garanderen en ervoor te zorgen dat ze op gepaste wijze worden verwerkt door personeel dat speciaal daartoe bevoegd is (artikel 7 van de richtlijn).

Inzake de passende technische en organisatorische maatregelen bedoeld om de bewaarde gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, kan verwezen worden naar de referentiemaatregelen opgesteld door de CBPL, die van toepassing kunnen zijn op de bescherming van de verwerking van persoonsgegevens.

Artikel 126, § 5, eerste lid, 4°, bepaalt dat na afloop van de bewaringstermijn de bewaarde gegevens onverwijld vernietigd worden.

We herinneren er eveneens aan dat paragraaf 1 van artikel 126 uitdrukkelijk bepaalt dat het moet worden opgevat "Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens." Er wordt verwezen naar de opmerkingen op deze bepaling hierboven.

De paragrafen 6 en 7 van artikel 126 nemen een verzoek over van de CBPL en voorzien in een tweevoudige evaluatie van de wet. Enerzijds moet er twee jaar na de inwerkingtreding van het toekomstige koninklijk besluit ter uitvoering van artikel 126 een grote eenmalige evaluatie komen waarbij de verantwoordelijke ministers verslag zullen uitbrengen aan de Kamer van volksvertegenwoordigers over de toepassing van de wet, en waarbij eventueel inhoudelijke aanbevelingen gedaan kunnen worden omtrent bewaringstermijnen, inhoud van de bewaarde gegevens, praktische toepassing, *etc*. Deze evaluatie kan in voorkomend geval tot passende initiatieven leiden. Anderzijds voorziet het ontwerp van wet ook in een jaarlijkse rapportering aan de Kamer van volksvertegenwoordigers. Het gaat hier eerder om een statistisch rapport zoals die voor een aantal onderzoeksmaatregelen ook is opgenomen in artikel 90*decies* van het Wetboek van Strafvordering.

Les statistiques annuelles à fournir par les fournisseurs de services ou de réseaux à l'IBPT sont déterminées par arrêté royal.

Art. 6

Vu que la directive 2006/24/CE stipule explicitement à l'article 13.2, que chaque État membre doit prendre, en particulier, les mesures nécessaires pour faire en sorte que tout accès intentionnel aux données conservées ou tout transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la directive, soient passibles de sanctions efficaces, proportionnées et dissuasives, le projet de loi insère une disposition pénale additionnelle, complétant les dispositions pénales déjà existantes dans le Code pénal concernant le hacking externe et interne.

Le projet de loi s'écarte ici de l'avis de la CPVP, parce qu'il est apparu, après analyse, que le texte soumis à la CPVP est incohérent avec les dispositions pénales déjà existantes dans le Code pénal. Néanmoins, le but de l'article, qui est partagé par la CPVP, reste le même: protéger la confidentialité des données et garantir l'accès à, la possession et l'utilisation de ces données conformément aux finalités légalement prévues. Cependant, il ne faut pas créer de nouvelles incriminations pour des actes qui sont déjà couverts par d'autres dispositions pénales. Il serait utile de le faire seulement si l'on estime que les dispositions pénales existantes ne sont pas suffisante.

Il est donc nécessaire de distinguer différents cas de figure et de voir quelles sont les dispositions existantes qui pourraient s'y appliquer afin de ne créer une nouvelle infraction que pour ce qui n'est pas encore couvert.

Lorsqu'une personne qui n'est pas autorisée à accéder au système y accède quand même, nous renvoyons ici à l'article 550*bis*, § 1er, du Code pénal: le hacking externe, avec les circonstances aggravantes en cas de détention, divulgation, distribution ou usage des données (§§ 3 et 7).

Lorsqu'une personne est autorisée à accéder au système et outrepasse son pouvoir d'accès, il peut être renvoyé au hacking interne (article 550*bis*, § 2 Code pénal et §§ 3 et 7). Ce sera, par exemple, le cas de la personne qui travaille à la Cellule Justice d'un opérateur mais qui accède aux données en dehors de toute requête judiciaire. Néanmoins, lorsqu'elle n'outrepasse pas son pouvoir d'accès, mais fait ultérieurement un usage non autorisé par la loi des données qu'elle a

De jaarlijkse statistieken die de diensten- of netwerkaanbieders aan het BIPT moeten verstrekken, worden bij koninklijk besluit bepaald.

Art. 6

Aangezien Richtlijn 2006/24/EG uitdrukkelijk bepaalt in artikel 13.2 dat elke lidstaat in het bijzonder de noodzakelijke maatregelen moet nemen om ervoor te zorgen dat elke opzettelijke toegang tot of overbrenging van gegevens die worden bewaard en die niet is toegestaan uit hoofde van de krachtens de richtlijn vastgestelde nationale uitvoeringsbepalingen strafbaar is met effectieve, evenredige en afschrikkende sancties, voegt het ontwerp van wet een extra strafbepaling in, die een aanvulling is op de al bestaande strafbepalingen in het Strafwetboek betreffende externe en interne hacking.

Het ontwerp wijkt hier af van het advies van de CBPL, omdat na analyse gebleken is dat de tekst die aan de CBPL werd voorgelegd incoherent is met de al bestaande strafbepalingen in het Strafwetboek. Niettemin blijft de doelstelling van het artikel, die gedeeld wordt door de CBPL, dezelfde: de vertrouwelijkheid van de gegevens beschermen en waarborgen dat de toegang tot, het gebruik van en het bezit van deze gegevens voldoen aan de wettelijk vastgelegde doelstellingen. Toch moeten er geen nieuwe incriminaties gecreëerd worden voor daden die reeds door andere strafbepalingen gedekt worden. Dit is enkel nuttig indien men van mening is dat de bestaande strafbepalingen niet voldoende zijn.

Het is dus noodzakelijk om verschillende gevallen te onderscheiden en te kijken welke de bestaande bepalingen zijn die erop van toepassing kunnen zijn, om slechts een nieuw strafbaar feit te creëren voor de gevallen die nog niet gedekt zijn.

Wanneer een persoon niet gemachtigd is om toegang te hebben tot het systeem en er zich toch toegang toe verschaft, kan er verwezen worden naar artikel 550*bis*, § 1, van het Strafwetboek: externe hacking, met verzwarende omstandigheden in geval van bezit, onthulling, verspreiding of gebruik van de gegevens (§§ 3 en 7).

Wanneer een persoon gemachtigd is om toegang te hebben tot het systeem en zijn toegangsbevoegdheid overschrijdt, kan er verwezen worden naar de interne hacking (artikel 550*bis*, § 2, van het Strafwetboek en §§ 3 en 7). Dit zal bijvoorbeeld het geval zijn voor de persoon die in de cel Justitie van een operator werkt maar zich toegang verschaft tot de gegevens zonder gerechtelijke vordering. Niettemin, de persoon die zijn toegangsbevoegdheid niet overschrijdt, maar later

extraites du système d'une manière légale et justifiée, cette hypothèse n'est pas couverte par la loi.

C'est la raison pour laquelle on introduit dans le projet de loi une nouvelle incrimination qui reprend les éléments qui ne sont pas encore couverts par les articles du Code pénal, et qui rend punissable toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126, et toute personne qui, sachant que les données ont été obtenues par la commission de cette infraction, les détient, les révèle à une autre personne, ou les divulgue ou fait un usage quelconque des données ainsi obtenues.

Les nouvelles sanctions pénales introduites par l'article 4 laissent intactes les autres sanctions déjà en vigueur.

À cet égard, l'article 39 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel prévoit une amende pénale de 100 à 100 000 EUR selon la législation actuellement en vigueur pour tout responsable de traitement (ou préposé ou mandataire) qui enfreint l'article 4, § 1er, de ladite loi, à savoir la qualité des données (pas de données excessives, pas de durée de conservation éternelle, pas d'utilisation incompatible avec les finalités prévues, *etc.*).

L'article 14, § 3, de la loi du 17 janvier 2003 relatif au statut du régulateur des secteurs des postes et des télécommunications belges donne, en outre, la compétence à l'Institut pour contrôler notamment le respect de la loi du 13 juin 2005 relative aux communications électroniques et de ses arrêtés d'exécution, et l'article 21, § 6, de la loi du 17 janvier 2003 permet à l'IBPT d'infliger une amende administrative pouvant aller, pour un contrevenant qui réalise un chiffre d'affaires et, en cas de non respect d'une première décision de l'IBPT lui imposant une amende administrative, jusqu'à 10 % du chiffre d'affaires du contrevenant réalisé au cours de l'exercice complet le plus récent dans le secteur des communications électroniques en Belgique.

L'ensemble des dispositions précitées implique que non seulement l'IBPT et la CPVP, mais aussi les

onwettig gebruikmaakt van de gegevens die hij op een wettelijke en gerechtvaardigde manier uit het systeem heeft gehaald, is een hypothese die niet gedekt is door de wet.

Dit is dan ook de reden waarom in het ontwerp van wet een nieuwe incriminatie ingevoegd wordt die de elementen overneemt die nog niet gedekt zijn door de artikelen van het Strafwetboek, en die de persoon strafbaar stelt die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt, en de persoon die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van dit misdrijf, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.

De nieuwe strafsancties ingevoerd door artikel 4 doen geen afbreuk aan de andere sancties die reeds van toepassing zijn.

In dit kader voorziet artikel 39 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, in een boete van 100 tot 100.000 EUR naargelang van de van kracht zijnde wetgeving voor de verantwoordelijke voor verwerking (of de aangestelde of gevolmachtigde) die artikel 4, § 1, van de voornoemde wet overtreedt, met name betreffende de kwaliteit van de gegevens (niet buitensporig veel gegevens, geen oneindige bewaringstermijn, geen oneigenlijk gebruik ten opzichte van de bepaalde doeleinden, enz.).

Artikel 14, § 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector maakt het Instituut bovendien bevoegd voor de controle op de naleving van de wet van 13 juni 2005 betreffende de elektronische communicatie en de bijbehorende uitvoeringsbesluiten, en krachtens artikel 21, § 6, van de wet van 17 januari 2003 mag het BIPT een administratieve boete opleggen die in het geval van een overtreder met een omzet en in geval van niet-naleving van een eerste besluit van het BIPT waarin hem een administratieve boete wordt opgelegd, kan gaan tot 10 % van de omzet van de overtreder gerealiseerd in de loop van het meest recente volledige boekjaar in de elektronischecommunicatiesector in België.

Het geheel van de voormelde bepalingen houdt in dat niet alleen het BIPT en de CBPL, maar ook de

autorités judiciaires peuvent contrôler le bon déroulement de la conservation des données.

CHAPITRE 3

Modification de l'article 90*decies* du Code d'instruction criminelle

Art. 7

Cet article complète l'article 90*decies* du Code d'instruction criminelle. Le rapport annuel par le ministre de la Justice prévu par cet article contiendra désormais des informations statistiques concernant la conservation des données visée à l'article 126 de la loi relative aux communications électroniques.

Le ministre de l'Economie,

Johan VANDE LANOTTE

Le ministre de la Justice,

Annemie TURTELBOOM

gerechtelijke autoriteiten toezicht kunnen houden op het goede verloop van de bewaring van de gegevens.

HOOFDSTUK 3

Wijziging van artikel 90*decies* van het Wetboek van Strafvordering

Art. 7

Dit artikel vervolledigt artikel 90*decies* van het Wetboek van Strafvordering. Het jaarlijkse verslag van de minister van Justitie dat door dit artikel wordt voorgeschreven, zal voortaan ook statistische informatie bevatten over de bewaring van gegevens zoals bedoeld door artikel 126 van de wet betreffende de elektronische communicatie.

De minister van Economie,

Johan VANDE LANOTTE

De minister van Justitie,

Annemie TURTELBOOM

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-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 90*decies* du Code d'instruction criminelle

CHAPITRE I^ER

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

Article 1er

L'article 1er de la loi du 13 juin 2005 relative aux communications électroniques, complété par la loi du 10 juillet 2012, est complété par un alinéa rédigé comme suit:

"La présente loi transpose partiellement la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de donnés 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 (directive "conservation de données") (J.O. 13 avril 2006, L 105/54)".

Art. 2

L'article 2, 11°, de la même loi est remplacé par ce qui suit:

"11° "opérateur": toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;".

Art. 3

L'article 126 de la même loi est remplacé par ce qui suit:

"Art. 126. § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic, les données de localisation, les données d'identification d'utilisateurs finals, les données d'identification du service de communications électroniques utilisé et les données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Par fourniseurs au sens du présent article, on entend également les revendeurs en nom propre et pour leur propre compte.

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

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

HOOFDSTUK I

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

Artikel 1

Artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, aangevuld bij de wet van 10 juli 2012, wordt aangevuld met een lid luidende:

"Deze wet voorziet in een gedeeltelijke omzetting van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn genereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG ("Dataretentierichtlijn") (PB 13 april 2006, L 105/54)".

Art. 2

Artikel 2, 11°, van dezelfde wet wordt vervangen als volgt:

"11° "operator": een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9;".

Art. 3

Artikel 126 van dezelfde wet wordt vervangen als volgt:

"Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, of internettelefoniediensten, en de aanbieders van de onderliggende openbare elektronische- communicatienetwerken de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische-communicatiedienst en de gegevens voor identificatie van de vermoedelijk gebruikte eindapparatuur, die door hen worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten.

Onder aanbieders in de betekenis van dit artikel worden ook de doorverkopers in eigen naam en voor eigen rekening verstaan.

Par service de téléphonie au sens du présent article, on entend les appels téléphoniques - notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données-, les services supplémentaires - notamment le renvoi ou le transfert d'appels- et les services de messagerie et multimédias, notamment les services de messages brefs (SMS), les services de médias améliorés (EMS) et les services multimédias (MMS).

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de service en application de l'alinéa 1er ainsi que les exigences auxquelles ces données doivent répondre.

Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée.

§ 2. Les données visées au paragraphe 1er, al. 1er, sont conservées en vue:

a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46*bis* et 88*bis* du Code d'Instruction criminelle;

b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107;

c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

d) de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 1er, alinéa 1er , soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières.

§ 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées à partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de dernière communication entrante ou sortante enregistrée.

Onder telefoniedienst in de betekenis van dit artikel wordt verstaan: telefoonoproepen — met inbegrip van spraakoproepen, voicemail, conference call of datacommunicatie-, aanvullende diensten -met inbegrip van call forwarding en call transfer-, en de messaging- en multimediadiensten — met inbegrip van short message service (sms), enhanced media service (EMS) en multimedia service (MMS).

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de krachtens het eerste lid te bewaren gegevens per type dienst alsook de vereisten waaraan deze gegevens moeten beantwoorden.

Behoudens andersluidende wettelijke bepaling, mogen geen gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, bewaard worden.

§ 2. De gegevens beoogd in paragraaf 1, eerste lid, worden bewaard met het oog op:

a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering;

b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of –dienst, zoals bedoeld in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en 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.

§ 3. De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

Les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises au premier alinéa et celles au deuxième.

§ 4. À la suite du rapport d'évaluation visé au paragraphe 7, le Roi peut, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de la Commission de la protection de la vie privée, adapter le délai de conservation des données pour certaines catégories de données, sans ce que ce délai puisse dépasser 18 mois.

Le Roi peut, dans les circonstances visées à l'article 4, § 1er, par arrêté délibéré en Conseil des ministres, et après avis de l'Institut et de la Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à douze mois.

Lorsque, dans les circonstances visées à l'alinéa 2, le Roi fixe un délai de conservation supérieur à vingt-quatre mois, le ministre notifie immédiatement à la Commission européenne et aux autres États membres de l'Union européenne toute mesure prise, accompagnée de sa motivation.

§ 5. Pour la conservation des données visées au paragraphe 1er, alinéa 1er, les fournisseurs de réseaux ou de services de communications électroniques visés au paragraphe 1er, alinéa 1er:

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

3° garantissent que l'accès aux données conservées n'est effectué qu'à la demande et sous la surveillance de la Cellule de Coordination de Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques;

4° veille à ce que les données conservées soient détruites lorsqu'est expiré le délai de conservation applicable à ces données.

De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de gegevens die zijn onderworpen aan het eerste lid en deze die zijn onderworpen aan het tweede lid.

§ 4. Naar aanleiding van het evaluatieverslag beoogd in paragraaf 7, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, de bewaringstermijn van de gegevens voor bepaalde categorieën van gegevens aanpassen, zonder een termijn van meer dan 18 maanden vast te leggen.

De Koning kan, in de omstandigheden zoals bedoeld in artikel 4, § 1, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een beperkte periode, een bewaringstermijn voor de gegevens vastleggen die langer is dan twaalf maanden.

Wanneer in de omstandigheden bedoeld in het tweede lid de Koning een bewaringstermijn oplegt die langer is dan vierentwintig maanden, stelt de minister de Europese Commissie en de overige lidstaten van de Europese Unie onverwijld in kennis van alle genomen maatregelen, met vermelding van de redenen die eraan ten grondslag liggen.

§ 5. Voor de bewaring van de in paragraaf 1, eerste lid, bedoelde gegevens geldt het onderstaande voor de aanbieder van een netwerk of dienst voor elektronische communicatie bedoeld in paragraaf 1, eerste lid:

1° hij garandeert dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;

2° hij zorgt ervoor dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

3° hij garandeert dat de toegang tot de bewaarde gegevens enkel op verzoek van en onder het toezicht van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie gebeurt;

4° hij zorgt ervoor dat de gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, worden vernietigd.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les mesures techniques et administratives que les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, doivent prendre en vue garantir la protection des données à caractère personnelle conservées.

Les founisseurs de services et réseaux visés paragraphe 1er, alinéa 1er, sont considérés comme responsables du traitement de ces données au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

§ 6. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Commission européenne et à la Chambre des Représentants. Ces statistiques comprennent notamment:

1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, a) seront également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine, sur proposition du ministre de la Justice et ministre et sur avis de l'Institut, les statistiques que les fournisseurs de services ou de réseaux transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 7. Sans préjudice du rapport visé au paragraphe 6, alinéa 3, le ministre et le ministre de la Justice font un rapport d'évaluation à la Chambre des Représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, alinéa 3, sur la mise en œuvre de cet article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die de aanbieders van diensten en netwerken beoogd in paragraaf 1, eerste lid, moeten nemen teneinde de bescherming van de bewaarde persoonsgegevens te garanderen.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, worden beschouwd als verantwoordelijk voor de verwerking van deze gegevens in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

§ 6. De minister en de minister van Justitie zorgen ervoor dat jaarlijks aan de Europese Commissie en de Kamer van volksvertegenwoordigers statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare communicatiediensten of netwerken. Die informatie heeft onder meer betrekking op:

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken niet konden worden ingewilligd.

Deze statistische informatie mag geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, a) worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van Strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt, op voorstel van de minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders van diensten of netwerken jaarlijks moeten overzenden aan het Instituut en deze die het Instituut overzendt aan de minister en aan de minister van Justitie.

§ 7. Onverminderd het verslag bedoeld in paragraaf 6, derde lid, brengen de minister en de minister van Justitie, twee jaar na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, derde lid, aan de Kamer van volksvertegenwoordigers een evaluatieverslag uit over de toepassing van dit artikel, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de te bewaren gegevens en de bewaringstermijn.

Art. 4

Dans l'article 145 de la même loi, modifié par la loi du 25 avril 2007, il est inséré un paragraphe 3*ter* rédigé comme suit:

"§ 3*ter*. Est puni d'une amende de 50 à 50 000 EUR et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement:

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126;

2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1° les détient, les révèle à une autre personne, ou les divulgue ou fait un usage quelconque des données ainsi obtenues.".

CHAPITRE II

Modification de l'article 90*decies* du code d'instruction criminelle

Art. 5

L'article 90*decies* du Code d'instruction criminelle, inséré par la loi du 30 juin 1994 et modifié par les lois du 8 avril 2002, 7 juillet 2002 et du 6 janvier 2003, est complété par un alinéa, rédigé comme suit:

"À ce rapport est joint le rapport dressé en application de l'article 126, § 6, alinéa 3 de la loi du 13 juin 2005 relative aux communications électroniques."

Art. 4

In artikel 145 van dezelfde wet, gewijzigd bij de wet van 25 april 2007, wordt een paragraaf 3*ter* ingevoegd, luidende:

"§ 3*ter*. Met een geldboete van 50 tot 50.000 EUR en met een gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.".

HOOFDSTUK II

Wijziging van artikel 90*decies* van het Wetboek van Strafvordering

Art. 5

Artikel 90*decies* van het Wetboek van Strafvordering, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 8 april 2002, 7 juli 2002 en 6 januari 2003, wordt aangevuld met een lid, luidende:

"Bij dit verslag wordt tevens het verslag bijgevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie."

AVIS DU CONSEIL D'ÉTAT N° 53 272/4 DU 27 MAI 2013

Le 26 avril 2013, le Conseil d'État, section de législation, a été invité par le vice premier ministre et ministre de l'Économie à communiquer un avis, dans un délai de trente jours, sur un avant-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".

L'avant-projet a été examiné par la quatrième chambre le 27 mai 2013. La chambre était composée de Pierre LIÉNARDY, président de chambre, Luc CAMBIER et Bernard BLERO, conseillers d'État, et Colette GIGOT, greffier.

Le rapport a été présenté par Anne VAGMAN, premier auditeur.

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

L'avis, dont le texte suit, a été donné le 27 mai 2013.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 1°, des lois coordonnées sur le Conseil d'État, tel qu'il est remplacé par la loi du 2 avril 2003, la section de législation limite son examen au fondement juridique de l'avant-projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

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

OBSERVATION LIMINAIRE

L'avant-projet à l'examen se donne pour objet de transposer partiellement la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 "sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, et modifiant la directive 2002/58/CE" (ci-après, la directive 2006/24/CE).

L'exposé des motifs doit être complété par la présentation d'un tableau de correspondance entre le texte de l'avant-projet et celui des normes européennes pertinentes afin que les Chambres législatives puissent se prononcer en connaissance de cause sur le choix des moyens mis en œuvre par l'auteur de l'avant-projet, et éviter que l'exercice du droit d'amendement inscrit dans l'article 76 de la Constitution ne

ADVIES VAN DE RAAD VAN STATE NR. 53 272/4 VAN 27 MEI 2013

Op 26 april 2013 is de Raad van State, afdeling Wetgeving, door de vice-eerste minister en minister van Economie verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet "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".

Het voorontwerp is door de vierde kamer onderzocht op 27 mei 2013. De kamer was samengesteld uit Pierre LIÉNARDY, kamervoorzitter, Luc CAMBIER en Bernard BLERO, staatsraden, en Colette GIGOT, griffier.

Het verslag is uitgebracht door Anne VAGMAN, eerste auditeur.

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

Het advies, waarvan de tekst hierna volgt, is gegeven op 27 mei 2013.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 1°, van de gecoördineerde wetten op de Raad van State, zoals het is vervangen bij de wet van 2 april 2003, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

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

INLEIDENDE OPMERKING

Het voorliggende voorontwerp strekt tot de gedeeltelijke omzetting van 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" (hierna richtlijn 2006/24/EG genoemd).

Aan de memorie van toelichting moet een tabel worden toegevoegd waarin voor elke bepaling van het voorontwerp de overeenkomstige bepalingen van de relevante Europese richtlijnen wordt aangegeven, opdat de Wetgevende Kamers zich met kennis van zaken kunnen uitspreken over de middelen die de steller van het voorontwerp heeft gekozen en opdat het amenderingsrecht vervat in artikel 76 van de Grondwet niet

dépasse les limites du pouvoir d'appréciation laissé aux États membres par le droit européen.[1]

Ce tableau de correspondance permettra par ailleurs de vérifier aisément si la transposition des différents articles de la directive 2006/24/CE est complètement ou seulement partiellement assurée et par le biais de quelles dispositions, qu'il s'agisse de dispositions déjà existantes dans l'arsenal juridique belge, des dispositions de l'avant projet examiné ou de dispositions encore à prendre notamment par arrêté royal. Pour éclairer ce dernier aspect, l'auteur de l'avant projet indiquera non seulement les mesures législatives et réglementaires qui devraient encore être adoptées de manière à parfaire la transposition de la directive mais aussi les arrêtés royaux qu'il y aurait lieu de modifier ou d'abroger.

Par ailleurs, pour les raisons évoquées à l'observation générale qui suit, ce tableau devra faire mention de l'article 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 "concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)" (ci-après, la directive 2002/58/CE).

OBSERVATIONS GÉNÉRALES

1. L'article 126 de la loi du 13 juin 2005, tel qu'en vigueur, dispose comme suit:

"§ 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

[1] Principes de technique législative — Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be, onglet "Technique législative", recommandations nos 191 à 195.À cette occasion, la section de législation rappelle que ces tableaux auraient dû lui être communiqués d'initiative.

verder reikt dan de beoordelingsbevoegdheid die de lidstaten krachtens het Europees recht kunnen uitoefenen.[1]

Dankzij die concordantietabel zal overigens makkelijk kunnen worden nagegaan of de omzetting van de onderscheiden artikelen van richtlijn 2006/24/EG volledig of slechts ten dele tot stand wordt gebracht en door middel van welke bepalingen, ongeacht of het gaat om bepalingen die reeds in het Belgische juridisch instrumentarium voorkomen, bepalingen van het voorliggende voorontwerp of bepalingen die nog moeten worden uitgevaardigd, inzonderheid bij koninklijk besluit. Om het laatstgenoemde aspect te verduidelijken, dient de steller van het voorontwerp niet alleen op te geven welke wets- en verordeningsbepalingen nog zouden moeten worden aangenomen om voor een perfecte omzetting van de richtlijn te zorgen, maar ook welke koninklijke besluiten gewijzigd of opgeheven dienen te worden.

Omwille van de redenen die hierna in de algemene opmerking worden aangegeven, moet deze tabel voorts melding maken van artikel 15 van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 "betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)" (hierna richtlijn 2002/58/EG genoemd).

ALGEMENE OPMERKINGEN

1. Artikel 126 van de wet van 13 juni 2005 luidt in de thans geldende versie als volgt:

"§ 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en van de minister en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

§ 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut.

[1] Beginselen van de wetgevingstechniek — Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbevelingen 191 tot 195. Hierbij merkt de afdeling Wetgeving op dat deze tabellen haar spontaan hadden moeten worden overgelegd.

Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique".

2. Lors de son adoption en 2005, cette disposition avait pour objet de mettre en œuvre la possibilité conférée aux États membres par l'article 15 de la directive 2002/58/CE[2].

Cet article 15 disposait comme suit:

"Article 15

Application de certaines dispositions de la directive 95/46/CE

1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques".

La directive 2006/24/CE a inséré, dans cette disposition, un paragraphe 1*bis*, rédigé comme suit:

"1*bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics

De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België".

2. Toen deze bepaling is aangenomen, beoogde ze de mogelijkheid te realiseren die bij artikel 15 van richtlijn 2002/58/EG aan de lidstaten is verleend[2].

Dat artikel 15 luidde als volgt:

"Artikel 15

Toepassing van een aantal bepalingen van Richtlijn 95/46/EG

1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

2. Het bepaalde in hoofdstuk III van Richtlijn 95/46/EG inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

3. De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, ingesteld bij artikel 29 van Richtlijn 95/46/EG, voert de in artikel 30 van die richtlijn vermelde taken ook uit ten aanzien van aangelegenheden die onder de onderhavige richtlijn vallen, namelijk de bescherming van de fundamentele rechten en vrijheden en van rechtmatige belangen in de sector elektronische communicatie".

Richtlijn 2006/24/EG heeft in deze bepaling een lid 1*bis* ingevoegd dat luidt als volgt:

"1*bis*. Lid 1 is niet van toepassing op de uit hoofde van 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 te bewaren

[2] Ceci ressort notamment du tableau de transposition transmis à la section de législation à l'époque, avec la demande d'avis sur l'avant-projet devenu la loi du 13 juin 2005 "relative aux communications électroniques".

[2] Dit blijkt inzonderheid uit de omzettingstabel die destijds samen met de adviesaanvraag over het voorontwerp dat ontstaan heeft gegeven aan de wet van 13 juni 2005 "betreffende de elektronische communicatie" aan de afdeling Wetgeving is overgelegd.

de communication aux fins visées à l'article 1er, paragraphe 1, de ladite directive"[3].

Dans le même temps, la directive 2006/24/CE a mis en place un régime ayant pour objectif "d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne"[4].

Ces données sont "les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur"[5].

Elles ont trait aux services de téléphonie fixe en réseau, de téléphonie mobile, d'accès à l'internet, de courrier électronique par l'internet et de téléphonie par l'internet[6].

3. Le droit européen a donc ainsi mis en place un système double de conservation de certaines données par les opérateurs en matière de communications électroniques:

— l'un, issu de la directive 2002/58/CE, qui offre aux États membres la possibilité de mettre en place des systèmes de conservation de données, en vue de sauvegarder la sécurité nationale, la défense et la sécurité publique, ou d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques;

— l'autre, issu de la directive 2006/24/CE, qui, dans un but d'harmonisation en vue d'éliminer des entraves au marché intérieur[7], impose aux États membres, de mettre en place un système de conservation de données afin de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne (par exemple, la criminalité organisée et les actes de terrorisme[8]).

gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden"[3].

Tegelijkertijd heeft richtlijn 2006/24/EG een regeling opgezet met als doel "een harmonisatie tot stand te brengen van de nationale bepalingen van de lidstaten waarbij aan aanbieders van elektronische communicatiediensten of een openbaar communicatienetwerk verplichtingen worden opgelegd inzake het bewaren van bepaalde gegevens die door hen gegenereerd of door hen worden verwerkt, teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten"[4].

Deze gegevens zijn de "verkeers- en locatiegegevens, en de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren"[5].

Ze hebben betrekking op de diensten voor telefonie over een vast netwerk, voor mobiele telefonie, voor internettoegang, e-mail over het internet en voor internettelefonie[6].

3. Het Europees recht heeft zodoende een tweeledige regeling opgezet waarmee de operatoren inzake elektronische communicatie bepaalde gegevens bewaren:

— de ene regeling komt voort uit richtlijn 2002/58/EG en biedt de lidstaten de mogelijkheid om de gegevensbewaring te regelen teneinde de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen of ervoor te zorgen dat strafbare feiten of onbevoegd gebruik van het elektronische-communicatiesysteem worden voorkomen, onderzocht, opgespoord en vervolgd;

— de andere regeling komt voort uit richtlijn 2006/24/EG en streeft ernaar de veschillende nationale wetgevingen op elkaar af te stemmen teneinde te voorkomen dat de werking van de interne markt wordt belemmerd[7]; ze verplicht de lidstaten een regeling voor gegevensbewaring in te voeren om te garanderen dat deze gegevens beschikbaar zijn om ernstige strafbare feiten zoals gedefinieerd in de nationale wetgevingen van de lidstaten, (bijvoorbeeld georganiseerde misdaad en terroristische daden) te onderzoeken, op te sporen en te vervolgen[8].

---

3 Quant à la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, elle a inséré, dans le même article, un paragraphe 1er*ter*, rédigé comme suit:
"1*ter.* Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1er, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse".

4 Article 1er, paragraphe 1er, de la directive 2006/24/CE.

5 Article 2, paragraphe 2, a), de la directive 2006/24/CE.

6 Article 5 de la directive 2006/24/CE.

7 Voir le considérant (6) de la directive 2006/24/CE.

8 Voir les considérants (7), (8) et (10) de la directive 2006/24/CE.

3 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 heeft in hetzelfde artikel een lid 1ter ingevoegd, luidende als volgt:
"1*ter.* Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord".

4 Artikel 1, lid 1, van richtlijn 2006/24/EG.

5 Artikel 2, lid 2, a), van richtlijn 2006/24/EG.

6 Artikel 5 van richtlijn 2006/24/EG.

7 Zie overweging (6) van richtlijn 2006/24/EG.

8 Zie overwegingen (7), (8) en (10) van richtlijn 2006/24/EG.

Comme la Commission européenne l'a relevé:

"Cette relation juridique compliquée entre la directive [2006/24/CE] et la directive [2002/58/CE], à laquelle s'ajoute l'absence de définition, dans les deux instruments, de la notion d''infraction grave', rend malaisée toute distinction entre, d'une part, les mesures prises par les États membres pour transposer les obligations relatives à la conservation des données énoncées dans la directive et, d'autre part, la pratique plus générale de conservation des données dans les États membres qu'autorise l'article 15, paragraphe 1, de la directive [2002/58/CE]"[9].

Concernant cette difficulté de distinguo, et s'agissant plus spécialement de la définition de la finalité de conservation des données concernées, il y a lieu de relever que tant l'article 126 en vigueur de la loi du 13 juin 2005, que l'article 126 en projet imposent la conservation de données dans des buts qui dépassent largement les finalités prévues par la directive 2006/24/CE, à savoir "des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne".

Ainsi, le paragraphe 4 de la disposition en projet prévoit que:

"§ 2. Les données visées au paragraphe 1er, al. 1er, sont conservées en vue:

a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46*bis* et 88*bis* du Code d'Instruction criminelle;

b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107;

c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

d) de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité".

Concernant la circonstance que les dispositions en matière de conservation des données en vigueur dans les États membre postérieurement à l'adoption de la directive 2006/24/CE imposent, dans de nombreux cas[10], la conservation de certaines données en vue de rencontrer des objectifs dépassant la recherche, la détection et la poursuite "d'infractions graves

De Commissie heeft het volgende gesteld:

"Dit ingewikkelde juridische verband tussen de richtlijn gegevensbewaring en de e privacyrichtlijn maakt het, mede vanwege het ontbreken van een definitie in beide richtlijnen van het begrip 'ernstige criminaliteit', moeilijk om maatregelen die de lidstaten nemen om de gegevensbewaringsverplichtingen van de richtlijn om te zetten, te onderscheiden van de meer algemene praktijk in de lidstaten om gegevens te bewaren op grond van artikel 15, lid 1, van de e-privacyrichtlijn".[9]

In verband met de moeilijkheid die dit subtiel onderscheid doet rijzen, inzonderheid inzake de definitie van het doeleinde waarmee de betreffende gegevens worden bewaard, moet worden opgemerkt dat het oogmerk waarmee zowel krachtens het thans geldende artikel 126 van de wet van 13 juni 2005 als krachtens het ontworpen artikel 126 gegevens worden bewaard, beduidend verder reikt dan de doelstellingen bepaald in richtlijn 2006/24/EG, te weten "het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten".

Aldus luidt paragraaf 4 van de ontworpen bepaling als volgt:

"§ 2. De gegevens beoogd in paragraaf 1, eerste lid, worden bewaard met het oog op:

a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46bisen 88*bis* van het Wetboek van Strafvordering;

b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of dienst, zoals bedoeld in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten".

Betreffende de omstandigheid dat de bepalingen inzake gegevensbewaring die na de aanneming van richtlijn 2006/24/EG in de Europese lidstaten van kracht zijn geworden, in tal van gevallen[10] voorschrijven bepaalde gegevens te bewaren teneinde doelstellingen te verwezenlijken die verder reiken dan het onderzoeken, opsporen en vervolgen van "ernstige

9 COM(2011) 225 final du 18 avril 2011 — Rapport de la Commission au Conseil et au Parlement européen d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE), p. 5.

10 Comme c'est déjà le cas de l'article 126 en vigueur de la loi du 13 juin 2005.

9 COM(2011) 225 definitief van 18 april 2011 — Evaluatieverslag van de Commissie aan de Raad en het Europees Parlement van de richtlijn gegevensbewaring (Richtlijn 2006/24/EG), 5.

10 Zoals reeds het geval is met het thans geldende artikel 126 van de wet van 13 juni 2005.

telles qu'elles sont définies par chaque État membre dans son droit interne", la Commission européenne a relevé ce qui suit:

"La plupart des États membres qui ont transposé la directive autorisent, dans leur législation, l'accès aux données conservées et leur utilisation pour des finalités dépassant celles couvertes par la directive, comme la prévention et la répression de la criminalité en général et les risques pour la vie humaine. Si la directive sur la vie privée autorise ce dépassement, le degré d'harmonisation obtenu par la législation de l'UE à cet égard demeure limité. Or, si les finalités de la conservation des données diffèrent d'un pays à l'autre, cela risque d'affecter le volume et la fréquence des demandes et, par conséquent, les coûts qu'implique le respect des obligations fixées par la directive. De plus, cette situation ne répondrait pas suffisamment à l'exigence de prévisibilité à laquelle est soumise toute mesure législative qui restreint le droit à la vie privée[11]. La Commission évaluera la nécessité d'une harmonisation plus poussée dans ce domaine et les options pour y parvenir[12]"[13].

4. Il résulte des considérations qui précèdent que les États membres peuvent prévoir, sur la base de la directive 2002/58/CE, des systèmes imposant aux opérateurs de conserver de données dans des buts qui dépassent celui prévu par la directive 2006/24/CE, tout en respectant toutefois certaines conditions, étant celles fixées par l'article 15 de la directive 2002/58/CE.

C'est le système retenu par l'article 126 en projet: cette disposition non seulement transpose certes la directive 2006/24/CE, mais en outre, en tant qu'elle dépasse l'objectif lié aux "infractions graves" assigné par cette directive, elle fait écho et trouve appui sur l'article 15 de la directive 2002/58/CE.

Il reste que, vu la complexité du droit européen et, pour reprendre les termes de la Commission européenne, vu "la relation juridique compliquée" entre la directive 2006/24/CE et la directive 2002/58/CE, il est permis de se demander si la solution qui serait la plus de nature à garantir le respect du droit européen ne consisterait pas à mettre en place deux

[11] Note de bas de page 40 du rapport cité: Arrêt de la Cour de justice du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01 (demande de décision préjudicielle du *Verfassungsgerichtshof* et l'*Oberster Gerichtshof)*: *Rechnungshof* (C-465/00) contre *Österreichischer Rundfunk* et autres, et Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) contre *Österreichischer Rundfunk* (Protection des personnes physiques à l'égard du traitement de données à caractère personnel — Directive 95/46/CE — Protection de la vie privée — Divulgation des données sur les revenus de salariés d'entités soumises au contrôle du *Rechnungshof*).

[12] Note de bas de page 41 du rapport cité: Lors de l'adoption de la directive, la Commission avait publié une déclaration suggérant de retenir la liste des infractions figurant dans le mandat d'arrêt européen (décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres).

[13] Voir COM(2011) 225 final du 18 avril 2011, op. cit., p. 7 à 10, spéc. p. 10.

criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten", heeft de Europese Commissie het volgende opgemerkt:

"De meeste lidstaten die de richtlijn hebben omgezet, gaan, in overeenstemming met hun nationale wetgeving, verder in het toestaan van toegang tot en gebruik van bewaarde gegevens dan de richtlijn zelf, bijvoorbeeld voor het voorkomen en bestrijden van criminaliteit in het algemeen en van gevaar voor lijf en leden. Hoewel dit is toegestaan uit hoofde van de e-privacyrichtlijn, blijft de mate van harmonisatie die met EU-wetgeving tot stand is gekomen op dit gebied beperkt. Verschillen in het doel van de gegevensbewaring hebben gevolgen voor het aantal en de frequentie van de verzoeken en dus ook voor de kosten die moeten worden gemaakt voor het nakomen van de verplichtingen die voortvloeien uit de richtlijn. Bovendien biedt deze situatie wellicht in onvoldoende mate de voorspelbaarheid die vereist is bij elke wetgevende maatregel die het recht op privacy beperkt[11]. De Commissie zal nagaan of en hoe verdere harmonisatie op dit vlak moet worden verwezenlijkt[12]"[13].

4. Uit de voorgaande overwegingen blijkt dat de lidstaten op basis van richtlijn 2002/58/EG regelingen kunnen opzetten die de operatoren verplichten gegevens te bewaren met oogmerken die verder reiken dan het oogmerk bepaald door richtlijn 2006/24/EG, met naleving evenwel van bepaalde voorwaarden die zijn vastgesteld door artikel 15 van richtlijn 2002/58/EG.

Dat is de regeling die door het ontworpen artikel 126 in aanmerking wordt genomen: deze bepaling zet niet alleen richtlijn 2006/24/EG om, maar beantwoordt bovendien aan en vindt steun in artikel 15 van richtlijn 2002/58/EG in zoverre ze verder reikt dan de doelstelling in verband met de "ernstige criminaliteit" die door deze richtlijn wordt aangegeven.

Desalniettemin, gelet op de complexiteit van het Europees recht en, om de bewoordingen van de Europese Commissie aan te halen, gelet op "dit ingewikkelde juridische verband" tussen richtlijn 2006/24/EG en richtlijn 2002/58/EG, kan men zich afvragen of de beste oplossing om te garanderen dat het Europees recht wordt nageleefd er niet in bestaat

[11] Voetnoot 40 van het geciteerde verslag: Arrest van het Europese Hof van Justitie van 20 mei 2003 in gevoegde zaken C-465/00, C-138/01 en C-139/01 (verzoeken om een prejudiciële beslissing van het *Verfassungsgerichtshof* en het *Oberster Gerichtshof*: *Rechnungshof* (C-465/00) tegen *Österreichischer Rundfunk* en anderen en Christa Neukomm (C-138/01) en Joseph Lauermann (C-139/01) tegen *Österreichischer Rundfunk* (Bescherming van natuurlijke personen bij de verwerking van persoonsgegevens — Richtlijn 95/46/EG — Bescherming van persoonlijke levenssfeer — Bekendmaking van gegevens over het inkomen van werknemers van rechtspersonen die onder toezicht van het Rechnungshof staan).

[12] Voetnoot 41 van het geciteerde verslag: Bij de goedkeuring van de richtlijn heeft de Commissie een verklaring uitgegeven waarin zij voorstelt de lijst van strafbare feiten in het Europees aanhoudingsbevel in overweging te nemen (Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten).

[13] Zie COM(2011) 225 definitief van 18 april 2011, op.cit., 7-10, inzonderheid 10.

systèmes parallèles, l'un transposant la directive 2006/24/CE, l'autre s'appuyant sur la directive 2002/58/CE. À cet égard, la section de législation observe par ailleurs que les considérants 15 et 16 du préambule de la directive 2006/24/CE mentionnent que "[l]a directive 95/46/CE et la directive 2002/58/CE sont pleinement applicables aux données conservées conformément à la [directive 2006/24/CE]".

Quoi qu'il en soit, dès lors que l'auteur de l'avant projet a opté pour un système qui s'appuie sur les deux directives précitées, il est tenu de respecter le double cadre juridique européen auquel il est fait écho.

Les observations particulières qui suivent prennent en compte cette exigence.

OBSERVATIONS PARTICULIÈRES

ARRÊTÉ DE PRÉSENTATION

L'arrêté de présentation sera rédigé comme suit:

"ALBERT II, Roi des Belges,

À tous, présents et à venir, Salut.

Sur la proposition du ministre de l'Economie et du ministre de la Justice,

NOUS AVONS ARRÊTE ET ARRÊTONS:

Le ministre de l'Économie et la ministre de la Justice sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:"[14].

DISPOSITIF

Article 1er nouveau

Un article premier nouveau doit être inséré dans l'avant-projet à l'examen, qui sera rédigé comme suit:

"Art. 1er. La présente loi règle une matière visée à l'article 78 de la Constitution"[15].

Les autres articles seront renumérotés en conséquence.

[14] Principes de technique législative — Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be, onglet "Technique législative", recommandations nos 226 et 227, formule F 5.

[15] Voir l'article 83 de la Constitution et l'article 2, § 1er, alinéa 2, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973.

twee naast elkaar bestaande regelingen op te zetten: een regeling die richtlijn 2006/24/EG omzet en een andere regeling die op richtlijn 2002/58/EG steunt. In dit verband merkt de afdeling Wetgeving voorts op dat in overwegingen 15 en 16 van de aanhef van richtlijn 2006/24/EG wordt vermeld dat "de Richtlijnen 95/46/EG en 2002/58/EG integraal van toepassing zijn op de overeenkomstig (…) richtlijn [2006/24/EG] bewaarde gegevens".

Hoe het ook zij, daar de steller van het voorontwerp heeft gekozen voor een regeling die op de twee voornoemde richtlijnen steunt, moet hij het tweeledige juridisch kader naleven waarop hij zich beroept.

In de bijzonder opmerkingen die hierna volgen, wordt met dit vereiste rekening gehouden.

BIJZONDERE OPMERKINGEN

INDIENINGSBESLUIT

Het indieningsbesluit moet worden gesteld als volgt:

"ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Op de voordracht van de minister van Economie en van de minister van Justitie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Economie en de minister van Justitie zijn ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze naam aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen:".[14]

DISPOSITIEF

Nieuw artikel 1

In het voorliggende voorontwerp moet een nieuw artikel 1 worden ingevoegd, luidende als volgt:

"Art. 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet".[15]

De andere artikelen moeten dienovereenkomstig worden hernummerd.

[14] Beginselen van de wetgevingstechniek — Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbevelingen 226 en 227, formule F 5

[15] Zie artikel 83 van de Grondwet en artikel 2, § 1, tweede lid, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973.

Article 3
(devenant article 4)

L'article 3 de l'avant-projet entend remplacer l'article 126 de la loi du 13 juin 2005 "relative aux communications électroniques".

Outre l'observation générale ci-avant, l'article 126 en projet appelle les observations suivantes.

1. S'agissant des transmissions de données qui seront réalisées en vertu de l'article 126, § 2, alinéa 1er, a) et d) en projet, les articles du Code d'instruction criminelle et de la loi du 30 novembre 1998 'organique des services de renseignement et de sécurité' visés, comportent des éléments essentiels relatifs aux cas et procédures à suivre en la matière. Le commentaire des articles relatif au texte en projet précise par ailleurs ce qui suit:

"Les modalités pratiques d'accès des services publics concernés aux données conservées par les fournisseurs ne sont pas réglées dans le présent avant-projet de loi ni dans son arrêté d'exécution mais dans d'autres législations. On citera à cet égard par exemple l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité.

Par ailleurs, tant le procureur du Roi que le juge d'instruction, chacun pour leurs 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 des données conservées. À cet égard, il convient de souligner que le fait de pouvoir avoir accès à ces données conservées peut tout autant permettre aux autorités judiciaires d'inculper la personne que de l'innocenter".

Concernant les transmissions de données qui seront réalisées en vertu de l'article 126, § 2, alinéa 1er, b) et c) en projet, par contre, tant le texte en projet que les dispositions législatives auxquelles il est renvoyé sont muets sur l'autorité et, surtout, sur les modalités précises selon lesquelles les données seront demandées et transmises. Le commentaire des articles n'apporte pas d'explication complémentaire.

S'agissant d'un régime de nature à porter atteinte à un droit fondamental étant la protection de la vie privée, il convient que le législateur fixe lui-même les éléments essentiels du régime de ces transmissions.

Le texte en projet sera complété en conséquence.

Artikel 3
(dat artikel 4 wordt)

Artikel 3 van het voorontwerp strekt ertoe artikel 126 van de wet van 13 juni 2005 "betreffende de elektronische communicatie" te vervangen.

Naast de algemene opmerking hierboven geeft het ontworpen artikel 126 aanleiding tot de volgende opmerkingen.

1. In verband met de overdracht van de gegevens die zal plaatsvinden krachtens het ontworpen artikel 126, § 2, eerste lid, a) en d), bevatten de vermelde artikelen van het Wetboek van Strafvordering en van de wet van 30 november 1998 'houdende regeling van de inlichtingen- en veiligheidsdiensten' elementen die van wezenlijk belang zijn voor de betreffende situaties en de procedures die ter zake moeten worden gevolgd. De artikelsgewijze toelichting met betrekking tot de ontworpen tekst luidt voorts als volgt:

"De praktische werkwijze voor toegang tot de door de aanbieders bewaarde gegevens voor de overheidsdiensten, wordt niet geregeld in dit voorontwerp van wet noch in het bijbehorende uitvoeringsbesluit maar in andere wetgevingen. Zie ook in dit kader bijvoorbeeld het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en het koninklijk besluit van 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie.

Zowel de procureur des Konings als de onderzoeksrechter, elk voor hun eigen bevoegdheden, moeten trouwens 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".

In verband met de overdracht van de gegevens die zal plaatsvinden krachtens het ontworpen artikel 126, § 2, eerste lid, b) en c), wordt in de ontworpen tekst en in de wetsbepalingen waarnaar wordt verwezen, evenwel niets gezegd over de overheidsinstanties en, bovenal, evenmin over de precieze regels voor het aanvragen en overdragen van de gegevens. De artikelsgewijze toelichting bevat geen bijkomende uitleg.

Aangezien het een regeling betreft die strijdig kan zijn met een grondrecht, te weten de bescherming van de persoonlijke levenssfeer, moet de wetgever zelf de kernpunten van de regeling inzake deze overdracht vastleggen.

De ontworpen tekst moet dienovereenkomstig worden aangevuld.

2. S'agissant du même paragraphe, la section de législation se demande si l'hypothèse visée par l'alinéa 1er, b), n'est pas déjà couverte par le a) du même alinéa.

3. L'article 126, § 3, alinéas 1er et 2, en projet, est rédigé comme suit:

"§ 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées a partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de dernière communication entrante ou sortante enregistrée.

Les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication".

Le commentaire de l'article 126, § 3, en projet justifie comme suit cette différence de régime:

"Pour ce qui concerne le point de départ du délai de conservation, le paragraphe 3 de l'article 126 fait la distinction suivante.

Les données de trafic et de localisation sont conservées pendant douze mois à partir de la date de la communication.

Par contre, les données visant à identifier les utilisateurs finals, le service de communications électroniques utilise et l'équipement terminal qui est présumé avoir été utilise (ci-après les données d'identification) sont conservées dès la souscription au service, que ce soit dans le cadre d'un abonnement ou non, aussi longtemps qu'une communication entrante ou sortante est possible á l'aide du service souscrit et pendant douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.

Dans la pratique, une communication est parfois encore possible après la fin de l'abonnement ou, lorsqu'un abonnement n'a pas été contracté, après la fin de la durée de validité du service, ainsi que les exemples suivants l'illustrent:

— il existe des formules d'abonnement où l'abonné ne peut plus établir de communications sortantes lui-même à la fin de l'abonnement, mais où il peut encore recevoir des communications entrantes pendant trois mois;

— pour les cartes prépayées pour la téléphonie mobile, où l'utilisateur peut encore être appelé pendant trois mois après que son propre crédit d'appel ait été utilisé.

Le point de départ du délai de conservation est fonction du type de données à conserver. Or, ces données à conserver sont fixées précisément dans l'arrêté royal d'exécution de l'article 126. Par conséquent, alors que les principes en la matière sont fixés dans le paragraphe 3 de l'article 126, c'est l'arrêté royal précité qui précise quel point de départ du délai de conservation s'applique a quelle donnée.

2. In verband met dezelfde paragraaf vraagt de afdeling Wetgeving zich af of het geval dat in het eerste lid, b), bedoeld wordt, niet reeds in de bepaling onder a) van hetzelfde lid wordt behandeld.

3. Het ontworpen artikel 126, § 3, eerste en tweede lid, luidt als volgt:

"§ 3. De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronischecommunicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie".

In de toelichting op het ontworpen artikel 126, § 3, wordt dit verschil in regeling als volgt gerechtvaardigd:

"Wat betreft het startpunt voor de bewaringstermijn, maakt paragraaf 3 van artikel 126 het volgende onderscheid.

De verkeers- en locatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie.

De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur (hierna "identificatiegegevens") worden daarentegen bewaard vanaf de inschrijving op de dienst, ongeacht of dit in het kader van een abonnement is of niet, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

In de praktijk is communicatie soms nog mogelijk na afloop van het abonnement of, wanneer geen abonnement werd genomen, na afloop van de geldigheidsduur van de dienst, zoals blijkt uit de volgende voorbeelden:

— er bestaan abonnementsformules waarbij de abonnee zelf geen uitgaande communicatie meer tot stand kan brengen op het einde van het abonnement, maar hij wel nog inkomende communicatie kan ontvangen gedurende drie maanden;

— voorafbetaalde kaarten voor mobiele telefonie, waarbij de gebruiker nog gedurende drie maanden kan worden gebeld nadat zijn eigen belkrediet is opgebruikt.

Het beginpunt voor de bewaringstermijn hangt af van het te bewaren type van gegevens. Deze te bewaren gegevens worden overigens nauwkeurig vastgelegd in het koninklijk besluit tot uitvoering van artikel 126. Bijgevolg, terwijl de principes ter zake worden bepaald in paragraaf 3 van artikel 126, is het het voorgaande koninklijk besluit dat het beginpunt bepaalt voor de bewaringstermijn voor elk gegeven.

L'article 126, paragraphe 3, alinéa 1er, qui vise les données d'identification, ne reprend pas le libellé de l'article 6 de la directive qui prévoit que le point de départ pour le calcul du délai de conservation est la 'date de la communication'. En effet, ce libellé est adéquat pour les données de trafic et de localisation dès lors que ces données sont particulières à chaque communication et doivent être conservées pour chaque communication. Par contre, ce libellé est difficile a appliquer aux données d'identification qui ne constituent pas en tant que telles des communications et qui peuvent exister indépendamment de toute communication.

Si la date de la communication était également prise comme point de départ pour le calcul du délai de conservation pour les données d'identification, alors

— les fournisseurs n'auraient pas l'obligation de conserver ces données entre la date de la souscription au service et la première communication;

— les fournisseurs n'auraient pas l'obligation de conserver ces données en l'absence de communication, alors qu'il est possible que des appels infructueux soient adressés à un utilisateur final, qui sont une indication d'un lien avec d'autres parties;

— les fournisseurs devraient conserver ces données d'identification pour chaque communication, de la première jusqu'à la dernière communication, ce qui augmenterait le volume des données à conserver.

Dès lors, l'article 126, paragraphe 3, alinéa 1er, reprend le principe posé par la directive (délai de conservation de douze mois à compter de la dernière communication) mais se limite à imposer aux fournisseurs de conserver une seule fois les données d'identification au début de la souscription au service".

L'on peut comprendre la logique de la justification ainsi donnée, la question se pose toutefois de savoir si le système ainsi mis en place ne dépasse pas dans certaines hypothèses la limite du délai de conservation des données qui résulte de la combinaison des articles 5 et 6 de la directive 2006/24/CE.

4. Afin de se conformer à l'article 7, d), de la directive 2006/24/CE, l'article 126, § 5, alinéa 1er, 4°, sera rédigé comme suit:

"4° veille à ce que les données conservées soient détruites lorsqu'est expiré le délai de conservation applicable à ces données, à l'exception des données auxquelles on a pu accéder et qui ont été préservées".

5. L'article 7, c), de la directive 2006/24/CE impose aux États membres de veiller

Artikel 126, paragraaf 3, eerste lid, dat de identificatiegegevens beoogt, gebruikt niet de formulering van artikel 6 van de richtlijn, dat bepaalt dat het startpunt voor de berekening van de bewaringstermijn de 'datum van de communicatie' is. Die formulering is inderdaad gepast voor de verkeers- en locatiegegevens omdat die gegevens specifiek zijn voor elke communicatie en moeten worden bewaard voor elke communicatie. Die formulering kan daarentegen maar moeilijk worden toegepast op de identificatiegegevens die niet aldus communicatie vormen en die los van alle communicatie kunnen bestaan.

Indien de communicatiedatum ook als startpunt zou worden genomen voor de berekening van de bewaringstermijn voor de identificatiegegevens, dan:

— zouden de aanbieders niet verplicht zijn om deze gegevens te bewaren tussen de datum van inschrijving op de dienst en de eerste communicatie;

— zouden de aanbieders niet verplicht zijn om deze gegevens te bewaren indien er geen communicatie plaatsvindt, terwijl het mogelijk is dat mislukte oproepen worden gedaan naar een eindgebruiker, die een indicatie zijn van een link met andere partijen;

— zouden de aanbieders deze identificatiegegevens moeten bewaren voor elke communicatie, van de eerste tot de laatste communicatie, wat het volume van te bewaren gegevens zou vergroten.

Artikel 126, paragraaf 3, eerste lid, neemt dan ook het principe over van de richtlijn (bewaringstermijn van twaalf maanden vanaf de laatste communicatie) maar beperkt zich ertoe de aanbieders te verplichten om één enkele keer de identificatiegegevens te bewaren aan het begin van de inschrijving op de dienst".

De logica van de aldus geformuleerde rechtvaardiging valt te begrijpen, maar de vraag rijst of met de regeling die hier wordt opgezet in sommige gevallen de termijn voor de gegevensbewaring, zoals die naar voren komt wanneer de artikelen 5 en 6 van richtlijn 2006/24/EG in onderling verband worden gelezen, niet wordt overschreden.

4. Ter wille van de overeenstemming met artikel 7, d), van richtlijn 2006/24/EG, moet artikel 126, § 5, eerste lid, 4°, gesteld worden als volgt:

"4° hij zorgt ervoor dat de gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, worden vernietigd, met uitzondering van de geraadpleegde en vastgelegde gegevens".

5. Artikel 7, c), van richtlijn 2006/24/EG verplicht de lidstaten erop toe te zien:

"à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications respectent au minimum les principes suivants en matière de sécurité des données, pour ce qui concerne les données conservées conformément à la présente directive:

[…]

c) les données font l'objet de mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé;".

Afin d'assurer la transposition correcte de cette disposition, l'article 126, § 5, alinéa 1er, 3°, en projet, doit prévoir non pas que l'accès aux données conservées n'est effectué "qu'à la demande et sous la surveillance de la Cellule de Coordination de Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques", mais que cet accès n'est effectué que "par un ou plusieurs membres de la Cellule de Coordination de Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques".

La disposition à l'examen sera modifiée en conséquence.

6. L'article 3, paragraphe 2, de la directive 2006/24/CE dispose comme suit:

"L'obligation de conserver les données visées au paragraphe 1 inclut la conservation des données visées à l'article 5 relatives aux appels téléphoniques infructueux, lorsque ces données sont générées ou traitées, et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet), dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'État membre concerné. La présente directive n'impose pas la conservation des données relatives aux appels non connectés".

L'article 126 en projet ne comporte aucune subdivision ayant pour objet de transposer cette disposition de droit européen.

Compte tenu de ce que l'article 3, paragraphe 2, reproduit ci-avant porte sur l'objet même de l'obligation de conserver les données concernées, et a ainsi trait à un élément essentiel de cette obligation, c'est au législateur qu'il appartient de transposer ledit article 3, paragraphe 2, et non, éventuellement, au pouvoir exécutif.

"dat de aanbieders van elektronische communicatiediensten of de aanbieders van een publiek communicatienetwerk ten minste de volgende beginselen van gegevensbeveiliging respecteren met betrekking tot gegevens die bewaard worden overeenkomstig deze richtlijn:

[…]

c) de gegevens worden onderworpen aan passende technische en organisatorische maatregelen om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen,".

Teneinde ervoor te zorgen dat deze bepaling naar behoren wordt omgezet, moet in het ontworpen artikel 126, § 5, eerste lid, 3° niet worden bepaald dat de toegang tot de bewaarde gegevens "enkel op verzoek van en onder het toezicht van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie gebeurt", maar dat deze toegang "door een of meerdere leden van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie plaatsvindt".

De voorliggende bepaling moet dienovereenkomstig worden gewijzigd.

6. Artikel 3, lid 2, van richtlijn 2006/24/EG luidt als volgt:

"De verplichting tot gegevensbewaring voorzien in lid 1 omvat de bewaring van de in artikel 5 bedoelde gegevens betreffende oproeppogingen zonder resultaat waarbij die gegevens, voor zover die in verband met de aanbieding van de bedoelde communicatiediensten worden gegenereerd, verwerkt en opgeslagen (wat telefoniegegevens betreft) of gelogd (wat internetgegevens betreft) door onder de rechtsmacht van de betrokken lidstaat vallende aanbieders van openbaar beschikbare elektronische communicatiediensten of van een openbaar communicatienetwerk. Deze richtlijn bevat geen vereisten betreffende de bewaring van gegevens in verband met niet tot stand gekomen verbindingen".

Het ontworpen artikel 126 bevat geen onderverdeling die strekt tot omzetting van deze Europeesrechtelijke bepaling.

Gelet op het feit dat het hierboven aangehaalde artikel 3, lid 2, betrekking heeft op het voorwerp zelf van de verplichting de betreffende gegevens te bewaren, en dus op een wezenlijk onderdeel van deze verplichting, staat het aan de wetgever en niet, in voorkomend geval, aan de uitvoerende macht om het voornoemde artikel 3, lid 2, om te zetten.

Le texte en projet sera complété en conséquence, y compris l'ajout de la notion "d'appel téléphonique infructueux"[16] parmi les définitions de l'article 2 de l'avant-projet de loi.

*

Le greffier, *Le président,*

Colette GIGOT Pierre LIÉNARDY

De ontworpen tekst moet dienovereenkomstig worden aangevuld, inclusief de toevoeging van het begrip "oproeppoging zonder resultaat"[16] aan de definities in artikel 2 van het voorontwerp van wet.

*

De griffier, *De voorzitter,*

Colette GIGOT Pierre LIÉNARDY

[16] Voir l'article 2, paragraphe 2, f), de la directive 2006/24/CE.

[16] Zie artikel 2, lid 2, f), van richtlijn 2006/24/EG.

PROJET DE LOI

ALBERT II, Roi des Belges,

À tous, présents et à venir,

Salut.

Sur la proposition du Ministre de l'Economie et de la Ministre de la Justice;

Nous avons arrêté et arrêtons:

Le Ministre de l'Economie et la Ministre de la Justice sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1er

Objet

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

La présente loi transpose partiellement en droit belge la directive 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 (directive "conservation de données") (J.O. 13 avril 2006, L 105/54) et l'article 15.1 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques") (J.O. 31 juillet 2002, L 201/37).

WETSONTWERP

ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen,

Onze Groet.

Op de voordracht van de Minister van Economie en van de Minister van Justitie;

hebben Wij besloten en besluiten Wij:

De Minister van Economie en de Minister van Justitie zijn ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze naam aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen:

HOOFDSTUK 1

Doel

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Deze wet zet 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 ("Dataretentierichtlijn") (PB, 13 april 2006, L 105/54) en artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ("richtlijn betreffende privacy en elektronische communicatie") (PB, 31 juli 2002, L 201/37) gedeeltelijk om in Belgisch recht.

CHAPITRE 2

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

Art. 2

L'article 1er de la loi du 13 juin 2005 relative aux communications électroniques, complété par la loi du 10 juillet 2012, est complété par un alinéa rédigé comme suit:

"La présente loi transpose partiellement la directive 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 (directive "conservation de données") (J.O. 13 avril 2006, L 105/54) et l'article 15.1 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques") (J.O. 31 juillet 2002, L 201/37).".

Art. 3

L'article 2, 11°, de la même loi est remplacé par ce qui suit:

"11° "opérateur": toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;".

Art. 4

L'article 2, de la même loi, est complété par ce qui suit:

"74° "Appels infructueux": toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau.".

Art. 5

L'article 126 de la même loi est remplacé par ce qui suit:

"Art. 126. § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard

HOOFDSTUK 2

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

Art. 2

Artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, aangevuld bij de wet van 10 juli 2012, wordt aangevuld met een lid luidende:

"Deze wet voorziet in een gedeeltelijke omzetting van 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 ("Dataretentierichtlijn") (PB 13 april 2006, L 105/54) en van artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB, 31 juli 2002, L 201/37).".

Art. 3

Artikel 2, 11°, van dezelfde wet wordt vervangen als volgt:

"11° "operator": een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9;".

Art. 4

Artikel 2 van dezelfde wet wordt aangevuld als volgt:

"74° "Oproeppoging zonder resultaat": een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord.".

Art. 5

Artikel 126 van dezelfde wet wordt vervangen als volgt:

"Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer

des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic, les données de localisation, les données d'identification d'utilisateurs finals, les données d'identification du service de communications électroniques utilisé et les données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Par fournisseurs au sens du présent article, on entend également les revendeurs en nom propre et pour leur propre compte.

Par service de téléphonie au sens du présent article, on entend les appels téléphoniques – notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données –, les services supplémentaires – notamment le renvoi ou le transfert d'appels – et les services de messagerie et multimédias, notamment les services de messages brefs (SMS), les services de médias améliorés (EMS) et les services multimédias (MMS).

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de service en application de l'alinéa 1er ainsi que les exigences auxquelles ces données doivent répondre.

Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée.

L'obligation de conserver les données visées à l'alinéa 1er s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés:

1° en ce qui concerne les données de la téléphonie, générées, traitées et stockées par les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou;

2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.

ten opzichte van de verwerking van persoonsgegevens, bewaren de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, of internettelefoniediensten, en de aanbieders van de onderliggende openbare elektronische- communicatienetwerken de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische-communicatiedienst en de gegevens voor identificatie van de vermoedelijk gebruikte eindapparatuur, die door hen worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten.

Onder aanbieders in de betekenis van dit artikel worden ook de doorverkopers in eigen naam en voor eigen rekening verstaan.

Onder telefoniedienst in de betekenis van dit artikel wordt verstaan: telefoonoproepen – met inbegrip van spraakoproepen, voicemail, conference call of data-communicatie-, aanvullende diensten -met inbegrip van call forwarding en call transfer-, en de messaging- en multimediadiensten – met inbegrip van short message service (sms), enhanced media service (EMS) en multimedia service (MMS).

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de krachtens het eerste lid te bewaren gegevens per type dienst alsook de vereisten waaraan deze gegevens moeten beantwoorden.

Behoudens andersluidende wettelijke bepaling, mogen geen gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, bewaard worden.

De verplichting om de in het eerste lid bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:

1° wat de telefoniegegevens betreft, worden gegenereerd, verwerkt en opgeslagen door de aanbieders van openbare diensten voor elektronische communicatie of van een openbaar netwerk voor elektronische communicatie, of;

2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.

§ 2. Les données visées au paragraphe 1er , alinéa 1er, sont conservées en vue:

a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle;

b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107;

c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

d) de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 1er, alinéa 1er , soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières.

§ 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées à partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.

Les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises au premier alinéa et celles au deuxième.

§ 4. A la suite du rapport d'évaluation visé au paragraphe 7, le Roi peut, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de la

§ 2. De gegevens beoogd in paragraaf 1, eerste lid, worden bewaard met het oog op:

a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering;

b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;

c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of –dienst, zoals bedoeld in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en 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.

§ 3. De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.

De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de gegevens die zijn onderworpen aan het eerste lid en deze die zijn onderworpen aan het tweede lid.

§ 4. Naar aanleiding van het evaluatieverslag beoogd in paragraaf 7, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het

Commission de la protection de la vie privée, adapter le délai de conservation des données pour certaines catégories de données, sans ce que ce délai ne puisse dépasser 18 mois.

Le Roi peut, dans les circonstances visées à l'article 4, § 1er, par arrêté délibéré en Conseil des ministres, et après avis de l'Institut et de la Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à douze mois.

Lorsque, dans les circonstances visées à l'alinéa 2, le Roi fixe un délai de conservation supérieur à vingt-quatre mois, le ministre notifie immédiatement à la Commission européenne et aux autres États membres de l'Union européenne toute mesure prise, accompagnée de sa motivation.

§ 5. Pour la conservation des données visées au paragraphe 1er, alinéa 1er, les fournisseurs de réseaux ou de services de communications électroniques visés au paragraphe 1er, alinéa 1er:

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

3° garantissent que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et par les agents et préposés de ces fournisseurs spécifiquement autorisés par ladite Cellule;

4° veille à ce que les données conservées soient détruites lorsqu'est expiré le délai de conservation applicable à ces données.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du

Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, de bewaringstermijn van de gegevens voor bepaalde categorieën van gegevens aanpassen, zonder een termijn van meer dan 18 maanden vast te leggen.

De Koning kan, in de omstandigheden zoals bedoeld in artikel 4, § 1, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een beperkte periode, een bewaringstermijn voor de gegevens vastleggen die langer is dan twaalf maanden.

Wanneer in de omstandigheden bedoeld in het tweede lid de Koning een bewaringstermijn oplegt die langer is dan vierentwintig maanden, stelt de minister de Europese Commissie en de overige lidstaten van de Europese Unie onverwijld in kennis van alle genomen maatregelen, met vermelding van de redenen die eraan ten grondslag liggen.

§ 5. Voor de bewaring van de in paragraaf 1, eerste lid, bedoelde gegevens geldt het onderstaande voor de aanbieder van een netwerk of dienst voor elektronische communicatie bedoeld in paragraaf 1, eerste lid:

1° hij garandeert dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;

2° hij zorgt ervoor dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

3° hij garandeert dat de toegang tot de bewaarde gegevens enkel door een of meer leden van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en door het personeel en de aangestelden van deze aanbieders die specifiek door deze cel gemachtigd zijn gebeurt;

4° hij zorgt ervoor dat de gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, worden vernietigd.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister

ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les mesures techniques et administratives que les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, doivent prendre en vue garantir la protection des données à caractère personnelle conservées.

Les founisseurs de services et réseaux visés paragraphe 1er, alinéa 1er, sont considérés comme responsables du traitement de ces données au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

§ 6. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Commission européenne et à la Chambre des représentants. Ces statistiques comprennent notamment:

1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, a), seront également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine, sur proposition du ministre de la Justice et ministre et sur avis de l'Institut, les statistiques que les fournisseurs de services ou de réseaux transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 7. Sans préjudice du rapport visé au paragraphe 6, 3ième alinéa, le ministre et le ministre de la Justice font un rapport d'évaluation à la Chambre des Représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé

van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die de aanbieders van diensten en netwerken beoogd in paragraaf 1, eerste lid, moeten nemen teneinde de bescherming van de bewaarde persoonsgegevens te garanderen.

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, worden beschouwd als verantwoordelijk voor de verwerking van deze gegevens in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

§ 6. De minister en de minister van Justitie zorgen ervoor dat jaarlijks aan de Europese Commissie en de Kamer van volksvertegenwoordigers statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare communicatiediensten of -netwerken. Die informatie heeft onder meer betrekking op:

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken niet konden worden ingewilligd.

Deze statistische informatie mag geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, a), worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van Strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt, op voorstel van de minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders van diensten of netwerken jaarlijks moeten overzenden aan het Instituut en deze die het Instituut overzendt aan de minister en aan de minister van Justitie.

§ 7. Onverminderd het verslag bedoeld in paragraaf 6, derde lid, brengen de minister en de minister van Justitie, twee jaar na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, derde lid, aan

au paragraphe 1er, alinéa 3, sur la mise en œuvre de cet article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation.”.

de Kamer van volksvertegenwoordigers een evaluatieverslag uit over de toepassing van dit artikel, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de te bewaren gegevens en de bewaringstermijn.”.

Art. 6

Dans l’article 145 de la même loi, modifié par la loi du 25 avril 2007, il est inséré un paragraphe 3*ter* rédigé comme suit:

“§ 3*ter*. Est puni d’une amende de 50 à 50 000 euros et d’une peine d’emprisonnement de six mois à trois ans ou d’une de ces peines seulement:

1° toute personne qui, à l’occasion de l’exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu’elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l’article 126;

2° celui qui, sachant que les données ont été obtenues par la commission de l’infraction visée au 1° les détient, les révèle à une autre personne, ou les divulgue ou fait un usage quelconque des données ainsi obtenues.”.

Art. 6

In artikel 145 van dezelfde wet, gewijzigd bij de wet van 25 april 2007, wordt een paragraaf 3*ter* ingevoegd, luidende:

“§ 3*ter*. Met een geldboete van 50 tot 50 000 euro en met een gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.”.

CHAPITRE 3

Modification de l’article 90*decies* du Code d’instruction criminelle

HOOFDSTUK 3

Wijziging van artikel 90*decies* van het Wetboek van Strafvordering

Art. 7

L’article 90*decies* du Code d’instruction criminelle, inséré par la loi du 30 juin 1994 et modifié par les lois du 8 avril 2002, 7 juillet 2002 et du 6 janvier 2003, est complété par un alinéa, rédigé comme suit:

Art. 7

Artikel 90*decies* van het Wetboek van Strafvordering, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 8 april 2002, 7 juli 2002 en 6 januari 2003, wordt aangevuld met een lid, luidende:

"A ce rapport est joint le rapport dressé en application de l'article 126, § 6, alinéa 3 de la loi du 13 juin 2005 relative aux communications électroniques.".

Donné à Bruxelles, le 26 juin 2013

ALBERT

Par le Roi:

Le ministre de l'Économie,

Johan VANDE LANOTTE

Le ministre de la Justice,

Annemie TURTELBOOM

"Bij dit verslag wordt tevens het verslag bijgevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.".

Gegeven te Brussel, 26 juni 2013

ALBERT

Van Koningswege:

De minister van Economie,

Johan VANDE LANOTTE

De minister van Justitie,

Annemie TURTELBOOM

ANNEXE 1

BIJLAGE 1

Tableau de transposition
Directive 2006/24/CE (conservation des données) et article 15.1 de la directive 2002/58/CE (vie privée et communications électroniques)

Législation belge vers directives

LCE : loi du 13 juin 2005 relative aux communications électroniques
AR du 9 janvier 2003 : arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques

Instrument de transposition	Norme finale ou modifiée	Directive 2006/24/CE et directive 2002/58/CE
Loi : art. 1	-	-
Loi : art. 2	LCE : art. 1	24 : art. 15.1
Loi : art. 3	LCE : art. 2, 11°	-
Loi : art. 4	LCE : art. 2, 74°	24 : art. 2, f)
Loi : art. 5	LCE : art. 126, § 1er, al.1	24 : art. 3.1
Loi : art. 5	LCE : art. 126, § 1er, al.2	24 : art. 3.1
Loi : art. 5	LCE : art. 126, § 1er, al. 3	24 : art. 2.2, c)
Loi : art. 5	LCE : art. 126, § 1er, al. 4	-
Loi : art. 5	LCE : art. 126, § 1er, al. 5	24 : art. 5.2
Loi : art. 5	LCE : art. 126, § 1er, al. 6	24 : art. 3.2
Loi : art. 5	LCE : art. 126, § 2, al. 1, a)	24 : art. 1.1
Loi : art. 5	LCE : art. 126, § 2, al. 1, b) à d)	58 : art. 15.1
Loi : art. 5	LCE : art. 126, § 2, al. 2	24 : art. 4 et art. 8
Loi : art. 5	LCE : art. 126, § 3	24 : art. 6
Loi : art. 5	LCE : art. 126, § 4, al. 1	24 : art. 6
Loi : art. 5	LCE : art. 126, § 4, al. 2 et 3	24 : art. 12.1
Loi : art. 5	LCE : art. 126, § 5, 1°	24 : art. 7, a)
Loi : art. 5	LCE : art. 126, § 5, 2°	24 : art. 7, b)
Loi : art. 5	LCE : art. 126, § 5, 3°	24 : art. 7, c)
Loi : art. 5	LCE : art. 126, § 5, 4°	24 : art. 7, d)
Loi : art. 5	LCE : art. 126, § 6, al. 1	24 : art. 10.1
Loi : art. 5	LCE : art. 126, § 6, al. 2 et 3	24 : art. 10.2
Loi : art. 5	LCE : art. 126, § 7	24 : art. 14.1
Loi : art. 6	LCE : art. 145, § 3*ter*	24 : art. 13.2
Loi : art. 7	Code d'instruction criminelle : article 90*decies*	-
AR du 9 janvier 2003 : art. 2	AR du 9 janvier 2003 : art. 2	24 : art. 4
AR du 9 janvier 2003 : art. 2, § 1, § 2, § 3 et § 4	AR du 9 janvier 2003 : art. 2, § 1, § 2, § 3 et § 4	24 : art. 7, a)
AR du 9 janvier 2003 : art. 2, § 5 et § 6	AR du 9 janvier 2003 : art. 2, § 5 et § 6	24 : art. 7, c)
AR : art. 1	AR : art. 1	24 : art. 15.1
AR : art. 2, 1°, 2°, 3°, 4° et 7°	AR : art. 2, 1°, 2°, 3°, 4° et 7°	-
AR : art. 2, 5°	AR : art. 2, 5°	24 : art. 2.2, d)
AR : art. 2, 6°	AR : art. 2, 6°	24 : art. 2.2, e)
AR : art. 3, § 1, 1°	AR : art. 3, § 1, 1°	24 : art. 5.1, a), 1), i) 24 : art. 5.1, e), 1)
AR : art. 3, § 1, 2°	AR : art. 3, § 1, 2°	24 : art. 5.1, a), 1), ii) 24 : art. 5.1, b), 1), ii)
AR : art. 3, § 1, 3°	AR : art. 3, § 1, 3°	58 : art. 15.1
AR : art. 3, § 1, 4°	AR : art. 3, § 1, 4°	24 : art. 5.1, d), 1)
AR : art. 3, § 1, 5°	AR : art. 3, § 1, 5°	58 : art. 15.1
AR : art. 3, § 1, 6°	AR : art. 3, § 1, 6°	58 : art. 15.1

Omzettingstabel
Richtlijn 2006/24/EG (dataretentierichtlijn) en artikel 15.1 van Richtlijn 2002/58/EG (privacy en elektronische communicatie)

Belgische wetgeving naar richtlijnen

WEC : Wet van 13 juni 2005 betreffende de elektronische communicatie
KB van 9 januari 2003 : Koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie

Akte van omzetting	Definitieve of gewijzigde norm	Richtlijn 2006/24/EG en richtlijn 2002/58/EG
Wet : art. 1	-	-
Wet : art. 2	WEC : art. 1	24 : art. 15.1
Wet : art. 3	WEC : art. 2, 11°	-
Wet : art. 4	WEC : art. 2, 74°	24 : art. 2, f)
Wet : art. 5	WEC : art. 126, § 1, lid 1	24 : art. 3.1
Wet : art. 5	WEC : art. 126, § 1, lid 2	24 : art. 3.1
Wet : art. 5	WEC : art. 126, § 1, lid 3	24 : art. 2.2, c)
Wet : art. 5	WEC : art. 126, § 1, lid 4	-
Wet : art. 5	WEC : art. 126, § 1, lid 5	24 : art. 5.2
Wet : art. 5	WEC : art. 126, § 1, lid 6	24 : art. 3.2
Wet : art. 5	WEC : art. 126, § 2, lid 1,a)	24 : art. 1.1
Wet : art. 5	WEC : art. 126, § 2, lid 1,b) tot d)	58 : art. 15.1
Wet : art. 5	WEC : art. 126, § 2, lid 2	24 : art. 4 en art. 8
Wet : art. 5	WEC : art. 126, § 3	24 : art. 6
Wet : art. 5	WEC : art. 126, § 4, lid 1	24 : art. 6
Wet : art. 5	WEC : art. 126, § 4, lid 2 en 3	24 : art. 12.1
Wet : art. 5	WEC : art. 126, § 5, 1°	24 : art. 7, a)
Wet : art. 5	WEC : art. 126, § 5, 2°	24 : art. 7, b)
Wet : art. 5	WEC: art. 126, § 5, 3°	24 : art. 7, c)
Wet : art. 5	WEC : art. 126, § 5, 4°	24 : art. 7, d)
Wet : art. 5	WEC: art. 126, § 6, lid 1	24 : art. 10.1
Wet : art. 5	WEC : art. 126, § 6, lid 2 en 3	24 : art. 10.2
Wet : art. 5	WEC : art. 126, § 7	24 : art. 14.1
Wet : art. 6	WEC : art. 145, § 3*ter*	24 : art. 13.2
Wet : art. 7	Wetboek van strafvordering : artikel 90*decies*	-
KB van 9 januari 2003 : art. 2	KB van 9 januari 2003 : art. 2	24 : art. 4
KB van 9 januari 2003 : art. 2, § 1, § 2, § 3 en § 4	KB van 9 januari 2003 : art. 2, § 1, § 2, § 3 en § 4	24 : art. 7, a)
KB van 9 januari 2003 : art. 2, § 5 en § 6	KB van 9 januari 2003 : art. 2, § 5 en § 6	24 : art. 7, c)
KB : art. 1	KB : art. 1	24 : art. 15.1
KB : art. 2, 1°, 2°, 3°, 4° en 7°	KB : art. 2, 1°, 2°, 3°, 4° en 7°	-
KB : art. 2, 5°	KB : art. 2, 5°	24 : art. 2.2, d)
KB : art. 2, 6°	KB : art. 2, 6°	24 : art. 2.2, e)
KB : art. 3, § 1, 1°	KB : art. 3, § 1, 1°	24 : art. 5.1, a), 1), i) 24 : art. 5.1, e), 1)
KB : art. 3, § 1, 2°	KB : art. 3, § 1, 2°	24 : art. 5.1, a), 1), ii) 24 : art. 5.1, b), 1), ii)
KB : art. 3, § 1, 3°	KB : art. 3, § 1, 3°	58 : art. 15.1
KB : art. 3, § 1, 4°	KB : art. 3, § 1, 4°	24 : art. 5.1, d), 1)
KB : art. 3, § 1, 5°	KB : art. 3, § 1, 5°	58 : art. 15.1

Instrument de transposition	Norme finale ou modifiée	Directive 2006/24/CE et directive 2002/58/CE
AR : art. 3, § 2, 1°	AR : art. 3, § 2, 1°	24 : art. 5.1, a), 1), i) 24 : art. 5.1, b), 1), i) 24 : art. 5.1, e), 1)
AR : art. 3, § 2, 2°	AR : art. 3, § 2, 2°	24 : art. 5.1, a), 1), ii) 24 : art. 5.1, b), 1), ii)
AR : art. 3, § 2, 3°	AR : art. 3, § 2, 3°	24 : art. 5.1, b), 1), i)
AR : art. 3, § 2, 4°	AR : art. 3, § 2, 4°	24 : art. 5.1, c), 1)
AR : art. 3, § 2, 5°	AR : art. 3, § 2, 5°	24 : art. 5.1, d), 1)
AR : art. 3, § 3, al. 1 et 2	AR : art. 3, § 3, al. 1 et 2	24 : art. 6
AR : art. 4, § 1, 1°	AR : art. 4, § 1, 1°	24 : art. 5.1, e), 2), i) et ii)
AR : art. 4, § 1, 2°	AR : art. 4, § 1, 2°	24 : art. 5.1, b), 1), ii)
AR : art. 4, § 1, 3°	AR : art. 4, § 1, 3°	58 : art. 15.1
AR : art. 4, § 1, 4°	AR : art. 4, § 1, 4°	24 : art. 5.1, e), 2), vi)
AR : art. 4, § 1, 5°	AR : art. 4, § 1, 5°	24 : art. 5.1, d), 1)
AR : art. 4, § 1, 6°	AR : art. 4, § 1, 6°	58 : art. 15.1
AR : art. 4, § 1, 7°	AR : art. 4, § 1, 7°	58 : art. 15.1
AR : art. 4, § 1, 8°	AR : art. 4, § 1, 8°	24 : art. 5.1, e, 2, iii) 24 : art. 5.1, e, 2, v)
AR : art. 4, § 2, 1°	AR : art. 4, § 2, 1°	24 : art. 5.1, a), 1), i) 24 : art. 5.1, b), 1), i) 24 : art. 5.1, e), 2), i)
AR : art. 4, § 2, 2°	AR : art. 4, § 2, 2°	24 : art. 5.1, b), 1), i)
AR : art. 4, § 2, 3°	AR : art. 4, § 2, 3°	24 : art. 5.1, e), 2), ii) 24 : art. 5.1, e), 2), iv)
AR : art. 4, § 2, 4°	AR : art. 4, § 2, 4°	24 : art. 5.1, e), 2), iii) 24 : art. 5.1, e), 2), v)
AR : art. 4, § 2, 5°	AR : art. 4, § 2, 5°	24 : art. 5.1, c), 1)
AR : art. 4, § 2, 6°	AR : art. 4, § 2, 6°	24 : art. 5.1, f), 1)
AR : art. 4, § 2, 7°	AR : art. 4, § 2, 7°	24 : art. 5.1, f), 2)
AR : art. 4, § 2, 8°	AR : art. 4, § 2, 8°	24 : art. 5.1, d), 1)
AR : art. 4, § 3, al. 1 et 2	AR : art. 4, § 3, al. 1 et 2	24 : art. 6
AR : art. 5, § 1, 1°	AR : art. 5, § 1, 1°	24 : art. 5.1, a), 2), i)
AR : art. 5, § 1, 2°	AR : art. 5, § 1, 2°	24 : art. 5.1, a), 2), iii)
AR : art. 5, § 1, 3°	AR : art. 5, § 1, 3°	58 : art. 15.1
AR : art. 5, § 1, 4°	AR : art. 5, § 1, 4°	58 : art. 15.1
AR : art. 5, § 1, 5°	AR : art. 5, § 1, 5°	24 : art. 5.1, e), 3), ii)
AR : art. 5, § 1, 6°	AR : art. 5, § 1, 6°	24 : art. 5.1, e), 3), ii)
AR : art. 5, § 1, 7°	AR : art. 5, § 1, 7°	58 : art. 15.1
AR : art. 5, § 2, 1°	AR : art. 5, § 2, 1°	24 : art. 5.1, a), 2), i) 24 : art. 5.1, c), 2), i)
AR : art. 5, § 2, 2°	AR : art. 5, § 2, 2°	24 : art. 5.1, a), 2), iii) 24 : art. 5.1, c), 2), i)
AR : art. 5, § 2, 3°	AR : art. 5, § 2, 3°	24 : art. 5.1, e), 3), ii) 24 : art. 5.1, f), 1)
AR : art. 5, § 2, 4°	AR : art. 5, § 2, 4°	24 : art. 5.1, c), 2), i)
AR : art. 5, § 2, 5°	AR : art. 5, § 2, 5°	58 : art. 15.1
AR : art. 5, § 2, 6°	AR : art. 5, § 2, 6°	24 : art. 5.1, d), 2) 24 : art. 5.1, f), 2)
AR : art. 5, § 3, al. 1 et 2	AR : art. 5, § 3, al. 1 et 2	24 : art. 6
AR : art. 6, § 1, 1°	AR : art. 6, § 1, 1°	24 : art. 5.1, a), 2), i) 24 : art. 5.1, b), 2), i)
AR : art. 6, § 1, 2°	AR : art. 6, § 1, 2°	24 : art. 5.1, a), 2), iii) 24 : art. 5.1, b),2), ii)
AR : art. 6, § 1, 3°	AR : art. 6, § 1, 3°	58 : art. 15.1

Akte van omzetting	Definitieve of gewijzigde norm	Richtlijn 2006/24/EG en richtlijn 2002/58/EG
KB : art. 3, § 1, 6°	KB : art. 3, § 1, 6°	58 : art. 15.1
KB : art. 3, § 2, 1°	KB : art. 3, § 2, 1°	24 : art. 5.1, a), 1), i) 24 : art. 5.1, b), 1), i) 24 : art. 5.1, e), 1)
KB : art. 3, § 2, 2°	KB : art. 3, § 2, 2°	24 : art. 5.1, a), 1), ii) 24 : art. 5.1, b), 1), ii)
KB : art. 3, § 2, 3°	KB : art. 3, § 2, 3°	24 : art. 5.1, b), 1), i)
KB : art. 3, § 2, 4°	KB : art. 3, § 2, 4°	24 : art. 5.1, c), 1)
KB : art. 3, § 2, 5°	KB : art. 3, § 2, 5°	24 : art. 5.1, d), 1)
KB : art. 3, § 3, lid 1 en 2	KB : art. 3, § 3, lid 1 en 2	24 : art. 6
KB : art. 4, § 1, 1°	KB : art. 4, § 1, 1°	24 : art. 5.1, e), 2), i) en ii)
KB : art. 4, § 1, 2°	KB : art. 4, § 1, 2°	24 : art. 5.1, b), 1), ii)
KB : art. 4, § 1, 3°	KB : art. 4, § 1, 3°	58 : art. 15.1
KB : art. 4, § 1, 4°	KB : art. 4, § 1, 4°	24 : art. 5.1, e), 2), vi)
KB : art. 4, § 1, 5°	KB : art. 4, § 1, 5°	24 : art. 5.1, d), 1)
KB : art. 4, § 1, 6°	KB : art. 4, § 1, 6°	58 : art. 15.1
KB : art. 4, § 1, 7°	KB : art. 4, § 1, 7°	58 : art. 15.1
KB : art. 4, § 1, 8°	KB : art. 4, § 1, 8°	24 : art. 5.1, e), 2), iii) 24 : art. 5.1, e), 2), v)
KB : art. 4, § 2, 1°	KB : art. 4, § 2, 1°	24 : art. 5.1, a), 1), i) 24 : art. 5.1, b), 1), i) 24 : art. 5.1, e), 2), i)
KB : art. 4, § 2, 2°	KB : art. 4, § 2, 2°	24 : art. 5.1, b), 1), i)
KB : art. 4, § 2, 3°	KB : art. 4, § 2, 3°	24 : art. 5.1, e), 2), ii) 24 : art. 5.1, e), 2), iv)
KB : art. 4, § 2, 4°	KB : art. 4, § 2, 4°	24 : art. 5.1, e), 2), iii) 24 : art. 5.1, e), 2), v)
KB : art. 4, § 2, 5°	KB : art. 4, § 2, 5°	24 : art. 5.1, c), 1)
KB : art. 4, § 2, 6°	KB : art. 4, § 2, 6°	24 : art. 5.1, f), 1)
KB : art. 4, § 2, 7°	KB : art. 4, § 2, 7°	24 : art. 5.1, f), 2)
KB : art. 4, § 2, 8°	KB : art. 4, § 2, 8°	24 : art. 5.1, d), 1)
KB : art. 4, § 3, lid 1 en 2	KB : art. 4, § 3, lid 1 en 2	24 : art. 6
KB : art. 5, § 1, 1°	KB : art. 5, § 1, 1°	24 : art. 5.1, a), 2), i)
KB : art. 5, § 1, 2°	KB : art. 5, § 1, 2°	24 : art. 5.1, a), 2), iii)
KB : art. 5, § 1, 3°	KB : art. 5, § 1, 3°	58 : art. 15.1
KB : art. 5, § 1, 4°	KB : art. 5, § 1, 4°	58 : art. 15.1
KB : art. 5, § 1, 5°	KB : art. 5, § 1, 5°	24 : art. 5.1, e), 3), ii)
KB : art. 5, § 1, 6°	KB : art. 5, § 1, 6°	24 : art. 5.1, e), 3), ii)
KB : art. 5, § 1, 7°	KB : art. 5, § 1, 7°	58 : art. 15.1
KB : art. 5, § 2, 1°	KB : art. 5, § 2, 1°	24 : art. 5.1, a), 2), i) 24 : art. 5.1, c), 2), i)
KB : art. 5, § 2, 2°	KB : art. 5, § 2, 2°	24 : art. 5.1, a), 2), iii) 24 : art. 5.1, c), 2), i)
KB : art. 5, § 2, 3°	KB : art. 5, § 2, 3°	24 : art. 5.1, e), 3), ii) 24 : art. 5.1, f), 1)
KB : art. 5, § 2, 4°	KB : art. 5, § 2, 4°	24 : art. 5.1, c), 2), i)
KB : art. 5, § 2, 5°	KB : art. 5, § 2, 5°	58 : art. 15.1
KB : art. 5, § 2, 6°	KB : art. 5, § 2, 6°	24 : art. 5.1, d), 2) 24 : art. 5.1, f), 2)
KB : art. 5, § 3, lid 1 en 2	KB : art. 5, § 3, lid 1 en 2	24 : art. 6
KB : art. 6, § 1, 1°	KB : art. 6, § 1, 1°	24 : art. 5.1, a), 2), i) 24 : art. 5.1, b), 2), i)
KB : art. 6, § 1, 2°	KB : art. 6, § 1, 2°	24 : art. 5.1, a), 2), iii) 24 : art. 5.1, b), 2), ii)

Instrument de transposition	Norme finale ou modifiée	Directive 2006/24/CE et directive 2002/58/CE
AR : art. 6, § 1, 4°	AR : art. 6, § 1, 4°	58 : art. 15.1
AR : art. 6, § 1, 5°	AR : art. 6, § 1, 5°	58 : art. 15.1
AR : art. 6, § 2, 1°	AR : art. 6, § 2, 1°	24 : art. 5.1, a), 2), i) 24 : art. 5.1, a), 2), iii) 24 : art. 5.1, b), 2), i) 24 : art. 5.1, b), 2), ii)
AR : art. 6, § 2, 2°	AR : art. 6, § 2, 2°	24 : art. 5.1, a), 2), ii) 24 : art. 5.1, a), 2), iii) 24 : art. 5.1, b), 2), i)
AR : art. 6, § 2, 3°	AR : art. 6, § 2, 3°	24 : art. 5.1, a), 2), iii) 24 : art. 5.1, c), 2), i)
AR : art. 6, § 2, 4°	AR : art. 6, § 2, 4°	24 : art. 5.1, c), 2), ii)
AR : art. 6, § 2, 5°	AR : art. 6, § 2, 5°	24 : art. 5.1, c), 2), ii)
AR : art. 6, § 2, 6°	AR : art. 6, § 2, 6°	24 : art. 5.1, d), 2) 24 : art. 5.1, e), 3), ii)
AR : art. 6, § 3, al. 1 et 2	AR : art. 6, § 3, al. 1 et 2	24 : art. 6
AR : art. 7, § 1 et § 2	AR : art. 7, § 1 et § 2	24 : art. 8
AR : art. 8	AR : art. 8	24 : art. 7, b) et c)
AR : art. 9	AR : art. 9	-
AR : art. 10	AR : art. 10	-
AR : art. 11	AR : art. 11	-

Akte van omzetting	Definitieve of gewijzigde norm	Richtlijn 2006/24/EG en richtlijn 2002/58/EG
KB : art. 6, § 1, 3°	KB : art. 6, § 1, 3°	58 : art. 15.1
KB : art. 6, § 1, 4°	KB : art. 6, § 1, 4°	58 : art. 15.1
KB : art. 6, § 1, 5°	KB : art. 6, § 1, 5°	58 : art. 15.1
KB : art. 6, § 2, 1°	KB : art. 6, § 2, 1°	24 : art. 5.1, a), 2), i) 24 : art. 5.1, a), 2), iii) 24 : art. 5.1, b), 2), i) 24 : art. 5.1, b), 2), ii)
KB : art. 6, § 2, 2°	KB : art. 6, § 2, 2°	24 : art. 5.1, a), 2), ii) 24 : art. 5.1, a), 2), iii) 24 : art. 5.1, b), 2), i)
KB : art. 6, § 2, 3°	KB : art. 6, § 2, 3°	24 : art. 5.1, a), 2), iii) 24 : art. 5.1, c), 2), i)
KB : art. 6, § 2, 4°	KB : art. 6, § 2, 4°	24 : art. 5.1, c), 2), ii)
KB : art. 6, § 2, 5°	KB : art. 6, § 2, 5°	24 : art. 5.1, c), 2), ii)
KB : art. 6, § 2, 6°	KB : art. 6, § 2, 6°	24 : art. 5.1, d), 2) 24 : art. 5.1, e), 3), ii)
KB : art. 6, § 3, lid 1 en 2	KB : art. 6, § 3, lid 1 en 2	24 : art. 6
KB : art. 7, § 1 en § 2	KB : art. 7, § 1 en § 2	24 : art. 8
KB : art. 8	KB : art. 8	24 : art. 7, b) en c)
KB : art. 9	KB : art. 9	-
KB : art. 10	KB : art. 10	-
KB : art. 11	KB : art. 11	-

ANNEXE 2

BIJLAGE 2

Tableau de transposition
Directive 2006/24/CE (conservation des données) et article 15.1. de la directive 2002/58/CE (vie privée et communications électroniques)

Directives vers législation belge

LCE : loi du 13 juin 2005 relative aux communications électroniques
AR du 9 janvier 2003 : arrêté du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques

Directive 2006/24/CE	Instrument de transposition	Norme finale ou modifiée
Art. 1.1	Loi : art. 5	LCE : article 126, § 2, al. 1er, a)
Art. 1.2	Pas nécessaire	-
Art. 2.1	Pas nécessaire (car LCE, art. 2)	-
Art. 2.2, a)	Pas nécessaire (car LCE ,art. 2, 6 : données de trafic + art. 2, 7°:données de localisation)	-
Art. 2.2, b)	Pas nécessaire (car LCE, article 2, 12°)	-
Art. 2.2, c)	Loi : art. 5	LCE : art. 126, § 1er, al. 3
Art. 2.2, d)	AR : art. 2, 5°	AR : art. 2, 5°
Art. 2.2, e)	AR : art. 2, 6°	AR : art. 2, 6°
Art. 2.2, f)	Loi : art. 4	LCE : art. 2, 74°
Art. 3.1	Loi : art. 5	LCE : art. 126, § 1er, al.1 et 2
Art. 3.2	Loi : art. 5	LCE : art.126, § 1er, al. 6
Art. 4	Loi : art. 5 AR du 9 janvier 2003 : art. 2	LCE : art. 126, § 2, al. 1 et 2 AR du 9 janvier 2003 : art. 2
Art. 5.1, a), 1), i)	AR : art. 3, § 1, 1° AR : art. 3, § 2, 1° AR : art. 4, § 2, 1°	AR : art. 3, § 1, 1° AR : art. 3, § 2, 1° AR : art. 4, § 2, 1°
Art. 5.1, a), 1), ii)	AR : art. 3, § 1, 2° AR : art. 3, § 2, 2°	AR : art. 3, § 1, 2° AR : art. 3, § 2, 2°
Art. 5.1, a), 2), i)	AR : art. 5, § 1, 1° AR : art. 5, § 2, 1° AR : art. 6, § 1, 1° AR : art. 6, § 2, 1°	AR : art. 5, § 1, 1° AR : art. 5, § 2, 1° AR : art. 6, § 1, 1° AR : art. 6, § 2, 1°
Art. 5.1, a), 2), ii)	AR : art. 6, § 2, 2°	AR : art. 6, § 2, 2°
Art. 5.1, a), 2), iii)	AR : art. 5, § 1, 2° AR : art. 5, § 2, 1° AR : art. 5, § 2, 2° AR : art. 6, § 1, 2° AR : art. 6, § 2, 1° AR : art. 6, § 2, 2° AR : art. 6, § 2, 3°	AR : art. 5, § 1, 2° AR : art. 5, § 2, 1° AR : art. 5, § 2, 2° AR : art. 6, § 1, 2° AR : art. 6, § 2, 1° AR : art. 6, § 2, 2° AR : art. 6, § 2, 3°
Art. 5.1, b), 1), i)	AR : art. 3, § 2, 1° AR : art. 3, § 2, 3° AR : art. 4, § 2, 1° AR : art. 4, § 2, 2°	AR : art. 3, § 2, 1° AR : art. 3, § 2, 3° AR : art. 4, § 2, 1° AR : art. 4, § 2, 2°
Art. 5.1, b), 1), ii)	AR : art. 3, § 1, 2° AR : art. 3, § 2, 2° AR : art. 4, § 1, 2°	AR : art. 3, § 1, 2° AR : art. 3, § 2, 2° AR : art. 4, § 1, 2°

Omzettingstabel
Richtlijn 2006/24/EG (dataretentierichtlijn) en artikel 15.1. van Richtlijn 2002/58/CE (privacy en elektronische communicatie)

Richtlijnen naar Belgische wetgeving

WEC : Wet van 13 juni 2005 betreffende de elektronische communicatie
KB van 9 januari 2003 : Koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie

Richtlijn 2006/24/EG	Akte van omzetting	Definitieve of gewijzigde norm
Art. 1.1	Wet : art. 5	WEC : artikel 126, § 2, lid 1, a)
Art. 1.2	Niet noodzakelijk	-
Art. 2.1	Niet noodzakelijk (want WEC, art. 2)	-
Art. 2.2, a)	Niet noodzakelijk (want WEC, art. 2, 6 : verkeersgegevens + art. 2, 7°: locatie-gegevens)	-
Art. 2.2, b)	Niet noodzakelijk (want WEC, artikel 2, 12°)	-
Art. 2.2, c)	Wet : art. 5	WEC : art. 126, § 1, lid 3
Art. 2.2, d)	KB : art. 2, 5°	KB : art. 2, 5°
Art. 2.2, e)	KB : art. 2, 6°	KB : art. 2, 6°
Art. 2.2, f)	Wet : art. 4	WEC : art. 2, 74°
Art. 3.1	Wet : art. 5	WEC : art. 126, § 1, lid 1 en 2
Art. 3.2	Wet : art. 5	WEC : art. 126, § 1, lid 6
Art. 4	Wet : art. 5 KB van 9 januari 2003 : art. 2	WEC : art. 126, § 2, lid 1 en 2 KB van 9 januari 2003 : art. 2
Art. 5.1, a), 1), i)	KB : art. 3, § 1, 1° KB : art. 3, § 2, 1° KB : art. 4, § 2, 1°	KB : art. 3, § 1, 1° KB : art. 3, § 2, 1° KB : art. 4, § 2, 1°
Art. 5.1, a), 1), ii)	KB : art. 3, § 1, 2° KB : art. 3, § 2, 2°	KB : art. 3, § 1, 2° KB : art. 3, § 2, 2°
Art. 5.1, a), 2), i)	KB : art. 5, § 1, 1° KB : art. 5, § 2, 1° KB : art. 6, § 1, 1° KB : art. 6, § 2, 1°	KB : art. 5, § 1, 1° KB : art. 5, § 2, 1° KB : art. 6, § 1, 1° KB : art. 6, § 2, 1°
Art. 5.1, a), 2), ii)	KB : art. 6, § 2, 2°	KB : art. 6, § 2, 2°
Art. 5.1, a), 2), iii)	KB : art. 5, § 1, 2° KB : art. 5, § 2, 1° KB : art. 5, § 2, 2° KB : art. 6, § 1, 2° KB : art. 6, § 2, 1° KB : art. 6, § 2, 2° KB : art. 6, § 2, 3°	KB : art. 5, § 1, 2° KB : art. 5, § 2, 1° KB : art. 5, § 2, 2° KB : art. 6, § 1, 2° KB : art. 6, § 2, 1° KB : art. 6, § 2, 2° KB : art. 6, § 2, 3°
Art. 5.1, b), 1), i)	KB : art. 3, § 2, 1° KB : art. 3, § 2, 3° KB : art. 4, § 2, 1° KB : art. 4, § 2, 2°	KB : art. 3, § 2, 1° KB : art. 3, § 2, 3° KB : art. 4, § 2, 1° KB : art. 4, § 2, 2°
Art. 5.1, b), 1), ii)	KB : art. 3, § 1, 2° KB : art. 3, § 2, 2° KB : art. 4, § 1, 2°	KB : art. 3, § 1, 2° KB : art. 3, § 2, 2° KB : art. 4, § 1, 2°

Directive 2006/24/CE	Instrument de transposition	Norme finale ou modifiée
Art. 5.1, b),2), i)	AR : art. 6, § 1, 1° AR : art. 6, § 2, 1° AR : art. 6, § 2, 2°	AR : art. 6, § 1, 1° AR : art. 6, § 2, 1° AR : art. 6, § 2, 2°
Art. 5.1, b),2), ii)	AR : art. 6, § 1, 2°	AR : art. 6, § 1, 2°
Art. 5.1, c), 1)	AR : art. 3, § 2, 4° AR : art. 4, § 2, 5°	AR : art. 3, § 2, 4° AR : art. 4, § 2, 5°
Art. 5.1, c), 2), i)	AR : art. 5, § 2, 1° AR : art. 5, § 2, 2° AR : art. 5, § 2, 4°	AR : art. 5, § 2, 1° AR : art. 5, § 2, 2° AR : art. 5, § 2, 4°
Art. 5.1, c), 2), ii)	AR : art. 6, § 2, 4° AR : art. 6, § 2, 5°	AR : art. 6, § 2, 4° AR : art. 6, § 2, 5°
Art. 5.1, d), 1)	AR : art. 3, § 1, 4° AR : art. 3, § 2, 5° AR : art. 4, § 1, 5° AR : art. 4, § 2, 8°	AR : art. 3, § 1, 4° AR : art. 3, § 2, 5° AR : art. 4, § 1, 5° AR : art. 4, § 2, 8°
Art. 5.1, d), 2)	AR : art. 5, § 2, 6° AR : art. 6, § 2, 6°	AR : art. 5, § 2, 6° AR : art. 6, § 2, 6°
Art. 5.1, e), 1)	AR : art. 3, § 1, 1° AR : art. 3, § 2, 1°	AR : art. 3, § 1, 1° AR : art. 3, § 2, 1°
Art. 5.1, e), 2), i)	AR : art. 4, § 1, 1° AR : art. 4, § 2, 1°	AR : art. 4, § 1, 1° AR : art. 4, § 2, 1°
Art. 5.1, e), 2), ii)	AR : art. 4, § 2, 3°	AR : art. 4, § 2, 3°
Art. 5.1, e), 2), iii)	AR : art. 4, § 1, 8° AR : art. 4, § 2, 4°	AR : art. 4, § 1, 8° AR : art. 4, § 2, 4°
Art. 5.1, e), 2), iv)	AR : art. 4, §2, 3°	AR : art. 4, §2, 3°
Art. 5.1, e), 2), v)	AR : art. 4, § 1, 8° AR : art. 4, § 2, 4°	AR : art. 4, § 1, 8° AR : art. 4, § 2, 4°
Art. 5.1, e), 2), vi)	AR : art. 4, § 1, 4°	AR : art. 4, § 1, 4°
Art. 5.1, e), 3), i)	Pas nécessaire (technique désuète :il n'y a plus de 0905)	-
Art. 5.1, e), 3), ii)	AR : art. 5, § 1, 5° AR : art. 5, § 1, 6° AR : art. 5, § 2, 3° AR : art. 6, § 2, 6°	AR : art. 5, § 1, 5° AR : art. 5, § 1, 6° AR : art. 5, § 2, 3° AR : art. 6, § 2, 6°
Art. 5.1, f), 1)	AR : art. 4, § 2, 6° AR : art. 5, § 2, 3°	AR : art. 4, § 2, 6° AR : art. 5, § 2, 3°
Art. 5.1, f), 2)	AR : art. 4, § 2, 7° AR : art. 5, § 2, 3° et 6°	AR : art. 4, § 2, 7° AR : art. 5, § 2, 3° et 6°
Art. 5.2	Loi : art. 5	LCE : 126, § 1er, al. 5
Art. 6	Loi : art. 5 AR : art. 3, § 3, al. 1 et 2 AR : art. 4, § 3, al. 1 et 2 AR : art. 5, § 3, al. 1 et 2 AR : art. 6, § 3, al. 1 et 2	LCE : art 126, § 3, al. 1 à 3 et § 4, al. 1 AR : art. 3, § 3, al. 1 et 2 AR : art. 4, § 3, al. 1 et 2 AR : art. 5, § 3, al. 1 et 2 AR : art. 6, § 3, al. 1 et 2
Art. 7, a)	Loi : art. 5 AR du 9 janvier 2003 : art. 2, §1, § 2, § 3 et § 4	LCE : art. 126, § 5, 1° AR du 9 janvier 2003 : art. 2, §1, § 2, § 3 et § 4
Art. 7, b)	Loi : art. 5 AR : art. 8	LCE : art. 126, § 5, 2° AR : art. 8

Richtlijn 2006/24/EG	Akte van omzetting	Definitieve of gewijzigde norm
Art. 5.1, b), 2), i)	KB : art. 6, § 1, 1° KB : art. 6, § 2, 1° KB : art. 6, § 2, 2°	KB : art. 6, § 1, 1° KB : art. 6, § 2, 1° KB : art. 6, § 2, 2°
Art. 5.1, b), 2), ii)	KB : art. 6, § 1, 2°	KB : art. 6, § 1, 2°
Art. 5.1, c), 1)	KB : art. 3, § 2, 4° KB : art. 4, § 2, 5°	KB : art. 3, § 2, 4° KB : art. 4, § 2, 5°
Art. 5.1, c), 2), i)	KB : art. 5, § 2, 1° KB : art. 5, § 2, 2° KB : art. 5, § 2, 4°	KB : art. 5, § 2, 1° KB : art. 5, § 2, 2° KB : art. 5, § 2, 4°
Art. 5.1, c), 2), ii)	KB : art. 6, § 2, 4° KB : art. 6, § 2, 5°	KB : art. 6, § 2, 4° KB : art. 6, § 2, 5°
Art. 5.1, d), 1)	KB : art. 3, § 1, 4° KB : art. 3, § 2, 5° KB : art. 4, § 1, 5° KB : art. 4, § 2, 8°	KB : art. 3, § 1, 4° KB : art. 3, § 2, 5° KB : art. 4, § 1, 5° KB : art. 4, § 2, 8°
Art. 5.1, d), 2)	KB : art. 5, § 2, 6° KB : art. 6, § 2, 6°	KB : art. 5, § 2, 6° KB : art. 6, § 2, 6°
Art. 5.1, e), 1)	KB : art. 3, § 1, 1° KB : art. 3, § 2, 1°	KB : art. 3, § 1, 1° KB : art. 3, § 2, 1°
Art. 5.1, e), 2), i)	KB : art. 4, § 1, 1° KB : art. 4, § 2, 1°	KB : art. 4, § 1, 1° KB : art. 4, § 2, 1°
Art. 5.1, e), 2), ii)	KB : art. 4, § 2, 3°	KB : art. 4, § 2, 3°
Art. 5.1, e), 2), iii)	KB : art. 4, § 1, 8° KB : art. 4, § 2, 4°	KB : art. 4, § 1, 8° KB : art. 4, § 2, 4°
Art. 5.1, e), 2), iv)	KB : art. 4, § 2, 3°	KB : art. 4, § 2, 3°
Art. 5.1, e), 2), v)	KB : art. 4, § 1, 8° KB : art. 4, § 2, 4°	KB : art. 4, § 1, 8° KB : art. 4, § 2, 4°
Art. 5.1, e), 2), vi)	KB : art. 4, § 1, 4°	KB : art. 4, § 1, 4°
Art. 5.1, e), 3), i)	Niet noodzakelijk (techniek achterhaald: 0905 bestaat niet meer)	-
Art. 5.1, e), 3), ii)	KB : art. 5, § 1, 5° KB : art. 5, § 1, 6° KB : art. 5, § 2, 3° KB : art. 6, § 2, 6°	KB : art. 5, § 1, 5° KB : art. 5, § 1, 6° KB : art. 5, § 2, 3° KB : art. 6, § 2, 6°
Art. 5.1, f), 1)	KB : art. 4, § 2, 6° KB : art. 5, § 2, 3°	KB : art. 4, § 2, 6° KB : art. 5, § 2, 3°
Art. 5.1, f), 2)	KB : art. 4, § 2, 7° KB : art. 5, § 2, 3° en 6°	KB : art. 4, § 2, 7° KB : art. 5, § 2, 3° en 6°
Art. 5.2	Wet : art. 5	WEC : 126, § 1, lid 5
Art. 6	Wet : art. 5 KB : art. 3, § 3, lid 1 en 2 KB : art. 4, § 3, lid 1 en 2 KB : art. 5, § 3, lid 1 en 2 KB : art. 6, § 3, lid 1 en 2	WEC : art 126, § 3, lid 1 tot 3 en § 4, lid 1 KB : art. 3, § 3, lid 1 en 2 KB : art. 4, § 3, lid 1 en 2 KB : art. 5, § 3, lid 1 en 2 KB : art. 6, § 3, lid 1 en 2
Art. 7, a)	Wet : art. 5 KB van 9 januari 2003 : art. 2, § 1, § 2, § 3 en § 4	WEC : art. 126, § 5, 1° KB van 9 januari 2003 : art. 2, §1, § 2, § 3 en § 4
Art. 7, b)	Wet : art. 5 KB : art. 8	WEC : art. 126, § 5, 2° KB : art. 8

Directive 2006/24/CE	Instrument de transposition	Norme finale ou modifiée
Art. 7, c)	Loi : art. 5 AR du 9 janvier 2003 : art. 2, § 5 et § 6 AR : art. 8	LCE : art. 126, § 5, 3° AR du 9 janvier 2003 : art. 2, § 5 et § 6 AR : art. 8
Art. 7, d)	Loi : art. 5	LCE : art. 126, § 5, 4°
Art. 8	Loi : art. 5 AR : art. 7, § 1 et § 2	LCE : art. 126, § 2, al. 2 AR : art. 7, § 1 et § 2
Art. 9.1	Pas nécessaire (Art. 14, §1, 3° Loi statut IBPT du 17 janvier 2003 + Art. 29 Loi du 8 décembre 1992 vie privée)	-
Art. 9.2	Pas nécessaire (Art.17 Loi statut IBPT du 17 janvier 2003 +Art. 29 Loi 8 décembre 1992 vie privée)	-
Art. 10.1	Loi : art. 5	LCE : art. 126, § 6, al. 1
Art. 10.2	Loi : art. 5	LCE : art. 126, § 6, al. 2 et al. 3
Art. 11	Pas nécessaire	-
Art. 12.1	Loi : art. 5	LCE : art. 126, § 4, al. 2 et 3
Art. 12.2	Pas nécessaire	-
Art. 12.3	Pas nécessaire	-
Art. 13.1	Pas nécessaire	-
Art. 13.2	Loi : art. 6	LCE : art. 145, §3*ter*
Art. 14.1	Loi : art. 5	LCE : art. 126, § 7
Art. 14.2	Pas nécessaire	-
Art. 15.1	Loi : art. 2 AR : art. 1	LCE : art. 2 AR : art. 1
Art. 15.2	Pas nécessaire	-
Art. 15.3	Pas nécessaire	-
Art. 16	Pas nécessaire	-
Art. 17	Pas nécessaire	-

Directive 2002/58/CE	Instrument de transposition	Norme finale ou modifiée
Art. 15.1	Loi : art. 5	LCE : art. 126, § 2, b) à d)
Art. 15.1	AR : art. 3, § 1, 3°	AR : art. 3, § 1, 3°
Art. 15.1	AR: art. 3, § 1, 5°	AR: art. 3, § 1, 5°
Art. 15.1	AR: art. 3, § 1, 6°	AR: art. 3, § 1, 6°
Art. 15.1	AR: art. 4, § 1, 3°	AR: art. 4, § 1, 3°
Art. 15.1	AR: art. 4, § 1, 6°	AR: art. 4, § 1, 6°
Art. 15.1	AR: art. 4, § 1, 7°	AR: art. 4, § 1, 7°
Art. 15.1	AR: art. 5, § 1, 3°	AR: art. 5, § 1, 3°
Art. 15.1	AR: art. 5, § 1, 4°	AR: art. 5, § 1, 4°
Art. 15.1	AR: art. 5, § 1, 7°	AR: art. 5, § 1, 7°
Art. 15.1	AR: art. 5, § 2, 5°	AR: art. 5, § 2, 5°
Art. 15.1	AR: art. 6, § 1, 3°	AR: art. 5, § 1, 3°
Art. 15.1	AR: art. 6, § 1, 4°	AR: art. 5, § 1, 4°
Art. 15.1	AR: art. 6, § 1, 5°	AR: art. 5, § 1, 5°

Richtlijn 2006/24/EG	Akte van omzetting	Definitieve of gewijzigde norm
Art. 7, c)	Wet : art. 5 KB van 9 januari 2003 : art. 2, § 5 en § 6 KB : art. 8	WEC : art. 126, § 5, 3° KB van 9 januari 2003 : art. 2, § 5 en § 6 KB : art. 8
Art. 7, d)	Wet : art. 5	WEC : art. 126, § 5, 4°
Art. 8	Wet : art. 5 KB : art. 7, § 1 en § 2	WEC : art. 126, § 2, lid 2 KB : art. 7, § 1 en § 2
Art. 9.1	Niet noodzakelijk (Art. 14, §1, 3° BIPT-statuutwet 17 januari 2003 + Art. 29 Wet van 8 december 1992 privacy)	-
Art. 9.2	Niet noodzakelijk (Art.17 BIPT-statuutwet 17 januari 2003 + Art. 29 Wet van 8 december 1992 privacy)	-
Art. 10.1	Wet : art. 5	WEC : art. 126, § 6, lid 1
Art. 10.2	Wet : art. 5	WEC : art. 126, § 6, lid 2 en 3
Art. 11	Niet noodzakelijk	-
Art. 12.1	Wet : art. 5	WEC : art. 126, § 4, lid 2 en 3
Art. 12.2	Niet noodzakelijk	-
Art. 12.3	Niet noodzakelijk	-
Art. 13.1	Niet noodzakelijk	-
Art. 13.2	Wet : art. 6	WEC : art. 145, §3*ter*
Art. 14.1	Wet : art. 5	WEC : art. 126, § 7
Art. 14.2	Niet noodzakelijk	-
Art. 15.1	Wet : art. 2 KB : art. 1	WEC : art. 2 KB : art. 1
Art. 15.2	Niet noodzakelijk	-
Art. 15.3	Niet noodzakelijk	-
Art. 16	Niet noodzakelijk	-
Art. 17	Niet noodzakelijk	-

Richtlijn 2002/58/EG	Akte van omzetting	Definitieve of gewijzigde norm
Art. 15.1	Wet : art. 5	WEC : art. 126, § 2, b) tot d)
Art. 15.1	KB: art. 3, § 1, 3°	KB: art. 3, § 1, 3°
Art. 15.1	KB: art. 3, § 1, 5°	KB: art. 3, § 1, 5°
Art. 15.1	KB: art. 3, § 1, 6°	KB: art. 3, § 1, 6°
Art. 15.1	KB: art. 4, § 1, 3°	KB: art. 4, § 1, 3°
Art. 15.1	KB: art. 4, § 1, 6°	KB: art. 4, § 1, 6°
Art. 15.1	KB: art. 4, § 1, 7°	KB: art. 4, § 1, 7°
Art. 15.1	KB: art. 5, § 1, 3°	KB: art. 5, § 1, 3°
Art. 15.1	KB: art. 5, § 1, 4°	KB: art. 5, § 1, 4°
Art. 15.1	KB: art. 5, § 1, 7°	KB: art. 5, § 1, 7°
Art. 15.1	KB: art. 5, § 2, 5°	KB: art. 5, § 2, 5°
Art. 15.1	KB: art. 6, § 1, 3°	KB: art. 5, § 1, 3°
Art. 15.1	KB: art. 6, § 1, 4°	KB: art. 5, § 1, 4°
Art. 15.1	KB: art. 6, § 1, 5°	KB: art. 5, § 1, 5°

ANNEXE 3

BIJLAGE 3

Avis n° 24 /2008 du 2 juillet 2008

Objet : avis relatif à l'avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 *relative aux communications électroniques* et au projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données (A/2008/024)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "LVP"), en particulier l'article 29 ;

Vu la demande d'avis du Ministre pour l'Entreprise et la Simplification, reçue le 23/05/2008 ;

Vu le rapport de Madame Anne Vander Donckt ;

Émet, le 02/07/2008, l'avis suivant :

A. INTRODUCTION

1. Le 23 mai 2008, le Ministre pour l'Entreprise et la Simplification a demandé à la Commission d'émettre un avis concernant les propositions visant à transposer la Directive européenne 2006/24/CE *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*.

2. Il s'agit plus précisément d'un avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après "l'avant-projet de loi"), et d'un projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données (ci-après "le projet d'arrêté royal"). La Commission émettra dès lors ci-après un avis sur ces projets, en tenant compte des informations dont elle dispose.

B. LÉGISLATION APPLICABLE

3. Tout d'abord, on peut faire référence à la Directive 2006/24/CE. Étant donné que des données à caractère personnel sont traitées, la LVP ainsi que la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après "la LCE") sont d'application. Enfin, il convient de mentionner l'arrêté royal du 9 janvier 2003 *portant exécution des articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3, du code d'instruction criminelle ainsi que de l'article 109ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques* (ci-après "l'arrêté royal du 9 janvier 2003").

C. ANTÉCÉDENTS

4. Par le passé, plusieurs États membres européens ont légiféré sur la conservation de données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales. Lesdites dispositions nationales varient considérablement. Les disparités législatives et techniques existant entre les dispositions nationales relatives à la conservation de données en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales constituent des entraves au marché intérieur des communications électroniques dans la mesure où les fournisseurs de services doivent satisfaire à des exigences différentes pour ce qui est des types de données relatives au trafic et à la localisation à conserver ainsi que des conditions et des durées de conservation.

5. Dans ses conclusions, le Conseil européen "Justice et affaires intérieures" du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment de la criminalité organisée. Dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, le Conseil européen a chargé le Conseil "Justice et affaires intérieures" d'envisager des propositions en vue de l'établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications. Le 13 juillet 2005, le Conseil européen a réaffirmé, dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation de données concernant les télécommunications.

6. **Les finalités de la Directive 2006/24/CE consistent dès lors à harmoniser les obligations imposées aux fournisseurs en matière de conservation de certaines données et à garantir que ces données soient disponibles à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne**.

7. Le Groupe 29[1] a précisé dans son avis n° 3/2006 concernant la Directive 2006/24 qu'afin de transposer uniformément ses dispositions et de respecter les conditions de l'article 8 de la CEDH, les États membres devraient mettre en place des garanties spécifiques suffisantes, comprenant au minimum les garanties suivantes :

   - description de la finalité : le terme "infraction grave" devrait être clairement défini et encadré ;
   - limitation de l'accès : les données devraient être mises à la disposition des seuls services répressifs expressément désignés ;
   - données limitées au minimum ;
   - pas d'exploration des données ;
   - contrôle indépendant de l'autorisation d'accès ;

[1] Ce groupe de travail a été établi en vertu de l'article 29 de la Directive 95/46/CE et est un organe consultatif indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la Directive 95/46/CE et à l'article 15 de la Directive 2002/58/CE.

- séparation des systèmes ;
- mesures de sécurité ;
- finalité de la conservation des données par les fournisseurs.
-

D. EXAMEN DE LA DEMANDE D'AVIS

D.1. COMPARAISON DE L'ACTUEL ARTICLE 126 DE LA LCE AVEC LE NOUVEL AVANT-PROJET

8. L'actuel article 126 de la LCE est formulé comme suit : "*§ 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques.*

   § 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

   Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique."

9. L'arrêté royal dont il est question au § 2 n'a jamais été adopté. L'actuel article 126 de la LCE s'applique aux opérateurs et non aux fournisseurs ou aux revendeurs prévus à l'article 9, §§ 5 et 6 de la LEC. Sont ainsi visés par exemple[2] les réseaux ou services destinés à être utilisés par les membres d'un groupe d'entreprises, un réseau d'une université, d'une banque et de ses agents, … Dans l'avant-projet de loi, les fournisseurs et les revendeurs sont bel et bien repris à l'article 126 de la LCE. L'avant-projet de loi ajoute également les données de localisation à l'actuel article 126 de la LCE.

[2] Voir la Chambre des représentants de Belgique, justification des amendements du projet de loi portant des dispositions diverses, Doc. 51, 2873/002.

10. Dans son avis n° 08/2004[3], la Commission a notamment déclaré ce qui suit concernant l'actuel article 126 de la LCE :

"***La Commission rappelle les observations déjà formulées dans son avis 33/99 du 13 décembre 1999 et réitérées au niveau européen à plusieurs reprises par le groupe des commissaires européens à la protection des données[4], quant à la compatibilité d'une rétention a priori des données de communication avec les principes fondamentaux de protection des données à caractère personnel***.

La Commission avait ainsi rappelé que "ni les textes internationaux (…), ni la loi du 8 décembre 1992 (principes de proportionnalité, durée limitée, …) n'autorisent les méthodes de surveillance globale indépendamment d'instructions relatives à des infractions particulières (si l'on excepte le cas très particulier de la recherche proactive, qui est strictement encadrée. La Commission se référait encore à la jurisprudence de la Cour européenne des droits de l'homme[5] "qui conduit à proscrire les mesures de surveillance exploratoire ou générale des télécommunications mises en œuvre sur une grande échelle. Ainsi, il ne pourrait être question d'obliger un fournisseur d'accès à enregistrer systématiquement tous les appels en provenance de ses clients mais uniquement lorsqu'une instruction est ordonnée vis-à-vis d'une personne en particulier. Il ne pourrait non plus être question de contraindre un fournisseur d'accès à tenir un log book des accès susceptibles de conforter l'instruction."

D.2. IMPLICATIONS PRATIQUES

11. Les présentes dispositions auront un impact important sur la gestion de l'entreprise, non seulement pour les grands opérateurs connus tels que par exemple Belgacom, Mobistar ou Telenet, mais également au sein d'une entreprise ou d'une PME qui prévoit un accès Internet et un service de courriers électroniques pour leurs travailleurs. Dans la version actuelle du projet, même un réseau domestique ne semble pas exclu, si on le met à disposition d'invités par exemple. À l'avenir, ils seront tenus de conserver et d'enregistrer les données demandées

---

[3] Avis n° 08/2004 du 14 juin 2004 *sur l'avant-projet de loi relatif aux communications électroniques*.

[4] Recommandation n° 3/99 du 7 septembre 1999 *relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du* droit ; Avis 5/2002 du 11 octobre 2002 *sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications : "Lorsque des données de trafic doivent être conservées, [la] nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou tout autre forme d'abus. La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable."*

[5] Arrêts Klass et Malone.

pendant 24 mois ou plus. Ils doivent aussi satisfaire à des mesures de sécurité péremptoires, dont la création d'une 'Cellule de coordination de la Justice' et la nomination de préposés à la protection des données à caractère personnel. En outre, ils doivent immédiatement pouvoir mettre les données conservées à la disposition des demandeurs. Tout cela semble difficilement réalisable en pratique, d'autant que les réseaux visés à l'article 9, §§ 5 et 6 de la LCE ne doivent pas faire de déclaration auprès de l'IBPT et qu'il est par conséquent difficile d'effectuer par exemple un contrôle du respect des mesures de sécurité nécessaires par ces réseaux. Ils doivent également tenir compte des réglementations existantes en matière de protection de la vie privée, comme par exemple la CCT n° 81 du 26 avril 2002 concernant le contrôle de l'utilisation d'Internet et du courrier électronique sur le lieu de travail. Ces réglementations sont en contradiction flagrante avec ce que l'avant-projet de loi prévoit pour les fournisseurs visés à l'article 9, §§ 5 et 6 de la LCE. Enfin, il faut préciser à cet égard que la Directive 2006/24 ne vise que les services de communications électroniques ou les réseaux de communications **publics** et donc pas les fournisseurs visés à l'article 9, §§ 5 et 6 de la LCE.

12. En outre, il convient de signaler que les dispositions de la directive ont été rédigées en tenant notamment compte des remarques des opérateurs de télécommunications en matière de modalités techniques et pratiques d'enregistrement, comme les données à conserver. La Commission se demande dès lors dans quelle mesure le projet d'arrêté royal tient compte des possibilités techniques des opérateurs, certainement en ce qui concerne les données à conserver qui ne sont pas prévues dans la directive. La consultation du secteur par l'IBPT[6], récemment clôturée, pourra probablement fournir plus de précisions à ce sujet.

D.3. PRATIQUE ACTUELLE

13. Actuellement, il existe déjà un règlement détaillé concernant l'identification de numéros de téléphone (article 46*bis* du Code d'instruction criminelle, ci-après 'CIC') et le repérage ou la localisation de (télé)communications privées (article 88*bis* du CIC).

14. L'article 46*bis* du CIC octroie au procureur du Roi la compétence de requérir les données d'identification des services de télécommunication auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. Ainsi, on peut vérifier quels numéros de téléphone sont liés à une personne déterminée. À l'inverse, au départ du numéro de téléphone que l'on a trouvé quelque part, on peut également demander quel abonné

[6] Consultation réalisée par le Conseil de l'IBPT à la demande du Ministre pour l'Entreprise et la Simplification du 27 mai 2008 concernant la transposition de la Directive 2006/24, délai de réponse jusqu'au 16 juin 2008 inclus.

ou utilisateur habituel y est associé[7]. L'article 46*bis*, § 2 du CIC stipule que "*Chaque opérateur (…) qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi (…) les données qui ont été demandées dans un délai à fixer par le Roi*". L'arrêté royal du 9 janvier 2003 a exécuté cette disposition.

15. Pour le repérage et la localisation, une ordonnance du juge d'instruction est requise. Il s'agit (1) du repérage de données d'appel des moyens de télécommunication desquels ou vers lesquels certains appels sont ou ont été passés et (2) de la localisation de l'origine ou de la destination de la télécommunication. Cela permet de localiser des personnes participant à une conversation par GSM, notamment via des liaisons satellites et en déterminant l'antenne émettrice[8]. L'article 88*bis* du CIC stipule que "*chaque opérateur (…) communique les informations qui ont été demandées dans un délai à fixer par le Roi (…)*". Les modalités de la collaboration technique sont également déterminées par le Roi. L'arrêté royal du 9 janvier 2003 a exécuté cette disposition.

16. Il n'est pas clair de savoir pour quelle raison les articles susmentionnés et l'arrêté royal du 9 janvier 2003 qui les exécute ne suffiraient pas pour l'information judiciaire et l'instruction. Quelle est la nécessité d'une obligation de conservation telle que prévue par l'avant-projet de loi ? Quel est l'impact de l'avant-projet de loi et du projet d'arrêté royal sur les articles 46*bis* et 88*bis* du CIC susmentionnés, ainsi que sur l'arrêté royal du 9 janvier 2003 ? Les projets de textes ne nous renseignent pas à ce sujet.

D.4. DISCUSSION DES ARTICLES DE L'AVANT-PROJET DE LOI

ARTICLE 2

17. L'article 2 remplace l'actuel article 126 de la LCE. Le § 1er de l'article 2 de l'avant-projet de loi est libellé comme suit :

"*Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les opérateurs, ainsi que les fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6, conservent les données de trafic, de localisation et les données d'identification d'utilisateurs finals qui sont générées ou traitées par eux lors de la fourniture de réseaux ou de services de communications électroniques, et ce en vue :*

[7] VAN DEN WYNGAERT, C., "Strafrecht, strafprocesrecht en internationaal strafrecht, in hoofdlijnen", Maklu, 2006, p. 979.

[8] VAN DEN WYNGAERT, C., op. cit., p. 979-980.

a) de la recherche, de la poursuite et de la répression d'infractions pénales ;

b) de la répression d'appels malveillants vers les services d'urgence ;

c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques."

18. Comme déjà précisé au point 9 susmentionné, l'article 2 de l'avant-projet de loi ne mentionne pas uniquement les opérateurs mais également les fournisseurs et les revendeurs visés à l'article 9, §§ 5 et 6 de la LCE. Ainsi, les entités qui étaient auparavant visées dans la LCE par deux dispositions distinctes en matière de conservation de données sont regroupées en une seule disposition (le nouvel article 126).

19. Dans l'ancien article 126 de la LCE, ce qui précède était déjà prévu pour un opérateur, à présent les fournisseurs et les revendeurs mentionnés à l'article 9, §§ 5 et 6 de la LCE viennent également s'y ajouter. L'article 9, § 7 prévoyait qu'ils devaient également enregistrer et conserver les données pour les finalités a) et b) mais pas pour la finalité c). Dorénavant, c'est le cas. Par fournisseurs et revendeurs, il faut par exemple entendre le réseau interne d'un groupe d'entreprises. Toutefois, ceux-ci ne sont pas visés par la Directive 2006/24/CE qui, conformément à l'article 3, s'applique uniquement aux fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications dans le cadre de la fourniture des services de communication concernés.

20. La raison de ne pas mentionner les fournisseurs et les revendeurs dans l'actuel article 126 de la LCE mais bien dans l'article 9, § 7 de la LCE peut être retrouvée dans la justification donnée pour l'un des amendements[9] du projet de loi portant des dispositions diverses concernant les §§§ 5, 6 et 7 : "*Par ailleurs, il est nécessaire de prévoir une collaboration avec les autorités judiciaires. L'obligation de coopération telle qu'elle est prévue pour les opérateurs (avec notamment l'obligation de désigner une personne de contact avec les autorités judiciaires, disponible 7 jours sur 7 et 24 heures sur 24) n'est également pas opportune à cet égard. Par conséquent, la possibilité de définir des modalités relatives à la conservation de données et à la coopération avec les autorités judiciaires dans un arrêt d'exécution est créée.*" Ce passage démontre que l'on ne peut pas assimiler ainsi les fournisseurs et les revendeurs dont il est question à l'article 9, §§ 5 et 6 de la LCE à un opérateur au sens de l'article 2, 11° de la LCE. On ne voulait certainement pas déclarer applicable de la même façon aux fournisseurs et aux revendeurs la lourde procédure de collaboration avec les autorités judiciaires, telle que prévue dans l'arrêté royal du 9 janvier 2003. Il est dès lors étrange que cela se produise à présent, en

[9] Voir le projet de loi portant des dispositions diverses, 9 juin 2006, doc. 51, 2518/007, page 4.

rendant l'article 126 de la LCE (via le présent article 2 de l'avant-projet de loi) applicable non seulement aux opérateurs, mais également aux fournisseurs et aux revendeurs. **Vu que ceux-ci n'étaient pas visés par la Directive 2006/24, ni par les implications pratiques mentionnées au point 11 et vu le passage précité de la justification de la loi du 20 juillet 2006 *portant des dispositions diverses*, la Commission estime recommandé de les soustraire à l'application de l'article 2 de l'avant-projet de loi et de les reprendre dans une autre disposition. En général, concernant les présents projets, il convient de faire remarquer que sous prétexte d'une transposition de la directive, on essaie d'imposer bien plus que ce que celle-ci prévoit, en tant que cadre maximum (comme par exemple viser également les réseaux privés en plus des réseaux publics, enregistrer des données supplémentaires, ...).**

21. La Commission fait en outre remarquer qu'un opérateur qui traite des données pour le compte de l'État, comme c'est le cas au point a) de l'article 2 de l'avant-projet de loi, agit en tant que son sous-traitant, tel que défini à l'article 1, § 5 de la LVP. L'État pourrait donc dans ce cas être considéré comme le responsable du traitement. Il faut dès lors recommander ici de préciser explicitement à l'article 2 que les opérateurs sont considérés comme des responsables du traitement au sens de la LVP.

22. L'Exposé des motifs et l'avant-projet de loi précisent que le nouvel article 126 s'applique sans préjudice des dispositions de la LVP. Dès lors, les opérateurs sont désormais explicitement tenus (ce qui était d'ailleurs déjà le cas auparavant) de respecter l'ensemble des dispositions de la LVP et de son arrêté d'exécution du 13 février 2001. Cela correspond aux dispositions de la directive qui prévoit également une application de la Directive 95/46/CE aux opérateurs[10].

23. L'Exposé des motifs stipule que les opérateurs et les fournisseurs doivent respecter la LVP, notamment en ce qui concerne les droits des personnes concernées : "*elle pourra accéder à ses données et pourra, le cas échéant, les faire rectifier ou supprimer*". Le droit de consultation, tel que prévu à l'article 10 de la LVP, et le droit de rectification (article 12) sont jugés d'application dans leur intégralité. Les fournisseurs ou les opérateurs devraient transmettre, sur demande, un aperçu complet des données conservées. À cet égard, il faut préciser que l'abonné d'un raccordement pourrait avoir, via le droit de consultation, une idée du comportement de communication ou des données de localisation de tous les utilisateurs sur une période plus longue. Dans ce contexte, on peut penser aux travailleurs ou aux membres de la famille, dont des mineurs. L'Exposé des motifs ignore, à tort, cette problématique. Dans le cadre de la téléphonie fixe et mobile, il existe des solutions pour protéger la vie privée, comme le masquage

[10] Voir les considérants 15 et 16.

des numéros. Toutefois, cela ne vaut pas pour Internet. En effet, pour la transmission d'e-mails, aucune facture spécifiée n'est fournie et il ne semble donc pas y avoir non plus de solution pour masquer les données d'adresse.

24. L'article 2 prévoit aux points a), b) et c) les finalités particulières pour lesquelles les données de trafic, de localisation et les données d'identification des utilisateurs peuvent être utilisées. À cet égard, on peut formuler les remarques suivantes :

25. La finalité prévue au point a) : *recherche, poursuite et répression d'infractions pénales* constitue une transposition de la Directive 2006/24, dont le but est la recherche, la détection et la poursuite d'**infractions graves**. L'avant-projet de loi ne fait toutefois référence qu'à des infractions pénales, ce qui implique *de facto* que les données conservées peuvent être utilisées pour n'importe quelle infraction pénale, y compris des contraventions. Ceci n'est certainement pas conforme au principe de la directive, ni au principe de proportionnalité, qui prévoient la conservation de certaines données pour la lutte contre le crime organisé et le terrorisme, et donc pas pour n'importe quel délit (cf. ci-dessus, points 4-6).

26. Par analogie avec par exemple la loi MPR[11] ou l'article 90*ter* du CIC concernant les écoutes de communications privées, le législateur pourrait prévoir dans l'actuel avant-projet de loi une énumération stricte des délits graves pour la recherche, la poursuite et la répression desquels les données conservées peuvent être utilisées. Il faut au moins tenir compte des articles 46*bis* et 88*bis* du CIC, qui prévoient actuellement respectivement la réclamation, par le procureur du Roi, de données d'identification relatives à un service de télécommunication et la réclamation, par le juge d'instruction, de données de localisation d'une télécommunication. De cette manière, il serait également plus clair de savoir qui a accès aux données conservées, pour les finalités mentionnées au point a). À ce sujet, les projets ne prévoient rien, à l'exception de l'accès interne au sein des opérateurs (Cellule de coordination de la Justice). La directive stipule à l'article 4, concernant l'accès aux données, que les États membres doivent prendre *les mesures nécessaires pour veiller à ce que les données conservées ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne*.

27. **En outre, tout autre usage de ces données devrait être punissable et une sanction de nullité devrait également y être liée.** Voir à cet égard ce qui est stipulé à l'article 13, point 2 de la directive : "*Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en*

[11] Loi du 6 janvier 2003 *concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête.*

application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives." Étant donné que l'IBPT est compétent[12] pour contrôler le respect de la loi du 13 juin 2005 *relative aux communications électroniques* et des arrêtés d'exécution y afférents, la possibilité de sanctions alternatives est prévue, notamment des amendes administratives, que l'IBPT peut infliger en vertu de l'article 21 de la loi du 17 janvier 2003. Les projets ne stipulent toutefois pas explicitement quelle instance publique contrôle la sécurité des données conservées, ce qui est néanmoins prévu par l'article 9 de la directive. **Il convient de recommander de reprendre les autorités de contrôle dans l'avant-projet de loi, de même que leurs compétences et les sanctions, et de ne pas seulement y faire référence dans l'Exposé des motifs.**

28. Qu'en est-il de la preuve obtenue en dépit des dispositions de cette loi, par exemple par des personnes qui ne sont pas compétentes pour disposer de ces informations ? Si l'on souhaite exclure un tel moyen de preuve, il est recommandé de le prévoir explicitement dans l'avant-projet de loi, et **d'imposer la nullité d'une telle preuve**. La doctrine d'Antigone[13] de la Cour de cassation n'exclut en effet pas *ipso facto* la preuve obtenue de manière irrégulière.

29. Le point b) de l'article 2 de l'avant-projet de loi mentionne 'la répression d'appels malveillants vers les services d'urgence'. Le point c) prévoit 'la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques'. Ces points ne découlent pas de la transposition de la Directive 2006/24 mais sont prévus dans des dispositions spécifiques. Conformément à l'article 43*bis*, § 3, 7° de la loi du 21 mars 1991[14], le Service de Médiation est chargé d'*examiner la demande de toute personne se prétendant victime d'une utilisation malveillante d'un réseau ou d'un service de communications électroniques visant à obtenir communication de l'identité et de l'adresse des utilisateurs de réseaux ou de services de communications électroniques l'ayant importunée, pour autant que ces données sont disponibles*.

---

[12] Voir l'article 14 de la loi du 17 janvier 2003 *relative au statut du régulateur des secteurs des postes et des télécommunications belges.*

[13] Voir notamment à cet égard l'arrêt de la Cour de cassation du 14 octobre 2003, T. Strafr. 2004, 129 avec note de Ph. TRAEST.

[14] Loi du 21 mars 1991 *portant réforme de certaines entreprises publiques économiques*.

30. **Les points b) et c) ne font pas partie de la transposition de la Directive 2006/24. Étant donné que les finalités de ces points n'ont aucun rapport avec des 'infractions graves', on peut se demander pour quelle raison les points a), b) et c) sont repris dans le même article et traités de la même façon dans l'avant-projet de loi et le projet d'arrêté royal.** En effet, aucune distinction n'est prévue quant aux données conservées auxquelles on peut recourir, ni quant à la durée d'utilisation de ces données. Pour le point b) par exemple, l'accès aux données relatives aux services de courriers électroniques ne semble pas être nécessaire. Il n'est pas non plus démontré pour quelle raison ces données devraient être accessibles pendant 24 mois pour cette finalité. **En raison du principe de proportionnalité et du principe de finalité, repris à l'article 4 de la LVP, l'avant-projet de loi ou du moins le projet d'arrêté royal devrait prévoir une distinction entre les points susmentionnés. Idéalement, les points b) et c) doivent être régis dans une législation distincte.**

31. L'article 2, § 1er de l'avant-projet de loi prévoit en outre ce qui suit : "*Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du Ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver en application de l'alinéa 1er ainsi que les conditions et la durée de conservation de ces données.*"

32. **La Commission fait remarquer que le choix de ne pas reprendre les types de données dans le texte même de la loi mais dans un arrêté royal est difficilement compatible avec le choix formulé dans la Directive 2006/24 au sujet des données à conserver.** Initialement, la Commission européenne avait en effet proposé de joindre une liste de données en annexe à la directive, ce qui aurait permis une procédure accélérée du processus décisionnel pour des adaptations de cette liste. Le Parlement européen a toutefois adopté, à une large majorité, un amendement du rapporteur Alvaro visant à reprendre les données dans le texte même de la directive. On opte ainsi également pour une procédure plus lourde d'adaptation des types de données à conserver, avec un consentement complet dans le chef du Parlement européen. **Une même remarque doit être formulée en ce qui concerne le délai de conservation des données, cf. ci-dessous aux points 33 et suivants.** Ce qui précède vaut d'autant plus que dans l'Exposé des motifs, il est stipulé que le cadre pour la conservation des données, tel que prévu par la directive, ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires. Cela explique pour quelle raison on souhaite reprendre dans le projet d'arrêté royal des données supplémentaires qui ne sont pas prévues par la directive, telles que des données bancaires.

33. Quant à la durée de conservation, l'article 2, § 1er de l'avant-projet de loi prévoit ce qui suit : "*La durée de la conservation des données visées à l'alinéa 1er ne peut être inférieure à 6 mois ni dépasser 24 mois.*" L'article 6 de la directive précise que les données peuvent être conservées pendant un minimum de 6 mois et un maximum de 24 mois, à compter de la date de la communication. En ce qui concerne la durée, le projet d'arrêté royal opte pour la durée maximale de 24 mois prévue par la directive. Le Rapport au Roi motive ce choix sommairement, en affirmant que "*la pratique observée auprès des différents services de police décentralisés ou auprès du Parquet fédéral en matière de demandes d'informations aux opérateurs et aux fournisseurs de réseaux ou de services de communications électroniques, amène à considérer qu'un délai uniforme de vingt-quatre mois pour la conservation des différents types de données visés à l'article 126 de la loi, constitue le mécanisme le plus approprié.*"[15]

34. La Directive 2006/24 prescrit à l'article 6 un délai de conservation de minimum 6 mois et de maximum 2 ans. Le Groupe 29 a toujours maintenu le point de vue selon lequel l'instauration d'une obligation de conservation pour les données de trafic historiques de tous les citoyens était une mesure très radicale dont la nécessité devait être prouvée de manière irréfutable[16]. L'article 8 de la CEDH consacre le droit fondamental des citoyens au respect de leur vie privée. Les autorités ne peuvent porter préjudice à ce droit par une loi que dans la mesure où cela est *nécessaire* dans une société démocratique. La nécessité impose de grandes exigences concernant la proportionnalité de chaque mesure spécifique qui limite la vie privée des citoyens. Les dispositions générales de la directive ne changent rien au fait que chaque mise en œuvre nationale doit être confrontée de manière indépendante à l'article 8 de la CEDH et à la jurisprudence y afférente de la Cour européenne des Droits de l'Homme. Cela vaut explicitement pour la nécessité d'un délai de conservation plus long que le délai nécessaire à la gestion d'entreprise des fournisseurs-opérateurs.

35. La Commission constate que le Rapport au Roi donne peu d'explications quant à la manière dont le délai maximum de 24 mois a été fixé. On fait référence à la pratique auprès des différents services

---

[15] Rapport au Roi, page 1.

[16] Voir l'avis 4/2001 *concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité*, l'avis 10/2001 *sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme*, l'avis 4/2005 *sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE* et l'avis 3/2006 *sur la directive 2006/24/CE du Parlement européen et du Conseil 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 communication, et modifiant la directive 2002/58/CE*.

de police. La Commission demande que la nécessité de ce délai de conservation soit justifiée de manière plus précise et qu'elle soit étayée. À l'instar des récents avis du Groupe 29 sur ce sujet, la Commission recommande dès lors une application minimale harmonisée des dispositions de la directive, avec un délai de conservation qui diverge le moins possible de la finalité initiale pour laquelle les données sont enregistrées par les fournisseurs de services de communication. Il est nécessaire d'étayer par des arguments convaincants la durée d'une obligation de conservation qui est en effet contraire à l'obligation générale de destruction de la Directive 2002/58/CE. "*Comme indiqué ci-dessus, la justification d'une conservation systématique et obligatoire des données doit être clairement démontrée et étayée de preuves. Ce principe s'applique également aux périodes maximales à fixer.*"[17]

36. De plus, la Commission fait remarquer que le principal fondement de la directive, formulé à l'article premier, est l'harmonisation des dispositions des États membres relatives aux obligations en matière de conservation, en vue de garantir la disponibilité des données à des fins de recherche, de détection et de poursuite d'infractions graves. Compte tenu des mises en œuvre et des propositions dans d'autres États membres de l'Union européenne dont la Commission a connaissance, elle constate que jusqu'à présent, il est peu question d'une quelconque harmonisation du délai de conservation. L'Allemagne semble opter pour un délai de conservation de 6 mois, tout comme la Finlande et la Tchéquie. La Suède, un des quatre pays à l'initiative de la réalisation d'une obligation de conservation au niveau européen, semble également opter pour une mise en œuvre minimale. D'autres pays comme la France, le Danemark et l'Espagne optent pour un délai de conservation de 12 mois. Les Pays-Bas semblent également opter pour un délai de 12 mois. Pour autant que l'on sache, seule l'Italie opte pour une durée de conservation de 24 mois, et ce uniquement pour les données téléphoniques, l'enregistrement des données Internet étant de 6 mois.

37. **Vu ce qui précède, la Commission estime que la durée de conservation de 24 mois actuellement prévue doit être davantage étayée par des arguments plus convaincants. En l'absence d'une telle justification, une adaptation du délai prévu doit être envisagée, le cas échéant, certainement compte tenu des délais de conservation en vigueur dans la plupart des autres pays européens, qui vont actuellement de 6 à 12 mois.**

38. L'article 2, § 2 de l'avant-projet de loi prévoit que "*si des circonstances particulières le justifient, le Roi peut, après avis de l'Institut et de la Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à 24 mois.*"

[17] Avis 4/2005 du Groupe 29, page 8.

39. La Commission souligne tout d'abord que la version néerlandaise et la version française de l'avant-projet de loi diffèrent en ce qui concerne la période, qui est 'une période *limitée*' dans la version française et 'een *onbeperkte* periode' dans la version néerlandaise. Conformément à l'article 12 de la directive, cette prolongation doit être limitée dans le temps, et la version néerlandaise doit être adaptée en conséquence.

40. Le Roi a donc ainsi la possibilité de fixer un délai plus long que le délai légal maximal de 24 mois, *dans des circonstances particulières*. L'article 12 de la directive formule ceci comme suit : "*Un État membre confronté à des circonstances particulières justifiant une prolongation, pour une période limitée, de la durée de conservation maximale prévue à l'article 6, peut prendre les mesures nécessaires.*" S'il s'agit d'une exception, il est pour le moins nécessaire, aux yeux de la Commission, de régler le principe de base de cette exception de manière formelle dans la loi. Cette règle générale peut ensuite être développée ultérieurement dans un arrêté royal, mais le fondement devrait être ancré dans la loi, ce qui n'est pas le cas : **les termes 'circonstances particulières' n'offrent pas suffisamment de sécurité juridique, sont extrêmement vagues et sont dès lors sujets à une trop grande interprétation.**

D.5. ANALYSE DU PROJET D'ARRÊTÉ ROYAL

D.5.1. Examen général du projet d'arrêté royal

41. En ce qui concerne la durée de conservation de 24 mois qui est prévue dans le projet d'arrêté royal, la Commission renvoie aux remarques formulées aux points 33 et suivants. Elle rappelle également que la durée de conservation et les types de données conservées devraient de préférence être définis dans la loi et non dans le projet d'arrêté royal, cf. supra au point 32.

42. La durée de conservation est abordée différemment dans le projet d'arrêté royal selon la nature des données : les données servant à l'identification de l'abonné et du service utilisé sont conservées pendant toute la durée de l'abonnement et pour une période de 24 mois à compter du jour où l'abonnement expire. Les données de trafic et de localisation sont conservées pour une période de 24 mois à compter du jour où elles ont été générées ou traitées par le fournisseur de services. Ce qui précède semble aller à l'encontre du texte de la directive, où la durée de conservation débute à compter de la date de la communication.

43. L'Exposé des motifs[18] stipule que la directive prévoit un cadre minimum pour la conservation des données en matière de communication électronique, qui ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. D'après l'Exposé des motifs, il manque ainsi, dans la liste établie par la directive, certaines données qui sont indispensables en vue de l'identification de personnes concernées par une communication pertinente dans le cadre d'une enquête en matière répressive, telles que des données bancaires. À noter que l'Exposé des motifs affirme que des données supplémentaires sont nécessaires pour l'enquête en matière répressive, mais que ces données sont également rendues publiques, ou du moins ne sont pas verrouillées, pour des enquêtes effectuées par le Service de médiation ou dans le cadre de la répression d'appels malveillants vers les services d'urgence. Comme déjà remarqué ci-dessus aux points 22 et 23, il faut préciser qui a accès à quelles données. À la lumière du principe de proportionnalité, on ne peut en effet avoir accès qu'aux données dont on a besoin réellement. Quoi qu'il en soit, la Commission ne peut pas adhérer à la considération de l'Exposé des motifs selon laquelle la directive prévoirait un cadre minimum : la directive prescrit de manière détaillée à l'article 5 quelles catégories de données doivent être conservées. Au considérant 21, la directive stipule que ses objectifs sont la recherche, la détection et la poursuite d'infractions graves et qu'elle n'excède pas ce qui est nécessaire pour atteindre ces objectifs. D'après le considérant 12 de la directive, la liste des "catégories de données" doit être comprise comme un cadre maximum. Pour la conservation d'autres données, les États membres peuvent recourir à l'article 15, premier alinéa de la Directive 2002/25/CE. **La législation qui est promulguée sur la base de cet article doit répondre de manière distincte à l'exigence de l'article 8 de la CEDH, à savoir qu'elle doit être, dans une société démocratique, nécessaire, raisonnable et proportionnelle en vue de garantir la sécurité nationale ou de prévenir, rechercher et poursuivre des infractions pénales.** La Commission a réclamé aux rédacteurs du projet une liste reprenant les données supplémentaires à conserver - c'est-à-dire en sus de ce qui est prévu dans la directive. Une telle liste n'a toutefois pas encore pu lui être fournie, de sorte que la Commission tente de vérifier elle-même ci-après – sous réserve d'une mauvaise interprétation – ce qui correspond à la directive et ce qui s'en écarte. La Commission a fait remarquer à cet égard que, pour chaque catégorie de données, l'on conserve visiblement davantage dans le projet d'arrêté royal que ce qui est prévu dans la directive, que ce choix soit motivé ou non. La Commission s'y penchera de plus près ci-dessous dans la discussion des articles.

[18] Exposé des motifs, p. 1-2.

D.5.2. Discussion des articles du projet d'arrêté royal

ARTICLE 1er

44. Cet article définit plusieurs notions, parmi lesquelles celle de "données personnelles" : on entend par là les nom et prénom et les adresses de facturation et de contact de l'abonné ou de l'utilisateur. Il y a lieu de préciser que cette définition ne correspond pas à celle des "données à caractère personnel" de l'article 1, § 1 de la LVP, qui est beaucoup plus large. La Commission part dès lors du principe que le but n'est pas d'utiliser ici la même définition que celle prévue par la LVP.

ARTICLE 2

45. L'article 2 concerne les données que doivent conserver les opérateurs en téléphonie fixe, c'est-à-dire ceux qui proposent un service de téléphonie fixe accessible au public. Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation lors d'une communication.

46. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. **La Commission fait remarquer que seuls les éléments 1° et 2° (le numéro attribué à l'abonné et les données personnelles de l'abonné) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 8° inclus.** Cette extension n'est pas motivée, sauf par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. Concernant l'élément 6°, le commentaire des articles stipule que "*Ces données peuvent se révéler extrêmement importantes afin de déterminer vers quel opérateur les autorités judiciaires devront éventuellement se tourner pour obtenir des informations antérieures ou postérieures à une période donnée*." En ce qui concerne l'élément 7°, les données bancaires, la Commission remarque que ces données peuvent être obtenues auprès des banques par les enquêteurs, étant donné que ces derniers disposent des données d'identité. Dans quelle mesure est-il donc proportionnel de reprendre ces données ici ?

47. La collecte des éléments 3° à 8° inclus va au-delà de la liste prévue à l'article 5 de la directive. Comme déjà précisé ci-dessus, cette liste doit être considérée comme un cadre maximum en vertu du considérant 12 de la directive. Pour conserver d'autres données, les États membres peuvent recourir à l'article 15, premier alinéa de la Directive 2002/25/CE. La législation qui est promulguée sur la base de cet article doit répondre de manière distincte à l'exigence de l'article 8 de la CEDH, à savoir qu'elle doit être, dans une société démocratique, nécessaire, raisonnable et proportionnelle en vue de garantir la sécurité nationale ou de prévenir, rechercher et poursuivre des infractions pénales. Jusqu'à présent, le projet d'arrêté royal n'y satisfait pas.

48. La deuxième catégorie de données est constituée de données générées lors d'une communication. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 3

49. Cet article concerne les données que doivent conserver les opérateurs en téléphonie mobile, c'est-à-dire ceux qui proposent un service de téléphonie mobile accessible au public. Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation lors d'une communication.

50. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. **La Commission fait remarquer que seuls les éléments 1° et 2° (le numéro attribué à l'abonné et les données personnelles de l'abonné) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 10° inclus.** Cette extension est motivée sommairement, principalement par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. Concernant les éléments 3° et 4°, le commentaire des articles stipule que "*Savoir quand la carte a été achetée, et quand elle a été utilisée la première fois peut fournir des indices précieux aux enquêteurs.* (...) *La conservation des informations relatives à la recharge de crédit liée à une carte prépayée permet de connaître la capacité d'utilisation dont dispose l'utilisateur, le mode de recharge qu'il a utilisé, ou encore l'endroit où la recharge a été effectuée. Ce type d'information sort du cadre des données normalement visées par la directive mais représente un réel intérêt dans le cadre d'une enquête où ce peu d'information est souvent la seule piste dont disposent*

les services de police afin de tenter d'identifier un suspect." La Commission suit cette explication, mais estime, en raison des remarques déjà formulées aux points 43 et 47, que cela ne suffit pas pour aller au-delà de ce qui est prévu par la directive.

51. La deuxième catégorie de données est constituée de données générées lors d'une communication. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 4

52. Cet article vise les fournisseurs d'un accès à l'Internet. Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation.

53. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. **La Commission fait remarquer que seuls les éléments 1° et 2° (le code identifiant attribué à l'abonné et les données personnelles de l'abonné) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 8° inclus.** Cette extension est motivée sommairement par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. La Commission prend note de cette explication mais estime, en raison des remarques déjà formulées aux points 43 et 47, que cela ne suffit pas pour aller au-delà de ce qui est prévu par la directive.

54. La deuxième catégorie de données comprend des données relatives au trafic et à la localisation. **La Commission fait remarquer que seuls les éléments 1° à 4° inclus et 6° (mais d'après la directive, uniquement pour le début, pas pour la fin) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 5° et 7°.** Cette extension n'est pas motivée, et ne peut dès lors pas être suivie vu les remarques déjà formulées ci-dessus.

ARTICLE 5

55. L'article 5 vise les données à conserver par les fournisseurs de services de courriers électroniques et par les fournisseurs de services téléphoniques par Internet. Par fournisseurs de services de courriers électroniques, on vise tant les courriers SMTP que les webmails tels que Hotmail, Yahoo, Gmail, … Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation.

56. En ce qui concerne les services de webmail tels que Hotmail et Gmail, on ne sait pas clairement sur quelle base ils sont soumis à l'obligation de conservation. Ni l'Exposé des motifs, ni le Rapport au Roi n'apportent des précisions à cet égard.

57. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci, ou lorsqu'il utilise les services proposés. **La Commission fait remarquer que seuls les éléments 1° et 2° (le code identifiant de l'abonné ou de l'utilisateur et les données personnelles de l'abonné ou de l'utilisateur) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 6° inclus.** Cette extension est motivée sommairement par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. La Commission prend note de cette explication mais estime, en raison des remarques déjà formulées aux points 43 et 47, que cela ne suffit pas pour aller au-delà de ce qui est prévu par la directive.

58. La deuxième catégorie de données est constituée de données générées lors d'une communication. La Commission n'a pas de remarque à formuler à cet égard, sauf au sujet du point 7° (concernant ce point, la directive prévoit uniquement l'enregistrement de la localisation au début).

ARTICLE 6

59. Le premier alinéa de l'article 6 vise les opérateurs qui fournissent différents services combinés, tel que par exemple l'envoi de mails via un gsm. Les données qu'ils devront conserver dans le cas précité doivent correspondre à ce qui a été prévu tant à l'article 3 (téléphonie mobile) qu'à l'article 5 (courrier électronique) du projet d'arrêté royal. **La Commission se réfère aux remarques formulées ci-avant pour les articles 2 à 5 inclus, qui s'appliquent *mutatis mutandis* à l'article 6.**

60. Les deuxième et troisième alinéas concernent des dispositions relatives aux indications de l'heure, qui ont été reprises de l'arrêté royal du 9 janvier 2003. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 7

61. D'après le commentaire des articles, l'article 7 fixe un certain nombre de conditions de conservation destinées à garantir la sécurité des données et à assurer leur traitement adéquat par du personnel autorisé. Les éléments 1°, 2° et 4° ont été directement repris de l'article 7 de la Directive 2006/24. Le point 1 prévoit un enregistrement distinct pour les données à conserver, ce qui concorde avec les recommandations du Groupe 29 qui prévoient un enregistrement décentralisé et tenu logiquement de manière distincte des données à conserver spécifiquement à des fins de recherche. D'un point de vue de la vie privée, il doit y avoir une distinction claire entre les données conservées par les opérateurs à des fins professionnelles et celles conservées dans le cadre des présents projets. Le projet d'arrêté royal reste par ailleurs relativement vague pour l'élément 2°, en ne faisant référence qu'à des "mesures techniques et organisationnelles appropriées", sans les développer davantage. À cet égard, la Commission se réfère pour information aux mesures de référence qu'elle a établies, lesquelles, selon le cas, doivent s'appliquer à un traitement de données à caractère personnel[19].

62. L'élément 3° oblige l'opérateur à garantir que seule la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 ait accès aux données.

[19] Voir à cet égard le document intitulé "Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" de la Commission de la protection de la vie privée, disponible sur son site Internet à l'adresse http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf.

63. **La Commission fait tout d'abord remarquer à cet égard que seul l'accès aux données auprès des opérateurs eux-mêmes est ainsi régi, c'est-à-dire en interne, et non à qui ces données peuvent être transmises en externe.** Conformément à l'article 2, § 1 de l'arrêté royal précité : "*Pour satisfaire à l'obligation de collaboration imposée par les articles 46bis, § 2, 88bis, § 2 et 90quater, § 2, du Code d'Instruction criminelle, chaque opérateur d'un réseau de communications et chaque fournisseur d'un service de télécommunications désigne nommément une ou plusieurs personnes chargées d'assumer les tâches résultant de l'obligation de coopérer et dénommée(s) ci-après la 'Cellule de coordination de la Justice'*". Comme déjà indiqué aux points 26, 29 et 30, il faudrait prévoir clairement à qui quelles données peuvent être transmises par la Cellule de coordination de la Justice. Conformément à l'article 2, § 1, c) de l'avant-projet de loi, le Service de médiation pour les télécommunications devrait par exemple également pouvoir obtenir un droit de regard, ce qui n'est pas prévu explicitement au stade actuel. **Il convient de déterminer clairement et de manière limitative, de préférence dans l'avant-projet de loi, qui a accès aux données conservées, à quelles données en particulier et pour quelles finalités spécifiques.**

64. **Il convient en outre de répéter que cette cellule de coordination n'a été installée par l'arrêté royal du 9 janvier 2003 qu'auprès des opérateurs et non auprès des fournisseurs et revendeurs mentionnés à l'article 9, §§ 5 et 6 de la LCE.** Le but est-il que les fournisseurs et revendeurs créent également une telle cellule de coordination, qui doit répondre aux mêmes dispositions, notamment en matière de disponibilité 24h/24 et 7j/7 ? Comme déjà remarqué ci-avant au point 16, le législateur a exclu précédemment cette égalité de traitement entre les opérateurs d'une part et les fournisseurs et revendeurs d'autre part, en n'y faisant pas référence dans la version actuelle de l'article 126 de la LCE, mais bien à l'article 9, § 7 de cette même loi, qui prévoit un règlement distinct pour cette catégorie.

65. **Ensuite, "la garantie" de l'opérateur que seule la Cellule de coordination de la Justice ait accès n'est pas suffisante ; le non-respect de cette règle d'accès interne devrait être sanctionné pénalement.** Voir à ce sujet ce qu'énonce l'article 13, point 2 de la directive : "*Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives*."

66. Enfin, chaque opérateur doit veiller à ce que les données soient détruites à l'expiration du délai de conservation, à l'exception des données auxquelles on a pu accéder et qui ont été

préservées. Aucun délai de conservation n'est prévu à l'égard de ces dernières données. Il semblerait toutefois logique que si les données ont été consultées dans le cadre d'une enquête judiciaire, celles-ci soient conservées ultérieurement par les services responsables pour la durée nécessaire à leur enquête et puissent être détruites chez l'opérateur. Si les instances qui mènent l'enquête estimaient toutefois que les données ne sont pas utiles pour l'enquête, il n'est pas nécessaire de faire conserver les données par l'opérateur au-delà du délai de conservation prévu.

ARTICLES 8 ET 9

67. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 10

68. Cet article dispose que le projet d'arrêté royal s'applique également aux tentatives d'appel ayant échoué. La Directive 2006/24 dispose à l'article 3, point 2 qu'elle n'impose pas la conservation des données relatives aux appels non connectés, mais bien concernant les appels téléphoniques infructueux, ce qui constitue, selon la directive, toute communication au cours de laquelle un appel téléphonique a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau[20].

69. La formulation de l'article 10 ne correspond pas tout à fait, affirmant que l'arrêté s'applique également aux appels qui n'ont pas pu aboutir en raison d'une intervention de la part du gestionnaire de réseau. Il serait recommandé de reformuler ce passage, par exemple comme suit : " (...) *également aux appels qui ont fait l'objet d'une intervention de la part du gestionnaire du réseau*."

ARTICLE 11

70. D'après le commentaire des articles, l'article 11 institue, au sein de chaque Cellule de coordination de la Justice, un préposé à la protection des données, comme le permet l'article 17*bis*, alinéas 2 et 3 de la LVP. L'article 11, alinéa 3 vise à garantir l'indépendance du préposé dans ses fonctions.

[20] Voir l'article 2, f) de la Directive 2006/24/CE.

71. La Commission souligne que le Roi n'a pas encore fixé le statut des préposés à la protection des données en application de l'article 17*bis* de la loi LVP. Il serait donc prématuré d'anticiper des dispositions futures. Toutes les définitions de fonctions de contrôle, qu'elles soient internes ou non, devraient donc tenir compte de la Directive 95/46/CE (considérant (49) et article 18). Les préposés à la protection des données visés ici devraient en pratique être des interlocuteurs privilégiés de la Commission, ce qui est encouragé dans le projet d'arrêté royal par l'obligation de communiquer à la Commission leurs données d'identification et leurs coordonnées. Il est également recommandé que le projet d'arrêté royal assure une grande visibilité pour leurs avis et rapports. Dans cette optique, la Commission recommande que le projet d'arrêté royal soit adapté de manière à ce que ces rapports lui soient également communiqués de manière systématique.

72. L'indépendance des préposés à la protection des données est primordiale. Il importe toutefois qu'elle soit garantie par des mesures appropriées. Les mesures suivantes peuvent être intégrées dans le projet d'arrêté royal, outre celles déjà mentionnées à l'article 11 :

• communication à la Commission de la nature du lien juridique entre ces préposés et le service dans lequel ils exerceront leur fonction de préposé, de tous les éléments concernant les qualifications professionnelles relatives à la fonction de préposé, des mesures prises par le responsable du traitement en fonction des missions que doit exercer le préposé à la protection des données ;

• obligation de placer les préposés à un niveau de la hiérarchie tel qu'ils aient la possibilité de communiquer directement avec le management/comité de direction et d'exercer leur mission directement auprès du responsable du traitement.

73. Il convient enfin de répéter que l'article 11, § 2, 3° doit être précisé, cf. le point 63 ci-dessus, étant donné que ni le projet d'arrêté royal, ni l'avant-projet de loi n'établissent clairement qui, au sein de la Cellule de coordination de la Justice, a accès en externe aux données conservées.

ARTICLE 12

74. L'article 12 oblige les opérateurs concernés à communiquer annuellement à l'Institut un certain nombre d'informations statistiques qui seront destinées à la Commission des Communautés européennes. Étrangement, l'article 12 n'impose cela qu'à "l'opérateur fournissant un service de téléphonie accessible au public". Si l'on choisit de déclarer que l'avant-projet de loi et le projet d'arrêté royal s'appliquent également aux fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6 de la LCE, ils doivent également être repris dans cet article. Il ne s'agit pas non plus, conformément à l'article 10 de la directive, d'un "service de téléphonie", mais bien d'un service de communication électronique ou d'un réseau de communication.

ARTICLES 13 ET 14

75. La Commission n'a pas de remarque à formuler à cet égard.

PAR CES MOTIFS,

la Commission estime que :

- vu le principe de légalité, les éléments essentiels en matière de conservation de données doivent être définis clairement dans l'avant-projet de loi. Dans cette optique, la durée de conservation devrait être définie dans l'avant-projet de loi, de même que les données à conserver ;
- la nécessité de conserver certaines données qui ne sont pas prévues dans la directive doit être justifiée, conformément aux principes de l'article 8 de la CEDH ;
- l'avant-projet de loi devrait préciser pour la recherche, la poursuite et la répression de quelles infractions pénales (graves) les données conservées peuvent être utilisées ;
- la durée de conservation de 24 mois doit être davantage fondée et justifiée et, le cas échéant, reconsidérée au vu des délais de conservation prévus dans la plupart des pays européens ;
- l'application de l'avant-projet de loi et du projet d'arrêté royal aux fournisseurs et aux revendeurs prévus à l'article 9, §§ 5 et 6 doit être réexaminée et doit éventuellement être prévue pour eux dans une autre disposition ;
- la conservation des données pour les finalités prévues à l'article 2, § 1, b) et c) (les appels malveillants vers les services d'urgence et le Service de médiation pour les

télécommunications) doit être retirée de l'application de l'avant-projet de loi, et qu'il faut prévoir à cet égard une réglementation distincte ;

- des exceptions ne peuvent pas être régies par un arrêté royal, mais que le principe de base de l'exception doit au moins être réglé dans la loi. La notion de "circonstances particulières" de l'article 2, § 2 de l'avant-projet de loi est trop vague ;
- la désignation des personnes ou instances qui ont accès aux données conservées via la Cellule de coordination de la Justice doit être faite explicitement dans l'avant-projet de loi, en mentionnant également qui a accès à quelles données ;
- le non-respect des exigences en matière d'accès et d'utilisation des données collectées doit être sanctionné ;
- les autorités de contrôle doivent être explicitement désignées dans l'avant-projet de loi, de même que leurs compétences et les sanctions en la matière.

Vu les remarques formulées dans le présent avis, la Commission de la protection de la vie privée émet un avis *défavorable* quant au contenu actuel de l'avant-projet de loi et du projet d'arrêté royal.

Pour l'Administrateur e.c.,
Le Chef de section OMR,

(sé) Patrick Van Wouwe

Le Président,

(sé) Willem Debeuckelaere

Advies nr. 24 /2008 van 2 juli 2008

Betreft: Advies betreffende het voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 *betreffende de elektronische communicatie*, en betreffende het ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van bewaring van de gegevens (A/08/024)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna "WVP"), inzonderheid artikel 29;

Gelet op het verzoek om advies van de Minister voor Ondernemen en Vereenvoudigen ontvangen op 23/05/2008;

Gelet op het verslag van mevrouw Anne Vander Donckt;

Brengt op 02/07/2008 het volgend advies uit:

A. INLEIDING

1. Op 23 mei 2008 heeft de Minister voor Ondernemen en Vereenvoudigen de Commissie verzocht om advies uit te brengen inzake het de voorstellen tot omzetting van de Europese Richtlijn 2006/24/EG *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*.

2. Het betreft meer bepaald een voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 *betreffende de elektronische communicatie* (hierna 'het voorontwerp van wet'), en een ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van de bewaring van die gegevens (hierna 'het ontwerp kb'). De Commissie zal hiernavolgend dan ook advies uitbrengen inzake deze ontwerpen, rekening houdend met de informatie waarover ze beschikt.

B. TOEPASSELIJKE WETGEVING

3. Vooreerst kan worden verwezen naar de Richtlijn 2006/24/EG. Aangezien er persoonsgegevens worden verwerkt is verder de WVP van toepassing, evenals de wet van 13 juni 2005 *betreffende de elektronische communicatie* (hierna 'WEC'). Tenslotte dient het koninklijk besluit vermeld van 9 januari 2003 *tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid, en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109ter, E, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven* (hierna 'het kb van 9 januari 2003').

C. VOORGESCHIEDENIS

4. Diverse Europese lidstaten hebben in het verleden wetgeving aangenomen op het gebied van het bewaren van gegevens door aanbieders van diensten ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Deze nationale bepalingen vertonen onderling aanzienlijke verschillen. De juridische en technische verschillen tussen de nationale bepalingen op het gebied van het bewaren van gegevens ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten belemmeren de werking van de interne markt voor elektronische communicatie. De aanbieders van diensten immers worden geconfronteerd met uiteenlopende voorschriften wat betreft de categorieën te bewaren verkeers- en locatiegegevens, de bewaringsvoorwaarden en bewaringstermijnen.

5. In de conclusies van de Europese Raad justitie en binnenlandse zaken van 19 december 2002 wordt benadrukt dat wegens de opmerkelijke toename van de mogelijkheden van elektronische communicatie, gegevens betreffende het gebruik daarvan van bijzonder belang zijn en een waardevol instrument bij het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, met name in de strijd tegen de georganiseerde misdaad. In zijn verklaring betreffende de bestrijding van terrorisme van 25 maart 2004 heeft de Europese Raad aan de Raad justitie en binnenlandse zaken opdracht gegeven maatregelen te bestuderen met het oog op het vaststellen van regels voor het bewaren van verkeersgegevens door telecommunicatieaanbieders. In de verklaring ter veroordeling van de terroristische aanslagen op Londen die is aangenomen door de bijzondere vergadering van de Europese Raad van 13 juli 2005 wordt nogmaals nadrukkelijk gewezen op de noodzaak om zo spoedig mogelijk gemeenschappelijke maatregelen aan te nemen in verband met het bewaren van verkeersgegevens van elektronische communicatie.

6. **De doelstellingen van de Richtlijn 2006/24/EG bestaan derhalve in het harmoniseren van de aan aanbieders opgelegde verplichtingen inzake het bewaren van sommige gegevens en het waarborgen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.**

7. De Groep 29[1] heeft in haar advies 3/2006 inzake de Richtlijn 2006/24 erop gewezen dat de lidstaten om de bepalingen van de richtlijn op uniforme wijze om te zetten en de bepalingen van artikel 8 van het EVRM in acht te nemen, afdoende specifieke garanties moeten invoeren, welke minstens het volgende zouden moeten omvatten :

- specificatie van het doel : duidelijke definitie en afbakening van 'ernstige strafbare feiten';
- beperking van de toegang : de gegevens mogen alleen beschikbaar zijn voor uitdrukkelijk aangewezen wetshandhavingautoriteiten;
- gegevensminimalisering;
- geen datamining;
- onafhankelijke controle van machtiging tot toegang;
- scheiding van systemen;
- veiligheidsmaatregelen;
- doel van bewaring van gegevens door aanbieders.

D. ONDERZOEK VAN DE ADVIESAANVRAAG

D.1.VERGELIJKING HUIDIGE ARTIKEL 126 WEC MET HET NIEUWE VOORONTWERP

8. Artikel 126 WEC luidt momenteel als volgt : ' *§ 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de Minister van Justitie en van de minister en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst.*
§ 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut.

[1] Deze werkgroep werd in het leven geroepen door artikel 29 van de Richtlijn 95/46/EG, en is een onafhankelijk adviserend orgaan met betrekking tot de bescherming van persoonsgegevens. Haar taken zijn beschreven in artikel 30 van de Richtlijn 95/46/EG en in artikel 15 van de Richtlijn 2002/58/EG.

De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België.'

9. Het kb waarvan sprake in §2 is er nooit gekomen. Het huidige artikel 126 WEC is van toepassing op de operatoren, en niet op de aanbieders en doorverkopers voorzien in artikel 9, §§5 en 6 WEC. Hiermee worden bijvoorbeeld[2] bedoeld de netwerken of diensten bestemd voor gebruik door leden van een groep van ondernemingen, een netwerk van een universiteit, een bank en haar agenten, … . In het voorontwerp van wet worden de aanbieders en doorverkopers wél opgenomen in artikel 126 WEC. Het voorontwerp van wet voegt ook de locatiegegevens toe aan het huidige artikel 126 WEC.

10. In haar advies 08/2004[3] heeft de Commissie over het huidige artikel 126 WEC onder meer verklaard :

'De Commissie herinnert aan de opmerkingen die zij formuleerde in haar advies 33/99 van 13 december 1999 en die op Europees niveau door de groep van Europese functionarissen voor gegevensbescherming meerdere keren werd herhaald en die het a priori vasthouden van communicatiegegevens en de verenigbaarheid hiervan met de fundamentele beginselen van bescherming van persoonsgegevens, betreffen[4].' Zo had de Commissie eraan herinnerd dat *'noch de internationale teksten (…) noch de wet van 8 december 1992 (beginselen van proportionaliteit, beperkte bewaartijd,…) algemene toezichtsmethodes toestaan die los staan van een onderzoek naar specifieke misdrijven (uitgezonderd het zeer specifieke geval van de proactieve recherche, die strikt omkaderd is).'* De Commissie refereert ook nog aan de jurisprudentie van het Europees Hof van de Rechten van de Mens[5] *'die leidt tot het verbieden van de op grote schaal gehanteerde verkennende en algemene toezichtsmethodes op telecommunicatiediensten. Aldus zou een access provider niet verplicht kunnen worden om systematisch alle oproepen uitgaande van zijn klanten te registreren, maar alleen wanneer een onderzoek wordt ingesteld naar een specifieke persoon. Hij zou ook niet*

---

[2] Zie Belgische Kamer van Volksvertegenwoordigers, verantwoording bij de amendementen bij het wetsontwerp houdende diverse bepalingen, Doc 51, 2873/002.

[3] Advies nr. 08/2004 van 14 juni 2004 betreffende het voorontwerp van wet betreffende de elektronische communicatie.

[4] Aanbeveling nr. 3/99 van 7 september 1999 over de bewaring van verkeersgegevens door Internetdienstenaanbieders voor wetshandhavingsdoeleinden ; Advies 5/2002 van 11 oktober 2002 over de verklaring van de Europese functionarissen voor gegevensbescherming tijdens de internationale conferentie van Cardiff (9-11 september 2002) over het verplicht systematisch bewaren van telecommunicatiegegevens : "Indien verkeersgegevens in specifieke gevallen moeten worden bewaard, moet de noodzaak daarvoor duidelijk worden aangetoond, moet de bewaarperiode zo kort mogelijk zijn en moet de desbetreffende praktijk duidelijk bij de wet zijn geregeld, op zodanige wijze dat voldoende waarborgen worden geboden tegen onrechtmatige toegang en andere misbruiken. Het systematisch bewaren van alle soorten verkeersgegevens voor een periode van een jaar of meer zou zeker in strijd zijn met het evenredigheidsbeginsel en derhalve in ieder geval onaanvaardbaar zijn."

[5] Arresten Klass en Malone.

mogen gedwongen worden om een logboek bij te houden van de toegangen die het onderzoek zouden kunnen sterken '.

D.2. PRAKTISCHE IMPLICATIES

11. De voorliggende bepalingen zullen een niet geringe impact hebben op de bedrijfsvoering, niet enkel van de grote gekende operatoren zoals bijvoorbeeld Belgacom, Mobistar, Telenet, maar eveneens binnen een onderneming of KMO, die internettoegang en emailverkeer voorzien voor hun werknemers. Onder de huidige versie van het ontwerp lijkt zelfs een thuisnetwerk niet uitgesloten, indien men dit bijvoorbeeld beschikbaar stelt voor gasten. Zij zullen in de toekomst gehouden zijn om de gevraagde gegevens te bewaren en op te slaan gedurende 24 maanden, of langer. Tevens dienen zij te voldoen aan stringente veiligheidsmaatregelen, waaronder de creatie van een 'Coördinatiecel Justitie' en de nominatie van aangestelden voor de bescherming van persoonsgegevens. Daarnaast moeten zij de bewaarde gegevens onverwijld ter beschikking kunnen stellen van de aanvragers. Één en ander lijkt in de praktijk moeilijk uitvoerbaar te zijn, temeer daar de netwerken geviseerd door artikel 9, §§5 en 6 WEC geen aangifte bij het BIPT dienen te doen, en er derhalve moeilijk een controle kan gebeuren naar bijvoorbeeld de naleving door deze netwerken van de noodzakelijke veiligheidsmaatregelen. Zij dienen ook rekening te houden met de bestaande privacyreglementeringen, zoals bijvoorbeeld de CAO nr. 81 van 26 april 2002 inzake de controle op het gebruik van internet en email op de werkvloer. Deze reglementeringen staan haaks op hetgeen door het voorontwerp van wet wordt voorzien voor de aanbieders bedoeld in artikel 9, §§5 en 6 WEC. Tenslotte dient er in dit verband op gewezen dat de Richtlijn 2006/24 enkel de **openbare** elektronische communicatiediensten of -netwerken viseert, en dus niet de aanbieders bedoeld in artikel 9, §§5 en 6 WEC.

12. Daarnaast dient opgemerkt dat de bepalingen van de richtlijn zijn opgesteld onder meer rekening houdende met de opmerkingen van de telecomoperatoren inzake de technische en praktische modaliteiten van opslag, zoals de te bewaren gegevens. De Commissie stelt zich dan ook de vraag in hoeverre het ontwerp kb met de technische mogelijkheden van de operatoren rekening houdt, zeker wat betreft de te bewaren gegevens buiten hetgeen wordt voorzien door de richtlijn. De recent afgesloten raadpleging van de sector door het BIPT[6] zal hierover waarschijnlijk meer duidelijkheid kunnen verschaffen.

[6] Raadpleging door de Raad van het BIPT op verzoek van de Minister voor Ondernemen en administratieve Vereenvoudiging van 27 mei 2008 betreffende de omzetting van Richtlijn 2006/24, antwoordtermijn t.e.m 16 juni 2008.

D.3. HUIDIGE PRAKTIJK

13. Er bestaat vandaag reeds een uitvoerige regeling betreffende de identificatie van telefoonnummers (art. 46bis wetboek van strafvordering, hierna 'Sv.') en het opsporen of lokaliseren van privé (tele)communicaties (art. 88bis Sv.).

14. Art. 46bis Sv. verleent aan de procureur des Konings de bevoegdheid de identificatiegegevens op te vorderen met betrekking tot de telecommunicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden. Zo kan nagegaan worden welke telefoonnummers gekoppeld zijn aan een bepaalde persoon. Omgekeerd kan ook, vertrekkend van het telefoonnummer dat men ergens heeft aangetroffen, opgevraagd worden welke abonnee of gewoonlijke gebruiker daaraan gekoppeld is.[7] Artikel 46bis, §2 Sv. bepaalt dat iedere operator van wie gevorderd wordt de in §1 bedoelde gegevens mee te delen, deze verstrekt aan de procureur des Konings binnen een termijn te bepalen door de Koning. Het kb van 9 januari 2003 heeft hieraan uitvoering gegeven.

15. Voor het opsporen of lokaliseren is een bevel van de onderzoeksrechter vereist. Het betreft (1) de opsporing van oproepgegevens van de telecommunicatiemiddelen van waaruit of waarnaar bepaalde oproepen worden of werden gedaan en (2) de lokalisering van oorsprong of bestemming van telecommunicatie. Hierdoor kunnen deelnemers aan een per GSM gevoerd gesprek worden gelokaliseerd, onder meer via satellietverbindingen en zendmastbepaling.[8] Artikel 88bis, §2 Sv. bepaalt dat iedere operator de gegevens waarom verzocht werd meedeelt binnen een termijn te bepalen door de Koning. De modaliteiten van de technische medewerking worden eveneens vastgesteld door de Koning. Het kb van 9 januari 2003 heeft hieraan uitvoering gegeven.

16. Het is niet duidelijk waarom voormelde artikelen, en het kb van 9 januari 2003 dat ze uitvoert, niet zouden volstaan voor het opsporingsonderzoek en het gerechtelijk onderzoek. Wat is de noodzaak van een bewaarplicht zoals voorzien door het voorontwerp van wet ? Wat is de impact van het voorontwerp van wet en ontwerp kb op de voormelde artikelen 46 bis en 88bis Sv., en het kb van 9 januari 2003 ? De ontwerpteksten geven hieromtrent geen uitsluitsel.

---

[7] VAN DEN WYNGAERT, C., Strafrecht, strafprocesrecht en internationaal strafrecht, in hoofdlijnen, Maklu, 2006, p. 979.

[8] VAN DEN WYNGAERT, C., o.c., p. 979-980.

D.4. ARTIKELSGEWIJZE BESPREKING VOORONTWERP VAN WET

Artikel 2

17. Artikel 2 vervangt het huidige artikel 126 WEC. §1 van artikel 2 van het voorontwerp van wet luidt als volgt :

'*Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de operatoren, alsook de aanbieders en doorverkopers bedoeld in artikel 9, §§5 en 6, de verkeers –en locatiegegevens en de gegevens voor identificatie van de eindgebruikers die door hen worden gegenereerd of verwerkt bij het aanbieden van elektronische communicatienetwerken –en diensten, met het oog op :*

a) het onderzoek, de vervolging en de beteugeling van strafbare feiten;
b) de beteugeling van kwaadwillige oproepen naar de nooddiensten;
c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk –of dienst.

18. Zoals reeds gesteld onder punt 9 supra, vermeldt artikel 2 van het voorontwerp van wet niet enkel de operatoren, maar eveneens de aanbieders en doorverkopers bedoeld in artikel 9, §§5 en 6 WEC. Hierdoor worden de entiteiten die voordien in de WEC door twee aparte bepalingen inzake de bewaring van gegevens werden geviseerd, in éénzelfde bepaling (het nieuwe artikel 126) gegroepeerd.

19. In het vroegere artikel 126 WEC was het voorgaande reeds voorzien voor een operator, nu komen er ook de aanbieders en doorverkopers bij die worden vermeld in artikel 9, §§5 en 6 WEC. Artikel 9, §7 voorzag dat zij eveneens gegevens moeten bewaren voor de doeleinden a) en b), doch niet voor het doeleinde c). Dit wordt nu wel voorzien. Onder aanbieders en doorverkopers moet bijvoorbeeld worden begrepen het interne netwerk van een bedrijvengroep. Deze worden evenwel niet geviseerd door de richtlijn 2006/24/EG, welke overeenkomstig artikel 3 enkel en alleen van toepassing is op aanbieders van openbare elektronische communicatiediensten of een openbaar communicatienetwerk bij het leveren van de betreffende communicatiediensten.

20. De reden voor het niet vermelden van de aanbieders en doorverkopers onder het huidige artikel 126 WEC, maar wel in artikel 9, §7 WEC kan worden teruggevonden in de verantwoording gegeven bij één van de amendementen[9] bij het wetsontwerp diverse bepalingen met betrekking tot de §§§ 5,6 en 7 : '*anderzijds blijft de nood om te voorzien in een samenwerking met de gerechtelijke autoriteiten. De samenwerkingsverplichting zoals die voorzien is voor de operatoren (met onder andere de verplichting om een contactpersoon voor de gerechtelijke autoriteiten aan te duiden die 7 dagen op 7 en 24 uur op 24 beschikbaar is) is in deze evenwel niet geschikt en daarom wordt de mogelijkheid gecreëerd om de nadere regels inzake het bewaren van gegevens en de samenwerking met de gerechtelijke autoriteiten in een uitvoeringsbesluit te omschrijven.'* Voormelde passage toont aan dat men de aanbieders en doorverkopers waarvan sprake in artikel 9, §§ 5 en 6 WEC niet zomaar kan gelijkstellen met een operator in de zin van artikel 2, 11° WEC. Zeker de zware procedure van samenwerking met de gerechtelijke autoriteiten zoals voorzien in het kb van 9 januari 2003 wilde men niet op éénzelfde wijze van toepassing verklaren op de aanbieders en doorverkopers. Het is dan ook vreemd dat zulks nu net wel gebeurt, door artikel 126 WEC (via het voorliggend artikel 2 van het voorontwerp van wet) niet enkel op de operatoren, doch eveneens op de aanbieders en doorverkopers van toepassing te maken. **Gezien het feit dat deze niet werden geviseerd door de Richtlijn 2006/24, de praktische implicaties vermeld onder punt 11, en gezien voormelde passage uit de verantwoording bij de wet van 20 juli 2006 houdende diverse bepalingen, lijkt het de Commissie aangewezen om de aanbieders en doorverkopers uit de toepassing van artikel 2 van het voorontwerp van wet te lichten, en in een andere bepaling onder te brengen. In het algemeen, met betrekking tot de voorliggende ontwerpen, dient opgemerkt dat men probeert onder het mom van de omzetting van de richtlijn veel meer op te leggen dan in de Richtlijn, bedoeld als maximumkader, wordt voorzien (zoals bijvoorbeeld naast de openbare ook de private netwerken te viseren, het opnemen van bijkomende gegevens, …).**

21. De Commissie merkt verder op dat een operator die gegevens verwerkt voor rekening van de Staat, zoals voor punt a) van artikel 2 van het voorontwerp van wet het geval is, handelt als zijn verwerker, zoals gedefinieerd in artikel 1, §5 WVP. De Staat zou in casu dan ook kunnen worden beschouwd als verantwoordelijke voor de verwerking. Het verdient hier dan ook aanbeveling om expliciet in artikel 2 te verduidelijken dat de operatoren als verantwoordelijke voor de verwerking in de zin van de WVP worden beschouwd.

---

[9] Zie Wetsontwerp houdende diverse bepalingen, 9 juni 2006, doc 51, 2518/007, p. 4.

22. De memorie van toelichting en het voorontwerp van wet verduidelijken dat het nieuwe artikel 126 van toepassing is onverminderd de bepalingen van de WVP. Daarom zijn de operatoren voortaan uitdrukkelijk verplicht (wat voorheen trouwens ook reeds het geval was) het geheel van de bepalingen van de WVP en haar uitvoeringsbesluit van 13 februari 2001 na te leven. Dit stemt overeen met de bepalingen van de richtlijn, die eveneens voorziet in een toepassing van de richtlijn 95/46/EG op de operatoren[10].

23. De memorie van toelichting stelt dat de operatoren en aanbieders de WVP moeten naleven, onder meer inzake de rechten van de betrokkenen : *'de persoon dient zijn gegevens te kunnen inzien en, indien nodig, deze te laten rechtzetten of verwijderen'* . Het recht op inzage zoals voorzien door artikel 10 WVP en het recht op verbetering (artikel 12) worden onverkort van toepassing geacht. Aanbieders of operatoren zouden desgevraagd een volledig overzicht moeten verstrekken van de bewaarde gegevens. Hieromtrent dient opgemerkt dat de abonnee van een aansluiting via het inzagerecht inzicht zou kunnen krijgen in het communicatiegedrag of de locatiegegevens van alle gebruikers over een langere periode. Daarbij valt te denken aan werknemers of gezinsleden, waaronder minderjarigen. De memorie van toelichting gaat ten onrechte aan deze problematiek voorbij. Bij vaste en mobiele telefonie zijn er oplossingen om de privacy te beschermen zoals het afschermen van nummers. Dit geldt echter niet voor internet. Voor het afleveren van e-mails worden immers geen gespecificeerde rekeningen verstrekt, en lijken er dus ook geen oplossingen voorhanden om de adresgegevens af te schermen.

24. Artikel 2 voorziet in de punten a), b) en c) de bijzondere finaliteiten waarvoor de verkeers, locatiegegevens en identificatiegegevens van de gebruikers kunnen worden aangewend. Hieromtrent kunnen de volgende bemerkingen gemaakt :

25. Het doeleinde voorzien onder punt a) : *onderzoek, vervolging en beteugeling van strafbare feiten* maakt een omzetting uit van de Richtlijn 2006/24, waarvan het doel het onderzoek, opsporen en vervolgen van **zware criminaliteit** betreft. Het voorontwerp van wet verwijst echter enkel naar strafbare feiten, hetgeen de facto inhoudt dat de bewaarde gegevens voor om het even welke strafbare inbreuk kunnen worden aangewend, zelfs overtredingen. Dit is niet bepaald in lijn met het uitgangspunt van de richtlijn en het principe van proportionaliteit, welke voorzien in de bewaring van bepaalde gegevens voor de strijd tegen de georganiseerde misdaad en het terrorisme, dus niet voor om het even welk misdrijf (cfr. supra, nrs. 4-6).

---

[10] Zie de overwegingen 15 en 16.

26. Naar analogie met bijvoorbeeld de BOM-wet[11] of artikel 90 ter Sv. inzake het aftappen van privé-communicatie, zou de wetgever in het huidige voorontwerp van wet kunnen voorzien in een strikte opsomming van de zware misdrijven voor het onderzoek, vervolging en beteugeling van dewelke de bewaarde gegevens kunnen worden aangewend. Minstens dient rekening te worden gehouden met de artikelen 46 bis en 88 bis Sv., welke momenteel respectievelijk voorzien in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot een telecommunicatiedienst en het opvragen door de onderzoeksrechter van locatiegegevens van een telecommunicatie. Op die manier zou tevens duidelijkheid worden verschaft over wie toegang heeft tot de bewaarde gegevens, voor de finaliteiten vermeld onder a). Hieromtrent voorzien de ontwerpen niets, behoudens voor de interne toegang bij de operatoren (Coördinatiecel Justitie). De Richtlijn bepaalt in artikel 4 inzake de toegang tot de gegevens dat de lidstaten bepalingen moeten aannemen om te waarborgen dat de gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving aan de bevoegde nationale autoriteiten worden verstrekt.

27. **Daarenboven zou elk ander gebruik van deze gegevens strafbaar moeten worden gesteld, en dient er tevens een nietigheidssanctie aan verbonden te worden.** Zie hieromtrent hetgeen wordt bepaald door artikel 13, 2. van de richtlijn : *'elke lidstaat neemt in het bijzonder de noodzakelijke maatregelen om ervoor te zorgen dat elke opzettelijke toegang tot of overbrenging van gegevens die overeenkomstig deze richtlijn worden bewaard die niet is toegestaan uit hoofde van krachtens deze richtlijn vastgestelde nationale uitvoeringsbepalingen, strafbaar is met sancties, met inbegrip van administratieve of strafrechtelijke sancties, die effectief, evenredig en afschrikkend zijn*.' Aangezien het BIPT bevoegd[12] is voor de controle op de naleving van de wet van 13 juni 2005 betreffende de elektronische communicatie en de bijbehorende uitvoeringsbesluiten, is voorzien in de mogelijkheid van alternatieve sancties, met name administratieve geldboetes, welke het IBPT overeenkomstig artikel 21 van de wet van 17 januari 2003 kan opleggen. De ontwerpen bepalen evenwel niet expliciet welke overheidsinstantie toezicht houdt op de veiligheid van de bewaarde gegevens, hetgeen nochtans wordt voorzien door artikel 9 van de Richtlijn. **Het verdient aanbeveling om de toezichthoudende autoriteiten op te nemen in het voorontwerp van wet evenals hun bevoegdheden en sancties, en er niet enkel naar te verwijzen in de memorie van toelichting.**

---

[11] Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere opsporingsmethoden.

[12] Zie artikel 14, wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post –en telecommunicatiesector.

28. Wat met het bewijs bekomen in strijd met de bepalingen van deze wet, bijvoorbeeld door personen die onbevoegd zijn om over deze informatie te beschikken ? Indien men zulk een bewijsmiddel wenst uit te sluiten, verdient het aanbeveling om zulks expliciet te voorzien in het voorontwerp van wet, en de **nietigheid van dergelijk bewijs op te leggen**. De Antigoonleer[13] van het Hof van Cassatie sluit onrechtmatig bekomen bewijs immers niet ipso facto uit.

29. Punt b) van artikel 2 van het voorontwerp van wet vermeldt 'de beteugeling van kwaadwillige oproepen naar de nooddiensten'. Punt c) voorziet in het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van personen die kwaadwillig gebruik hebben gemaakt van een elektronisch communicatienetwerk of –dienst. Deze punten vloeien niet voort uit de omzetting van de Richtlijn 2006/24, maar zijn voorzien in specifieke bepalingen. Overeenkomstig artikel 43bis § 3 7° van de wet van 21 maart 1991[14], is de ombudsdienst ermee belast van elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronische-communicatienetwerk of –dienst, het verzoek te onderzoeken om inlichtingen te krijgen over de identiteit en het adres van de gebruikers van elektronische-communicatienetwerken of –diensten die deze persoon hebben lastiggevallen, voorzover die gegevens beschikbaar zijn.

30. **De punten b) en c) maken geen deel uit van de omzetting van de richtlijn 2006/24. Aangezien de doeleinden van deze punten geen uitstaans hebben met 'ernstige criminaliteit', kan men zich de vraag stellen naar de opname in hetzelfde artikel, en de gelijkbehandeling van de punten a), b) en c) in het voorontwerp van wet en het ontwerp kb.** Er wordt namelijk geen enkel onderscheid voorzien naar de bewaarde gegevens waarop een beroep kan worden gedaan, noch naar de gebruiksduur van deze gegevens. Voor punt b) bijvoorbeeld lijkt toegang tot gegevens inzake emaildiensten niet noodzakelijk te zijn. Er wordt evenmin aangetoond waarom deze gegevens gedurende 24 maanden voor dit doeleinde zouden moeten toegankelijk zijn. **Omwille van het proportionaliteitsbeginsel en finaliteitsbeginsel, opgenomen in artikel 4 van de WVP, zou het voorontwerp van wet of minstens het ontwerp kb in een onderscheid tussen de voormelde punten moeten voorzien. Idealiter dienen de punten b) en c) in separate wetgeving te worden geregeld.**

---

[13] Zie hieromtrent onder meer het arrest Cass. 14 oktober 2003, T. Strafr. 2004, 129 met noot Ph. TRAEST.

[14] Wet betreffende de hervorming van sommige economische overheidsbedrijven.

31. Artikel 2, § 1 van het voorontwerp van wet voorziet verder : '*De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de krachtens het eerste lid te bewaren gegevens alsook de voorwaarden en termijn van bewaring van deze gegevens.'*

32. **De Commissie merkt op dat de keuze om de soorten gegevens niet in de wettekst zelf, maar in een koninklijk besluit op te nemen, moeilijk verenigbaar is met de keuze die in de richtlijn 2006/24 is gemaakt over de te bewaren gegevens.** Aanvankelijk was door de Europese Commissie namelijk voorgesteld om een lijst gegevens als bijlage bij de richtlijn te voegen, waarbij een versnelde besluitvormingsprocedure zou gelden voor aanpassingen aan die lijst. Het Europees Parlement heeft evenwel met grote meerderheid een amendement aangenomen van de rapporteur Alvaro, om de gegevens in de tekst van de richtlijn zelf op te nemen. Zo is tevens gekozen voor een zwaardere procedure van aanpassing van de soorten te bewaren gegevens, met volledig instemmingsrecht van het Europees Parlement. **Eenzelfde opmerking dient gemaakt voor wat betreft de termijn van bewaring van de gegevens, cfr. infra, nrs. 33 en volgenden**. Het voorgaande gaat des te meer op gezien het feit dat in de memorie van toelichting wordt verklaard dat het kader voor de bewaring van gegevens, zoals voorzien door de richtlijn, niet noodzakelijk aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voldoet. Vandaar dat men in het ontwerp kb bijkomende gegevens wenst op te nemen, welke niet worden voorzien door de richtlijn, zoals bankgegevens.

33. Omtrent de bewaarduur voorziet artikel 2, §1 van het voorontwerp van wet : '*De bewaringstermijn voor de gegevens bedoeld in het eerste lid mag niet korter zijn dan 6 maanden en niet langer dan 24 maanden.'* Artikel 6 van de richtlijn bepaalt dat de gegevens minimum 6 maanden en maximum 24 maanden kunnen worden bewaard, vanaf de datum van de communicatie. Voor wat de duur betreft, wordt in het ontwerp kb gekozen voor de door de richtlijn voorziene maximumduur van 24 maanden. Het verslag aan de Koning motiveert deze keuze summier door te stellen dat '*op basis van de praktijk die is waargenomen bij de verschillende gedecentraliseerde politiediensten of bij het federale parket inzake verzoeken om inlichtingen aan de operatoren en aan de aanbieders van netwerken of diensten voor elektronische communicatie, mag worden aangenomen dat een uniforme termijn van vierentwintig maanden voor de bewaring van de verschillende, in*

artikel 126 van de wet bedoelde soorten gegevens, het meest geschikte mechanisme vormt.[15]

34. De Richtlijn 2006/24 biedt in artikel 6 een bewaartermijn van ten minste 6 maanden en ten hoogste 2 jaar aan. De groep 29 heeft zich steeds op het standpunt gesteld dat het invoeren van een bewaarplicht voor de historische verkeersgegevens van alle burgers een zeer ingrijpende maatregel is waarvan de noodzaak onweerlegbaar dient te worden aangetoond[16]. In artikel 8 EVRM is het fundamentele recht van burgers verankerd op eerbiediging van hun persoonlijke levenssfeer. De overheid mag bij wet alleen inbreuk maken op dat recht voor zover dat in een democratische samenleving *noodzakelijk* is. De noodzaak stelt hoge eisen aan de proportionaliteit van elke specifieke maatregel die de persoonlijke levenssfeer van burgers inperkt. De algemene bepalingen uit de Richtlijn laten onverlet dat elke nationale implementatie zelfstandig getoetst moet worden aan artikel 8 EVRM en de bijbehorende jurisprudentie van het EHRM. Dat geldt nadrukkelijk voor de noodzaak van een bewaartermijn die langer is dan de termijn die noodzakelijk is voor de bedrijfsvoering van de aanbieders-operatoren.

35. De Commissie stelt vast dat het verslag aan de Koning nauwelijks uitlegt hoe de maximumtermijn van 24 maanden is bepaald. Men verwijst naar de praktijk bij de diverse politiediensten. De Commissie vraagt om de noodzaak van deze bewaartermijn duidelijker te rechtvaardigen en te onderbouwen. In navolging van de recente adviezen van de Groep 29 over dit onderwerp adviseert de Commissie daarom een geharmoniseerde minimale toepassing van de bepalingen van de Richtlijn, met een bewaartermijn die zo min mogelijk afwijkt van het oorspronkelijke doel waarvoor de gegevens door de aanbieders van communicatiediensten worden opgeslagen. Het is noodzakelijk om de lengte van een bewaarverplichting, die immers indruist tegen de algemene vernietigingsplicht uit Richtlijn 2002/58/EG, te onderbouwen met overtuigende argumenten. *"Zoals hierboven gezegd, moet de voor een algemene gegevensbewaarplicht aangevoerde rechtvaardigingsgrond met harde bewijzen aannemelijk kunnen worden gemaakt. Dat geldt ook voor de maximumtermijnen die in dat geval van toepassing zouden moeten zijn."*[17]

---

[15] Verslag aan de Koning, p. 1-2.

[16] Zie: advies 4/2001 over de ontwerp overeenkomst van de Raad van Europa inzake computercriminaliteit, 10/2001 over een evenwichtige benadering in de strijd tegen het terrorisme, 4/2005 over het voorstel van richtlijn en advies 3/2006 inzake richtlijn 2006/24/EG.

[17] Groep 29, advies 4/2005, p. 8.

36. Verder merkt de Commissie op dat de belangrijkste grondslag voor de Richtlijn, verwoord in artikel 1, het harmoniseren is van de nationale bepalingen in de lidstaten over bewaarplichten, teneinde te garanderen dat de gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit. Gezien de implementaties en voorstellen in andere EU lidstaten waarvan de Commissie kennis heeft, stelt ze vast dat van enige harmonisatie van de bewaartermijn vooralsnog weinig sprake is. Duitsland lijkt te kiezen voor een bewaartermijn van 6 maanden, net als Finland en Tsjechië. Ook Zweden, één van de vier initiatiefnemers van de totstandkoming van een Europese bewaarplicht, lijkt voor een minimumimplementatie te kiezen. Andere landen als Frankrijk, Denemarken en Spanje kiezen voor een bewaartermijn van 12 maanden. Nederland lijkt eveneens voor een termijn van 12 maanden te kiezen. Voor zover bekend opteert enkel Italië voor een bewaarduur van 24 maanden, en dan nog enkel voor telefoongegevens, de opslag van internetgegevens zou 6 maanden bedragen.

37. **Gelet op het voorgaande, meent de Commissie dat de actueel voorziene bewaarduur van 24 maanden verder onderbouwd dient te worden met meer overtuigende argumenten. Bij afwezigheid van zulk een rechtvaardiging, dient desgevallend een aanpassing van de voorziene termijn overwogen, zeker gelet op de gangbare bewaartermijnen in de meeste andere Europese landen, welke momenteel 6 tot 12 maanden bedragen.**

38. Artikel 2, §2 van het voorontwerp van wet voorziet dat de Koning, indien *uitzonderlijke omstandigheden* dat rechtvaardigen, na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een *onbeperkte periode,* een bewaringstermijn voor de gegevens kan vastleggen die langer is dan 24 maanden.

39. Vooreerst merkt de Commissie op dat de Nederlandse en Franse versie van het ontwerp kb verschillen, namelijk met betrekking tot de periode, welke in de Franse versie 'une période *limitée*' betreft, en in de Nederlandse 'een *onbeperkte* periode'. Overeenkomstig artikel 12 van de richtlijn dient deze verlenging in de tijd beperkt te zijn, en moet de Nederlandse versie dienovereenkomstig worden aangepast.

40. De Koning krijgt hierbij dus de mogelijkheid om een langere termijn dan het wettelijke maximum van 24 maanden te bepalen, *in uitzonderlijke omstandigheden*. Artikel 12 van de richtlijn verwoordt dit als volgt : '*Lidstaten met specifieke omstandigheden die een in de tijd beperkte verlenging van de in artikel 6 bedoelde bewaringsperiode rechtvaardigen, kunnen de noodzakelijke maatregelen treffen.'* Indien het gaat om een uitzondering, is het volgens de Commissie op zijn minst nodig om het basisprincipe van deze uitzondering formeel in de wet te regelen. Deze algemene regel kan nadien verder uitgewerkt worden in een koninklijk besluit, maar de grondslag zou in de wet moeten verankerd worden, wat hier niet het geval is : **de term 'uitzonderlijke omstandigheden' biedt niet voldoende rechtszekerheid, is uitermate vaag en is hierdoor te ruim interpreteerbaar.**

D.5. ANALYSE ONTWERP KB

D.5.1. Algemene bespreking ontwerp kb

41. De Commissie verwijst inzake de in het ontwerp kb voorziene bewaartermijn van 24 maanden naar de opmerkingen gedaan onder de nrs. 33 en volgenden. Zij herhaalt tevens dat de bewaarduur en soorten bewaarde gegevens bij voorkeur in de wet zouden moeten worden bepaald, en niet in het ontwerp kb, cfr. supra nr. 32.

42. De bewaarduur wordt in het ontwerp kb verschillend behandeld naargelang de aard van de gegevens : gegevens voor de identificatie van de abonnee en de gebruikte dienst worden bewaard gedurende de hele duur van het abonnement en voor een periode van 24 maanden vanaf de dag waarop het abonnement verstrijkt. De verkeers -en locatiegegevens, worden bewaard voor een periode van 24 maanden vanaf de dag waarop ze door de dienstenaanbieder zijn gegenereerd of verwerkt. Het voorgaande lijkt in te gaan tegen de tekst van de richtlijn, waar de bewaarduur ingaat vanaf de datum van de communicatie.

43. De memorie van toelichting[18] stelt dat de richtlijn een minimaal kader voorziet voor de bewaring van gegevens op het vlak van elektronische communicatie, hetwelk niet noodzakelijk voldoet aan de behoeften van de politiediensten en gerechtelijke autoriteiten voor het onderzoek, de vervolging en de beteugeling van strafbare feiten. Zo ontbreken volgens de memorie van toelichting in de door de richtlijn opgestelde lijst bepaalde gegevens die onmisbaar zijn voor identificatie van personen betrokken bij een relevante communicatie in het kader van een strafrechtelijk onderzoek, zoals bankgegevens. Merk op

[18] Mvt, p. 1-2.

dat de memorie stelt bijkomende gegevens nodig te hebben voor het strafrechtelijk onderzoek, maar deze gegevens eveneens openbaar maakt, of alleszins niet afsluit, voor onderzoeken door de Ombudsman of in het kader van de beteugeling van kwaadwillige oproepen naar de nooddiensten. Zoals hierboven onder de nrs. 22 en 23 reeds opgemerkt, dient verduidelijkt wie toegang heeft tot welke gegevens. In het licht van het proportionaliteitsbeginsel, kan men namelijk maar toegang hebben tot de gegevens welke men daadwerkelijk nodig heeft. In elk geval kan de Commissie zich niet vinden in de overweging van de memorie als zou de richtlijn een minimum kader voorzien : de richtlijn schrijft in artikel 5 gedetailleerd voor welke categorieën gegevens bewaard moeten worden. In overweging 21 bepaalt de richtlijn dat haar doel het onderzoeken, opsporen en vervolgen van zware criminaliteit uitmaakt, en zij niet verder gaat dan nodig is om deze doelstellingen te verwezenlijken. Volgens overweging 12 van de richtlijn moet de lijst van 'categorieën gegevens' als een maximum kader worden opgevat. Voor het bewaren van andere gegevens kunnen de lidstaten een beroep doen op artikel 15, eerste lid van richtlijn 2002/25/EG. **Wetgeving die op grond van dat artikel wordt uitgevaardigd, dient afzonderlijk te voldoen aan het vereiste van artikel 8 EVRM, namelijk dat ze in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.** De Commissie heeft een lijst opgevraagd bij de opstellers van het ontwerp met de extra –namelijk buiten hetgeen wordt voorzien door de richtlijn- te bewaren gegevens. Zulk een lijst kon haar vooralsnog evenwel niet worden overgemaakt, zodat de Commissie hiernavolgend -onder voorbehoud van misinterpretatie- zelf tracht na te gaan wat correspondeert met de richtlijn, en wat er buiten gaat. De Commissie heeft hierbij opgemerkt dat er voor elke categorie van gegevens in het ontwerp kb klaarblijkelijk meer wordt bewaard dan voorzien door de richtlijn, al dan niet met een motivering daaromtrent. De Commissie zal hiernavolgend in de artikelsgewijze bespreking hierop nader ingaan.

D.5.2. Artikelsgewijze bespreking van het ontwerp kb

ARTIKEL 1

44. Dit artikel definieert een aantal begrippen, waaronder 'Persoonsgegevens' : hieronder worden begrepen de naam en voornaam, het facturatie en het contactadres van de abonnee of de gebruiker. Er dient opgemerkt dat deze definitie niet overeenkomt met de definitie van 'persoonsgegeven' in artikel 1, §1 van de WVP, welke veel ruimer is. De Commissie gaat er dan ook vanuit dat het hier niet de bedoeling is om dezelfde definitie te hanteren als voorzien door de WVP.

45.

ARTIKEL 2

45. Artikel 2 betreft de gegevens die de operatoren voor vaste telefonie moeten bewaren, i.e. zij die een openbare vaste-telefoniedienst aanbieden. Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie op het ogenblik van een communicatie.

46. De eerste categorie bevat voornamelijk de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. **De Commissie merkt op dat enkel de elementen 1° en 2° (het aan de abonnee toegewezen nummer, en de persoonsgegevens van de abonnee) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 8°.** Deze uitbreiding wordt niet gemotiveerd, tenzij door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. Over element 6° stelt het verslag aan de koning dat *'deze gegevens kunnen uiterst belangrijk blijken te zijn om te bepalen tot welke operator de gerechtelijke autoriteiten zich eventueel moeten wenden om de inlichtingen te verkrijgen van voor of na een bepaalde periode*.' Voor wat punt 7, de bankgegevens, betreft, merkt de Commissie op dat deze gegevens door de onderzoekers bij de banken kunnen worden bekomen, aangezien de onderzoekers over de identiteitsgegevens beschikken. In hoeverre is het dan proportioneel om deze gegevens hier op te nemen ?

47. De verzameling van de elementen 3° tot en met 8° gaat verder dan de lijst zoals voorzien in artikel 5 van de richtlijn. Zoals hierboven reeds aangehaald, moet volgens overweging 12 van de richtlijn deze lijst als een maximum kader worden opgevat. Voor het bewaren van andere gegevens kunnen de lidstaten een beroep doen op artikel 15, eerste lid van richtlijn 2002/25/EG. Wetgeving die op grond van dat artikel wordt uitgevaardigd, dient afzonderlijk te voldoen aan het vereiste van artikel 8 EVRM, namelijk dat ze in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Het ontwerp kb voldoet hieraan vooralsnog niet.

48. De tweede categorie van gegevens zijn gegevens gegenereerd tijdens een communicatie. Hieromtrent heeft de Commissie geen opmerkingen.

ARTIKEL 3

49. Dit artikel betreft de gegevens die de operatoren voor mobiele telefonie moeten bewaren, i.e. de operatoren die een openbare mobiele telefonie dienst aanbieden. Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie op het ogenblik van een communicatie.

50. De eerste categorie bevat voornamelijk de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. **De Commissie merkt op dat enkel de elementen 1° en 2° (het aan de abonnee toegewezen nummer, en de persoonsgegevens van de abonnee) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 10°.** Deze uitbreiding wordt summier gemotiveerd, vooreerst door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. Over elementen 3° en 4° stelt het verslag aan de koning dat *'weten wanneer de kaart is gekocht en wanneer deze voor de eerste keer is gebruikt kan kostbare informatie opleveren voor de rechercheurs. … Door de inlichtingen over het opladen van krediet op een voorafbetaalde kaart te bewaren is het mogelijk de gebruikscapaciteit te kennen waarover de gebruiker beschikt, de wijze waarop hij heeft opgeladen, of de plaats waar de oplaadbeurt heeft plaatsgevonden. Dergelijke informatie valt buiten het bestek van de gegevens die normaal door de richtlijn worden beoogd, maar is werkelijk van belang in het kader van een onderzoek, waar dat kleine stukje informatie vaak de enige piste is waarover*

de politiediensten beschikken om een verdachte te proberen identificeren.' De Commissie volgt deze uitleg, maar meent omwille van de reeds onder de nrs. 43 en 47 genoemde opmerkingen dat zulks niet volstaat om verder te gaan dan hetgeen wordt voorzien door de richtlijn.

51. De tweede categorie van gegevens zijn gegevens gegenereerd tijdens een communicatie. Hieromtrent heeft de Commissie geen opmerkingen.

ARTIKEL 4

52. Dit artikel heeft betrekking op de aanbieders van internettoegang. Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie.

53. De eerste categorie bevat voornamelijk de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. **De Commissie merkt op dat enkel de elementen 1° en 2° (de identificatiecode van de abonnee, en de persoonsgegevens van de abonnee) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 8°.** Deze uitbreiding wordt summier gemotiveerd, door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. De Commissie neemt nota van deze uitleg, maar meent omwille van de reeds onder de nrs. 43 en 47 genoemde opmerkingen dat zulks niet volstaat om verder te gaan dan hetgeen wordt voorzien door de richtlijn.

54. De tweede categorie van gegevens zijn gegevens inzake het verkeer en de locatie. **De Commissie merkt op dat enkel de elementen 1° tot en met 4°, en 6° (maar volgens de richtlijn enkel bij de aanvang, niet bij het einde) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 5° en 7°.** Deze uitbreiding wordt niet gemotiveerd, en kan gelet op de hierboven reeds gemaakte opmerkingen dan ook niet worden gevolgd.

ARTIKEL 5

55. Artikel 5 heeft betrekking op de gegevens die moeten worden bewaard door de aanbieders van emaildiensten en door de aanbieders van internet telefoniediensten. Met de aanbieders van emaildiensten worden zowel SMTP mail bedoeld als webmail, zoals Hotmail, Yahoo, Gmail, … . Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie.

56. Voor wat betreft de webmail diensten zoals Hotmail en Gmail is het niet duidelijk op welke grond zij aan de bewaarplicht zijn onderworpen. De memorie van toelichting, noch het verslag aan de koning verschaft hier duidelijkheid over.

57. De eerste categorie bevat voornamelijk de gegevens die door de abonnee of gebruiker worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt, of wanneer hij van de aangeboden diensten gebruik maakt. **De Commissie merkt op dat enkel de elementen 1° en 2° (de identificatiecode van de abonnee of van de gebruiker, en de persoonsgegevens van de abonnee of de gebruiker) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 6°.** Deze uitbreiding wordt summier gemotiveerd, door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. De Commissie neemt nota van deze uitleg, maar meent omwille van de reeds onder de nrs. 43 en 47 genoemde opmerkingen dat zulks niet volstaat om verder te gaan dan hetgeen wordt voorzien door de richtlijn.

58. De tweede categorie van gegevens zijn gegevens gegenereerd tijdens een communicatie. Hieromtrent heeft de Commissie geen opmerkingen, behoudens aangaande punt 7 (wat betreft punt 7, voorziet de richtlijn enkel de opslag van de locatie bij de aanvang).

ARTIKEL 6

59. Het eerste lid van artikel 6 slaat op de operatoren die verschillende gecombineerde diensten aanbieden, zoals bijvoorbeeld het verzenden van mails via een gsm. De gegevens die zij in voormeld geval zullen moeten bewaren moeten overeenstemmen met zowel hetgeen werd voorzien door artikel 3 (mobiele telefonie) als artikel 5 (email) van het ontwerp kb. **De Commissie verwijst naar de hierboven gemaakte opmerkingen bij de artikelen 2 tot en met 5, welke *mutatis mutandis* op artikel 6 van toepassing zijn.**

60. Het tweede en derde lid betreft bepalingen inzake de tijdsaanduidingen, welke werden overgenomen uit het koninklijk besluit van 9 januari 2003. De Commissie heeft hieromtrent geen opmerkingen.

ARTIKEL 7

61. Artikel 7 stelt volgens het verslag aan de koning een aantal voorwaarden inzake bewaring vast die bedoeld zijn om de veiligheid van de gegevens te garanderen en ervoor te zorgen dat ze op gepaste wijze worden verwerkt door personeel dat daarvoor bevoegd is. De elementen 1°, 2°, en 4° werden rechtstreeks overgenomen uit de richtlijn 2006/24, artikel 7. Punt 1 voorziet in een gescheiden opslag voor de te bewaren gegevens, hetgeen overeenstemt met de aanbevelingen van de groep 29, welke voorzien in een decentrale, logisch gescheiden opslag van de specifiek voor opsporingsdoeleinden te bewaren gegevens. Er dient vanuit privacyoogpunt een duidelijke scheiding te zijn tussen de gegevens welke door de operatoren worden bewaard voor bedrijfsdoeleinden, en deze bewaard uit hoofde van de voorliggende ontwerpen. Het ontwerp kb blijft verder onder element 2° nogal vaag, door enkel te verwijzen naar 'passende technische en organisatorische maatregelen' en deze niet verder uit te werken. Hieromtrent verwijst de Commissie ter informatie naar de door haar opgestelde referentiemaatregelen welke volgens de Commissie, naargelang van geval tot geval, toepasbaar dienen te zijn op een verwerking van persoonsgegevens[19].

62. Element 3° legt de operator op om te garanderen dat enkel de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 toegang heeft tot de gegevens.

---

[19] Zie hieromtrent het document 'Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens' vanwege de Commissie voor de bescherming van de persoonlijke levenssfeer, te consulteren op haar website http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

63. **De Commissie merkt hieromtrent vooreerst op dat hierdoor enkel de toegang tot de gegevens bij de operatoren zelf wordt geregeld, i.e. intern, doch niet aan wie deze gegevens extern kunnen worden overgemaakt.** De coördinatiecel justitie is overeenkomstig artikel 2, §1 van voormeld kb : '*…Om aan de medewerkingsplicht te voldoen zoals opgelegd door artikel 46bis, §2, 88bis, §2 en 90quater, §2 van het wetboek van strafvordering, wordt er door iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst één of meerdere personen bij name aangeduid en belast met de taken die uit de medewerkingsplicht voortvloeien, hierna genoemd de 'Coördinatiecel Justitie'.* Zoals reeds aangegeven supra onder punten 26, 29 en 30, zou er duidelijk moeten worden voorzien aan wie welke gegevens kunnen worden overgemaakt door de Coördinatiecel Justitie. Overeenkomstig artikel 2, §1, c) van het voorontwerp van wet zou bijvoorbeeld ook de Ombudsman voor de telecommunicatie inzage moeten kunnen krijgen, hetgeen nu niet expliciet is voorzien. **Er dient duidelijk en limitatief te worden bepaald, bij voorkeur in het voorontwerp van wet, wie toegang heeft tot de bewaarde gegevens, tot welke gegevens in het bijzonder, en voor welke specifieke doeleinden.**

64. **Daarnaast dient herhaald dat deze Coördinatiecel door het kb van 9 januari 2003 enkel werd geïnstalleerd bij de operatoren, en niet bij de aanbieders en doorverkopers vermeld in artikel 9, §§5 en 6 WEC.** Is het de bedoeling dat de aanbieders en doorverkopers ook een dergelijke coördinatiecel in het leven roepen, die aan dezelfde bepalingen moet voldoen inzake 24/7 beschikbaarheid en dergelijke ? Zoals reeds opgemerkt supra onder punt 16 heeft de wetgever vroeger deze gelijkbehandeling van operatoren enerzijds en aanbieders en doorverkopers anderzijds uitgesloten door niet naar hen te verwijzen in de huidige versie van artikel 126 WEC, doch wel in artikel 9, §7 WEC, welke in een aparte regeling voor deze categorie zou voorzien.

65. **Verder is 'de garantie' van de operator dat enkel de coördinatiecel justitie toegang heeft niet voldoende, de niet-naleving van deze interne toegangsregel zou strafrechtelijk moeten worden gesanctioneerd.** Zie hieromtrent hetgeen wordt bepaald door artikel 13, 2. van de richtlijn : *'elke lidstaat neemt in het bijzonder de noodzakelijke maatregelen om ervoor te zorgen dat elke opzettelijke toegang tot of overbrenging van gegevens die overeenkomstig deze richtlijn worden bewaard die niet is toegestaan uit hoofde van krachtens deze richtlijn vastgestelde nationale uitvoeringsbepalingen, strafbaar is met sancties, met inbegrip van administratieve of strafrechtelijke sancties, die <u>effectief, evenredig en afschrikkend</u> zijn*.'

66. Tenslotte moet elke operator ervoor zorgen dat de gegevens aan het einde van de bewaringstermijn worden vernietigd, met uitzondering van de geraadpleegde en vastgelegde gegevens. Omtrent deze laatste gegevens wordt geen bewaarduur voorzien. Het zou evenwel logisch lijken dat indien de gegevens werden geraadpleegd in het kader van een gerechtelijk onderzoek, deze verder worden bewaard door de verantwoordelijke diensten voor zolang als nodig voor hun onderzoek, en kunnen worden vernietigd bij de operator. Indien de onderzoeksinstanties evenwel van oordeel waren dat de gegevens niet nuttig waren voor het onderzoek, is er geen noodzaak om de gegevens nog langer te laten bewaren door de operator na de voorziene bewaartermijn.

ARTIKELEN 8 EN 9

67. Hieromtrent heeft de commissie geen opmerkingen.

ARTIKEL 10

68. Dit artikel bepaalt dat het ontwerp kb ook van toepassing is op mislukte oproeppogingen. De richtlijn 2006/24 bepaalt in artikel 3, 2. dat zij geen vereisten bevat betreffende de bewaring van gegevens in verband met niet tot stand gekomen verbindingen, maar wel betreffende oproeppogingen zonder resultaat, hetgeen volgens de richtlijn een communicatie uitmaakt waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord[20].

69. De verwoording in artikel 10 sluit hier niet helemaal bij aan, waar zij stelt dat het besluit ook van toepassing is op oproepen die niet terechtgekomen zijn wegens een interventie van de netwerkbeheerder. Het ware aangewezen dit te herschrijven, bijvoorbeeld '*…ook van toepassing op oproepen die door het netwerkbeheer werden beantwoord*'.

[20] Zie artikel 2, f) Richtlijn 2006/24/EG.

ARTIKEL 11

70. Volgens het verslag aan de koning wijst artikel 11 binnen elke coördinatiecel Justitie een aangestelde voor de gegevensverwerking aan, zoals dat wordt toegestaan door artikel 17bis, tweede en derde lid, van de WVP. Artikel 11, derde lid is erop gericht de onafhankelijkheid van de aangestelde in zijn functie te garanderen.

71. De Commissie onderstreept dat de Koning het statuut van de aangestelden voor de gegevensbescherming nog niet heeft vastgesteld in toepassing van artikel 17bis van de WVP. Het zou dus voorbarig zijn vooruit te lopen op toekomstige bepalingen. Alle definities van controlefuncties, hetzij intern of niet, zouden dus rekening moeten houden met de Richtlijn 95/46/EG (overweging (49) en artikel 18). De hier bedoelde aangestelden voor de gegevensbescherming zouden in de praktijk een bevoorrechte gesprekspartner moeten zijn van de Commissie, hetgeen in het ontwerp kb wordt gestimuleerd door op te leggen om hun identificatie –en contactgegevens mee te delen aan de Commissie. Het is tevens aangewezen dat het ontwerp kb een grote zichtbaarheid verzekert voor hun adviezen en rapporten. In dit opzicht beveelt de Commissie aan dat het ontwerp kb zou aangepast worden opdat deze rapporten eveneens systematisch aan haar zouden meegedeeld worden.

72. De onafhankelijkheid van de aangestelden voor de gegevensbescherming is primordiaal. Het is evenwel belangrijk dat deze verzekerd wordt door gepaste maatregelen. De volgende maatregelen kunnen in het ontwerp kb aangenomen worden, bovenop deze die reeds vermeld zijn in artikel 11:

• Kennisgeving aan de Commissie van de aard van juridische band tussen deze aangestelden en de dienst waar zij hun functie van aangestelde zullen uitoefenen, alle elementen met betrekking tot de beroepskwalificaties in verband met de functie van aangestelde, maatregelen genomen door de verantwoordelijke voor de verwerking in functie van de door de aangestelde voor de bescherming van gegevens uit te voeren opdrachten;

• Verplichting om de aangestelden op een dusdanig niveau in de hiërarchie te plaatsen zodat zij over de mogelijkheid beschikken om rechtstreeks met het management/directiecomité te communiceren en hun opdracht rechtstreeks uit te oefenen bij de verantwoordelijke voor de verwerking;

73. Tenslotte dient nogmaals herhaald dat artikel 11, §2, 3° moet worden verduidelijkt, cfr. supra nr. 63, aangezien het ontwerp kb noch het voorontwerp van wet duidelijk stellen wie extern bij de coördinatiecel justitie toegang heeft tot de bewaarde gegevens.

ARTIKEL 12

74. Artikel 12 legt de betrokken operatoren de verplichting op om het instituut jaarlijks een aantal statistische inlichtingen mee te delen die bestemd zijn voor de EG Commissie. Vreemd genoeg legt artikel 12 dit enkel op aan de 'operator die een openbare telefoniedienst verstrekt'. Indien men ervoor kiest om het voorontwerp van wet en het ontwerp kb eveneens van toepassing te verklaren op de aanbieders en doorverkopers bedoeld in artikel 9, §§5 en 6 WEC, dienen zij eveneens in dit artikel te worden meegenomen. Het betreft overeenkomstig artikel 10 van de richtlijn ook niet enkel een 'telefoniedienst', doch wel een elektronische communicatiedienst of communicatienetwerk.

ARTIKELEN 13 EN 14

75. Hieromtrent heeft de commissie geen opmerkingen.

OM DEZE REDENEN,

Is de Commissie van oordeel dat

- gelet op het legaliteitsbeginsel, de essentiële elementen inzake de bewaring van gegevens in het voorontwerp van wet duidelijker dienen te worden bepaald. In dit opzicht zou de bewaarduur in het voorontwerp van wet moeten worden bepaald, en eveneens de te bewaren gegevens.
- de noodzaak voor het bewaren van bepaalde gegevens, die niet voorzien zijn in de richtlijn, dient gerechtvaardigd overeenkomstig de principes van artikel 8 EVRM.
- het voorontwerp van wet zou dienen te verduidelijken voor het onderzoek, de vervolging en de beteugeling van welke (zware) criminele feiten de bewaarde gegevens kunnen worden gebruikt.
- de bewaarduur van 24 maanden meer dient te worden gefundeerd en gerechtvaardigd, en desgevallend heroverwogen met het oog op de voorziene bewaartermijnen in de meeste andere Europese landen.

- de toepassing van het voorontwerp van wet en ontwerp kb op de aanbieders en doorverkopers voorzien in artikel 9, §§ 5 en 6 dient te worden herbekeken, en voor hen eventueel in een andere bepaling te voorzien.
- Het bewaren van de gegevens voor de doeleinden voorzien in artikel 2, §1, b) en c) (de kwaadwillige oproepen naar de nooddiensten en de ombudsdienst voor telecommunicatie) uit de toepassing van het voorontwerp van wet dienen gehaald, en hieromtrent in een separate regelgeving moet worden voorzien.
- uitzonderingen niet kunnen worden geregeld via een koninklijk besluit, doch dat minstens het basisprincipe van de uitzondering in de wet dient te worden geregeld. Het begrip 'uitzonderlijke omstandigheden' in artikel 2, §2 van het voorontwerp van wet is te vaag.
- de toewijzing van de personen of instanties die toegang hebben tot de bewaarde gegevens via de coördinatiecel justitie expliciet moet gebeuren in het voorontwerp van wet , waarbij tevens dient aangegeven wie toegang heeft tot welke gegevens.
- de niet naleving van de vereisten inzake toegang en gebruik van de verzamelde gegevens strafbaar dient gesteld.
- de toezichthoudende autoriteiten expliciet moeten worden aangeduid in het voorontwerp van wet , evenals hun bevoegdheden en sancties terzake.

Gelet op de in dit advies vermelde opmerkingen, brengt de Commissie voor de bescherming van de persoonlijke levenssfeer een *ongunstig* advies uit over de actuele inhoud van het voorontwerp van wet en ontwerp van koninklijk besluit.

Voor de Administrateur m.v.,
Het Afdelingshoofd ORM,

De Voorzitter,

(get.) Patrick Van Wouwe

(get.) Willem Debeuckelaere

ANNEXE 4

Réponse à l'avis n° 24/2008 du 2 juillet 2008 de la Commission de la protection de la vie privée

La présente note entend réagir à un certain nombre de remarques formulées dans l'avis n° 24/008 de la Commission de la protection de la vie privée concernant l'avant-projet de loi modifiant les articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques (LCE) et le projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données. La note suit la numérotation des points de l'avis.

Introduction: pourquoi la conservation de données de communications électroniques est nécessaire et pourquoi l'interception de communications électroniques ne peut être un instrument subsidiaire

La conservation des données d'identification d'utilisateurs et de certaines données de connexion de communications électroniques n'est pas neuve. En effet, les opérateurs conservent les données demandées à des fins de facturation ou de marketing, dans le cadre de la protection de leurs systèmes et dans le but de prévenir la fraude.

Dans le passé, il a dès lors été prévu de rendre le procureur du roi et le juge d'instruction compétents pour demander respectivement les données d'identification (art. 46*bis* du Code d'Instruction criminelle) et les données d'appel (art. 88*bis* du Code d'Instruction criminelle) relatives aux communications électroniques.

Du point de vue du respect de la vie privée, ces mesures d'investigation ont moins d'impact que l'interception du contenu des communications électroniques entre personnes. Pour certaines infractions, l'identification d'un auteur est suffisante pour pouvoir revenir ensuite aux méthodes d'investigation traditionnelles comme l'audition, la perquisition, *etc.*

Pour d'autres infractions, le juge d'instruction devra aller plus loin et ordonner l'interception du contenu des communications électroniques de certains inculpés. L'identification d'un service de communication utilisé par le criminel à l'aide des données à conserver est toutefois indispensable pour pouvoir déterminer précisément les services de communication qui doivent faire l'objet d'une interception. L'interception (art. 90*ter* du Code d'Instruction criminelle) est en outre une mesure d'instruction à ce point extrême que le juge d'instruction

BIJLAGE 4

Antwoord op het advies nr.24/2008 van 2 juli 2008 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer

Deze nota wenst in te gaan op een aantal opmerkingen in het advies nr. 24/2008 van 2 juli 2008 van de Commissie voor de bescherming van de persoonlijke levenssfeer over het voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (WEC), en het ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van de bewaring van die gegevens. In deze nota wordt de nummering van de paragrafen van het advies gevolgd.

Inleiding: waarom de bewaring van elektronische communicatiegegevens noodzakelijk is en de interceptie van elektronische communicatie geen subsidiair instrument kan zijn.

De bewaring van de identificatiegegevens van gebruikers en van bepaalde verbindingsgegevens uit elektronische communicaties is niets nieuws. De operatoren houden de gevraagde gegevens immers bij voor facturatiedoeleinden, voor marketing of binnen het kader van de beveiliging van hun systemen en om fraude te voorkomen.

In het verleden werd dan ook al voorzien dat de procureur des Konings en de onderzoeksrechter over de bevoegdheden beschikken om respectievelijk de identificatiegegevens (art. 46*bis* WSv) en de oproepgegevens (art. 88*bis* WSv) met betrekking tot elektronische communicaties op te vragen.

Deze onderzoeksmaatregelen zijn minder ingrijpend in de privacy dan de interceptie van de inhoud van de elektronische communicaties tussen personen. Voor bepaalde misdrijven is het identificeren van een dader voldoende om daarna terug te kunnen vallen op de traditionele onderzoeksmethodes zoals verhoor, huiszoeking, enz.

Voor andere misdrijven zal de onderzoeksrechter verder dienen te gaan en de interceptie van de inhoud van de elektronische communicaties van bepaalde verdachten bevelen. De identificatie van een door de crimineel gebruikte communicatiedienst aan de hand van de te bewaren gegevens is echter noodzakelijk om te kunnen bepalen welke communicatiediensten precies onder interceptie gezet moeten worden. Interceptie (art. 90*ter* WSv) is bovendien een zo vergaande onderzoeksmaatregel dat de onderzoeksrechter en in uitzonderlijke

et, dans des cas exceptionnels, le procureur du roi ne peut l'ordonner que pour un nombre limité d'infractions. C'est pourquoi l'interception en tant que mesure d'investigation ne peut être une alternative à l'obligation de conservation des opérateurs.

Pour certaines formes de criminalité grave (terrorisme, car-jacking et home-jacking, attaques à main armée, …), l'analyse des données de communication conservées permet, au départ d'une certaine communication, non seulement d'identifier le criminel concerné mais également de découvrir le réseau criminel sous-jacent. De même, ces données fournissent parfois la preuve de la présence d'un criminel à un certain endroit à un certain moment.

Toutefois, les communications électroniques auxquelles s'applique l'obligation de conservation ne sont pas seulement utilisées par des criminels pour communiquer entre eux. De plus en plus d'infractions sont en outre commises exclusivement par le biais de systèmes de communications électroniques, le criminel ne laissant plus que des traces électroniques. A cet égard, on peut penser à la diffusion de pornographie enfantine via Internet, à des escroqueries organisées via Internet ou, plus grave encore, à des attaques lancées contre des réseaux de communications électroniques mêmes. La conservation prévue de données de communications électroniques est la seule garantie pour les victimes de ces infractions de voir le criminel concerné recherché et poursuivi.

Pour une société devenue dans une très large mesure dépendante de ses systèmes de communication, il importe que l'ordre et le droit puissent également être maintenus dans ce monde virtuel. Elément essentiel, les données dont la conservation est demandée serviront également à rechercher et à établir les infractions au respect de la vie privée d'autrui, par exemple en cas de stalking, de hacking et d'espionnage via Internet.

1. Consultation du secteur par l'IBPT (point 12)

La Commission renvoie à la consultation par l'IBPT du secteur des opérateurs et des fournisseurs de services au sujet des projets de loi et d'arrêté royal. Cette consultation a entre-temps pris fin. Elle avait pour objectif de rassembler des remarques sur les textes et les frais d'exécution. L'enquête de l'IBPT ne révèle pas l'existence de difficultés techniques pour la fourniture des données demandées.

Certaines personnes interrogées se sont étonnées du fait que le projet d'arrêté royal ne se prononce pas sur les frais liés à l'exécution de ses dispositions ni sur une éventuelle compensation de ces frais.

gevallen de procureur des Konings ze alleen kan voorschrijven voor een beperkt aantal misdrijven. Om deze redenen kan de interceptie als onderzoeksmaatregel geen alternatief vormen voor de bewaringsverplichting door de operatoren.

Voor sommige vormen van zware criminaliteit (terrorisme, car- en homejacking, gewapende overvallen, ...) laat de analyse van de bewaarde communicatiegegevens toe om vertrekkend van een bepaalde communicatie niet enkel de betrokken crimineel te identificeren maar ook het achterliggende criminele netwerk te gaan blootleggen. Deze gegevens leveren soms ook bewijs van de aanwezigheid van een crimineel op een bepaalde locatie op een bepaald tijdstip.

De elektronische communicaties waarvoor de bewaringsverplichting wordt opgelegd, worden echter niet alleen gebruikt door criminelen om met elkaar te gaan communiceren. Meer en meer misdrijven worden bovendien uitsluitend gepleegd via de elektronische communicatiesystemen waardoor de crimineel enkel nog elektronische sporen achterlaat. Denken we hierbij maar aan de verspreiding van kinderpornografie via internet, de georganiseerde oplichtingen via internet of erger nog de aanvallen tegen elektronische communicatienetwerken zelf. De voorziene bewaring van gegevens uit de elektronische communicaties is de enige garantie voor slachtoffers van deze misdrijven dat de betrokken crimineel zal kunnen worden opgespoord en vervolgd.

Voor een maatschappij die in zeer hoge mate afhankelijk is geworden van haar communicatiesystemen, is het belangrijk dat ook orde en recht gehandhaafd kunnen worden in deze virtuele wereld. Niet in het minst zullen de gegevens waarvan de bewaring wordt gevraagd ook dienen om inbreuken op de privacy van anderen te kunnen onderzoeken en bewijzen. Bijvoorbeeld bij stalking of hacking en spionage via internet.

1. Raadpleging van de sector door het BIPT (§ 12)

De Commissie verwijst naar de raadpleging door het BIPT van de sector van operatoren en dienstenverstrekkers over de ontwerpen van wet en KB. Deze raadpleging is intussen afgesloten. Het doel van de raadpleging was opmerkingen te verzamelen over de teksten en de uitvoeringskosten. Uit de bevraging van het BIPT blijkt niet dat er technische bezwaren zouden bestaan om de gevraagde gegevens te leveren.

Sommige respondenten hebben zich erover verbaasd dat het ontwerp van KB niets zegt over de kosten voor de uitvoering van de bepalingen van het KB, noch over een eventuele compensatie van deze kosten.

Cela s'explique toutefois simplement:

Les indemnités par réquisition sur la base de l'article 46*bis* ou 88*bis* du Code d'Instruction criminelle figurent actuellement à l'annexe de l'arrêté royal portant exécution des articles 46*bis*, § 2, alinéa 1er, 88*bis,* § 2, alinéas 1er et 3, et 90*quater,* § 2, alinéa 3, du Code d'Instruction criminelle ainsi que de l'article 109*ter,* E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

Les indemnités par unité de temps et par type de demande sont par conséquent déjà prévues par cet arrêté royal dont la révision est en cours.

De même, la compensation des frais liés à l'exécution des dispositions de l'arrêté royal est déjà réglée dans le même arrêté royal qui contient un article 10 rédigé comme suit:

"Les frais d'investissement, d'exploitation et d'entretien pour les moyens techniques utilisés par les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications en exécution du présent arrêté sont à charge de ces opérateurs et de ces fournisseurs.

Les frais d'investissement, d'exploitation et d'entretien pour les moyens techniques utilisés par les autorités judiciaires en vue de l'exécution du présent arrêté sont à charge de la ministre de la Justice.

La seule indemnité que les opérateurs de réseaux de télécommunication et les fournisseurs de services de télécommunication obtiennent en échange de leur collaboration dans le cadre du présent arrêté figure à l'annexe du présent arrêté.".

En d'autres termes, les frais liés à l'extension de l'infrastructure nécessaire pour satisfaire aux exigences de cet arrêté royal étaient entièrement à charge des opérateurs. Ce doit également être le cas pour la rétention de données. Ça l'est d'ailleurs également dans d'autres pays. En Allemagne, il n'est pas non plus prévu de mécanisme de compensation des frais de conservation mais il existe une tarification générale pour la communication des données aux autorités compétentes. C'est également le cas au Portugal, en Espagne, en Suède, en Estonie et en Hongrie. Seules la Finlande et la France prévoient de compenser les frais de conservation par un financement public.

Dit valt echter eenvoudig te verklaren:

De vergoedingen per vordering op basis van artikel 46*bis* of 88*bis* van het Wetboek van Strafvordering zijn op dit moment opgenomen in de bijlage bij het Koninklijk Besluit van 9 januari 2003 tot uitvoering van de artikelen 46*bis*, § 2, eerste lid, 88*bis,* § 2, eerste en derde lid, en 90*quater*, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109*ter*, E, § 2 van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven.

Vergoedingen per tijdseenheid en per soort opvraging zijn dus al voorzien door dit KB, dat momenteel in herziening is.

Ook de compensatie van de kosten voor de uitvoering van de bepalingen van dat KB is al geregeld in hetzelfde KB van 9 januari 2003, waar een artikel 10 opgenomen is dat luidt als volgt:

"De investerings-, exploitatie-, en onderhoudskosten die verbonden zijn aan de technische middelen die in uitvoering van dit besluit aangewend worden door de operatoren van telecommunicatienetwerken en verstrekkers van telecommunicatiediensten zijn ten laste van deze operatoren van telecommunicatienetwerken en verstrekkers van telecommunicatiediensten.

De investerings-, exploitatie-, en onderhoudskosten die verbonden zijn aan de technische middelen die in uitvoering van dit besluit aangewend worden door de gerechtelijke autoriteiten zijn ten laste van de Minister van Justitie.

De enige tegemoetkoming die de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten ontvangen voor hun medewerking in het kader van dit besluit is vervat in de bijlage bij dit besluit."

M.a.w. de kosten verbonden aan de uitbreiding van de infrastructuur die nodig was om tegemoet te komen aan de vereisten van dit KB, waren volledig ten laste van de operatoren. Dit dient ook voor de dataretentie het geval te zijn. Dit is overigens ook in andere landen het geval. In Duitsland is het ook zo dat er niet voorzien is in een mechanisme voor de compensatie van de bewaringskosten, maar bestaat er een algemene tarifering voor de mededeling van de gegevens aan de bevoegde autoriteiten. Dit is ook het geval in Portugal, Spanje, Zweden, Estland en Hongarije. Slechts Finland en Frankrijk voorzien in compensatie van de bewaringskosten via overheidsfinanciering.

2. Fournisseurs et revendeurs prévus à l'article 9, §§ 5 et 6, de la LCE (points 9, 11 et 19 à 21 de l'avis)

La Commission précise à juste titre que les fournisseurs et les revendeurs prévus à l'article 9, §§ 5 et 6 de la LCE doivent être soustraits à l'application de l'article 2 de l'avant-projet de loi. Ils ne sont pas visés par la directive européenne 2006/24 d'une part ni par l'actuel article 126 de la LCE d'autre part. Cela s'explique par le fait que l'obligation de collaboration avec les autorités judiciaires ainsi que l'obligation de conservation des données ne peuvent pas être du même ordre pour ces fournisseurs et revendeurs que pour les "opérateurs" définis par la loi. La loi précise expressément qu'un arrêté d'exécution séparé doit être prévu pour les fournisseurs et revendeurs.

Conclusion: accord concernant la suppression de ces fournisseurs et revendeurs de la loi.

3. Pratique actuelle et rapport avec les articles 46*bis* et 88*bis* du Code d'Instruction criminelle et l'arrêté royal du 9 janvier 2003 (point 16 de l'avis)

L'article 46*bis* prévoit la demande de données d'identification concernant des services de télécommunication par le procureur du roi et l'article 88*bis*, le repérage et la localisation de communications par le juge d'instruction. Les deux articles prévoient une obligation de coopération des opérateurs. Cette obligation est réglée par l'arrêté royal du 9 janvier 2003, qui prévoit les délais et modalités de communication des données demandées conformément aux articles 46*bis* et 88*bis*.

C'est en vue de l'applicabilité pratique de ces articles et de l'arrêté royal du 9 janvier 2003 que les données d'identification, d'appel et de localisation visées doivent être conservées. A défaut d'obligation de conservation, les articles 46*bis* et 88*bis* ne seraient peut-être pas applicables parce que les opérateurs ne disposeraient peut-être pas des données demandées. D'où la nécessité de l'article 126 de la LCE et de l'arrêté royal relatif à la rétention de données sur lequel il est basé. Il n'a jamais été rédigé d'arrêté royal basé sur l'actuel article 126, § 2, de la LCE et devant déterminer les données à conserver ainsi que leur délai de conservation. Cette lacune est à présent comblée par l'avant-projet de loi et le projet d'arrêté royal.

2. De aanbieders en doorverkopers voorzien in artikel 9, §§ 5 en 6 van de WEC (advies § 9, 11, en 19 tot 21).

De Commissie stelt terecht dat de aanbieders en de doorverkopers voorzien in artikel 9, §§ 5 en 6 van de WEC uit de toepassing van artikel 2 van het voorontwerp van wet gelicht moeten worden. Zij worden enerzijds niet beoogd door de Europese richtlijn 2006/24, en anderzijds ook niet door het huidige artikel 126 van de WEC. Reden daarvoor is dat de samenwerkingsverplichting met de gerechtelijke autoriteiten evenals de verplichting gegevens te bewaren voor deze aanbieders en doorverkopers niet van dezelfde orde kan zijn als voor de "operatoren" zoals gedefinieerd door de wet. De wet voorziet uitdrukkelijk dat voor de aanbieders en doorverkopers een apart uitvoeringsbesluit voorzien dient te worden.

Conclusie: akkoord met het schrappen van deze aanbieders en doorverkopers uit de wet.

3. Huidige praktijk en de verhouding met de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering en het KB van 9 januari 2003 (advies § 16)

Artikel 46*bis* voorziet in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot telecommunicatiediensten, artikel 88*bis* voorziet in de opsporing en de lokalisatie van communicatie door de onderzoeksrechter. Beide artikelen voorzien in een medewerkingsplicht van de operatoren. Deze medewerkingsplicht wordt geregeld door het KB van 9 januari 2003, dat voorziet binnen welke termijn en volgens welke modaliteiten de gegevens meegedeeld moeten worden die opgevraagd worden overeenkomstig de artikelen 46*bis* en 88*bis*.

Het is met het oog op de praktische toepasbaarheid van deze artikelen en het KB van 9 januari 2003 dat de beoogde identificatiegegevens, oproepgegevens en locatiegegevens bewaard dienen te worden. Bij gebrek aan een bewaringsplicht, zouden de artikelen 46*bis* en 88*bis* misschien niet toepasbaar zijn omdat de operatoren eventueel niet over de gevraagde gegevens zouden beschikken. Vandaar de noodzaak aan artikel 126 van de WEC en het daarop gebaseerde KB dataretentie. Een KB op basis van het huidige artikel 126, § 2 WEC dat de te bewaren gegevens alsook de bewaartermijn had moeten bepalen is er nooit gekomen. Deze lacune wordt nu ingevuld door het voorontwerp van wet en het ontwerp van KB.

4. Droit de consultation et de rectification (point 23 de l'avis)

La Commission attire l'attention sur les droits des intéressés que leur confère la loi relative à la protection de la vie privée (LVP): le droit de consultation, de rectification et de suppression des données sont d'application dans leur intégralité.

Il convient de nuancer en ce sens que la loi impose aux opérateurs de conserver les données et qu'il n'est donc pas possible de faire supprimer les données de la personne concernée sur sa simple demande. Une comparaison peut être établie avec le casier judiciaire: le condamné ne peut pas demander tout simplement la suppression de ses données parce que la loi impose la conservation de certaines données sur le casier judiciaire. L'article 12, § 1er, alinéa 5, de la loi relative à la protection de la vie privée précise d'ailleurs que la personne concernée ne peut obtenir la suppression de ses données que si, compte tenu du but du traitement, il s'agit de données incomplètes ou non pertinentes ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui ont été conservée au-delà de la période autorisée.

En ce qui concerne le droit de consultation et de rectification, l'opérateur doit veiller à ce que, conformément à la loi relative à la protection de la vie privée, la personne concernée ne puisse consulter que ses propres données personnelles. Il devra pour ce faire prendre les mesures nécessaires de sorte que les données d'autres personnes soient occultées lors de l'exercice du droit de consultation. Cela implique par exemple qu'un employeur-abonné ne peut sans raison avoir accès aux données de communication des personnes qu'il emploie, même s'il est abonné aux numéros utilisés par celles-ci.

5. Recherche, poursuite et répression d'infractions pénales - criminalité grave (points 25 et 26 de l'avis)

La Commission de la protection de la vie privée estime que la finalité prévue à l'article 126, § 1er, a), en projet va au-delà de ce que prévoit la directive européenne parce que la rétention de données ne se limite pas à la recherche, à la poursuite et à la répression d'infractions "graves". Elle en conclut que les données conservées peuvent être utilisées pour n'importe quelle infraction, y compris des contraventions (voir avis de la Commission, p. 10).

Cette affirmation s'appuie sur une compréhension erronée de la réglementation relative à la rétention de données et des articles du Code d'Instruction criminelle en la matière.

4. Recht op inzage en verbetering (advies, § 23)

De commissie wijst op de rechten van de betrokkenen die door de WVP geboden worden: het recht op inzage, verbetering en verwijdering van de gegevens zijn onverkort van toepassing.

Dit dient genuanceerd te worden in die zin dat de wet de operatoren verplicht om de gegevens te bewaren en het is dus niet zomaar mogelijk is om op eenvoudig verzoek van de betrokkene zijn gegevens te doen verwijderen. De vergelijking kan gemaakt worden met het strafregister, waarbij veroordeelde personen ook niet zomaar kunnen vragen hun gegevens te schrappen, omwille van het feit dat de wet oplegt dat bepaalde gegevens in het strafregister dienen bewaard te worden. Overigens bepaalt artikel 12, § 1, 5° van de Privacywet dat de betrokkene de verwijdering van zijn gegevens slechts kan verkrijgen indien de gegevens, gelet op het doel van de verwerking, "onvolledig of niet ter zake dienend zijn, of waarvan de registratie, de mededeling of de bewaring verboden zijn, of die na verloop van de toegestane duur zijn bewaard".

Wat betreft het recht op inzage en verbetering, dient de operator ervoor te zorgen dat de betrokken persoon, conform de Privacywet, slechts zijn eigen persoonlijke gegevens kan inkijken. De operator zal daartoe de nodige maatregelen moeten nemen zodat gegevens van andere personen afgeschermd worden bij de uitoefening van het recht op inzage. Dit houdt in dat bv. een werkgever-abonnee niet zomaar toegang kan krijgen tot de communicatiegegevens van zijn werknemers, ook al is de werkgever de geabonneerde op de nummers gebruikt door zijn werknemers.

5. Onderzoek, opsporing en vervolging van strafbare feiten – zware criminaliteit (advies, § 25-26)

De commissie voor de bescherming van de persoonlijke levenssfeer is van mening dat het doeleinde voorzien in het ontwerpartikel 126, § 1, punt a) verder gaat dan wat in de Europese richtlijn voorzien is, omdat de dataretentie niet beperkt is tot het onderzoek, opsporing en vervolging van "zware" strafbare feiten. Ze trekt daar de conclusie uit dat de bewaarde gegevens voor om het even welk strafbaar feit kan worden gebruikt, zelfs voor overtredingen (zie advies commissie, p. 10).

Dit berust op een verkeerd begrip van de regeling betreffende dataretentie en de daarmee samenhangende artikelen in het Wetboek van Strafvordering.

Les données doivent en effet être conservées aux fins d'enquêtes pénales futures. Dans la plupart des cas, aucune enquête n'est encore en cours au moment où s'effectue la conservation des données, et si tel devait être le cas, l'opérateur n'en a en principe pas connaissance. Il est impossible pour l'opérateur d'opérer une sélection des données à conserver sur la base d'un critère tel que "criminalité grave". En d'autres termes, toutes les données énumérées dans l'arrêté royal doivent être conservées étant donné que les faits pour lesquelles elles pourront éventuellement être utilisées ne sont pas encore connus.

Il en va tout autrement pour l'accès aux données conservées. Celui-ci est réglé par les articles 46*bis* et 88*bis* du Code d'Instruction criminelle.

L'article 46*bis* prévoit la demande des données d'identification relatives aux services de télécommunication par le procureur du roi et l'article 88*bis*, le repérage et la localisation de communications par le juge d'instruction. C'est en vue de l'applicabilité pratique de ces articles que les données d'identification, d'appel et de localisation doivent être conservées. Les deux articles prévoient une obligation de coopération des opérateurs. Pour disposer des données demandées, les opérateurs doivent les conserver.

Les deux articles prévoient également des conditions telles que la subsidiarité et la proportionnalité de la mesure. L'article 46*bis* règle une compétence du procureur du roi, l'article 88*bis*, une compétence du juge d'instruction. Dans les deux cas, les mesures doivent être motivées par écrit. Il existe donc des garanties suffisantes empêchant n'importe qui d'avoir accès aux données conservées pour n'importe quelle raison (ou infraction).

Enfin, si les deux articles ne prévoient pas de liste d'infractions, ils incorporent toutefois un certain seuil étant donné qu'ils limitent les mesures aux crimes et délits. La subsidiarité et la proportionnalité sont donc définies d'une autre manière. C'est en soi déjà une raison suffisante pour ne pas utiliser la terminologie infractions "graves". Une énumération exhaustive des infractions graves ne semble dès lors ni nécessaire ni indiquée. En effet, compte tenu des diverses dispositions pénales particulières, une telle énumération n'est pas réalisable d'un point de vue pratique. En outre, tout ajout d'une infraction nécessiterait une modification de la loi.

Toutefois, pour répondre à la remarque de la Commission, et afin que l'explication ci-dessus transparaisse plus clairement dans l'avant-projet de loi, il

De gegevens dienen immers bewaard te worden met het oog op toekomstige strafrechtelijke onderzoeken. Op het moment van de bewaring van de gegevens is er, in de meeste gevallen, nog geen onderzoek aan de gang, en indien dit wel zo zou zijn dan is in principe de operator daar niet van op de hoogte. De operator kan onmogelijk een selectie maken van de te bewaren gegevens aan de hand een criterium als "zware criminaliteit". M.a.w. alle gegevens opgesomd in het KB dienen bewaard te worden, omdat men nog niet weet voor welke feiten die eventueel gebruikt zullen worden.

Iets geheel anders is de toegang tot de bewaarde gegevens. Dit wordt geregeld door de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering.

Artikel 46*bis* voorziet in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot telecommunicatiediensten, artikel 88*bis* voorziet in de opsporing en de lokalisatie van communicatie door de onderzoeksrechter. Het is met het oog op de praktische toepasbaarheid van deze artikelen dat de beoogde identificatiegegevens, oproepgegevens en locatiegegevens bewaard dienen te worden. Beide artikelen voorzien in een medewerkingsplicht van de operatoren. Opdat de operatoren over de gevraagde gegevens zouden beschikken, dienen zij die te bewaren.

Beide artikelen voorzien ook in voorwaarden zoals subsidiariteit en proportionaliteit van de maatregel. Artikel 46*bis* is een bevoegdheid van de procureur des Konings, artikel 88*bis* van de onderzoeksrechter. In beide gevallen moeten de maatregelen schriftelijk gemotiveerd worden. Er zijn dus voldoende garanties dat niet om het even wie toegang kan hebben tot de bewaarde gegevens voor om het even welke reden (of misdrijf).

Tot slot, beide artikelen voorzien niet in een lijst van misdrijven, doch er is wel een zekere drempel ingebouwd doordat deze artikelen de maatregelen beperkt tot wanbedrijven en misdaden. De subsidiariteit en de proportionaliteit worden dus op een andere manier gedefinieerd. Dat op zich is al voldoende reden om de terminologie "zware" strafbare feiten niet te hanteren. Een exhaustieve opsomming van de zware misdrijven lijkt dan ook niet nodig en ook niet aangewezen. Een dergelijke opsomming is immers, gelet op de diverse bijzondere strafbepalingen praktisch niet haalbaar. Bovendien zou telkens een wetswijziging nodig zijn indien een misdrijf zou moeten worden toegevoegd.

Niettemin, om tegemoet te komen aan de opmerking van de Commissie, en om bovenstaande uitleg duidelijker tot uiting te laten komen in het voorontwerp van wet,

sera renvoyé explicitement aux articles 46*bis* et 88*bis* du Code d'Instruction criminelle dans l'article 3, § 1er, a), de l'avant-projet. Ainsi, il sera clair que ces articles règlent l'accès aux données.

6. Dispositions pénales et autorité de contrôle (points 27 et 65 de l'avis)

L'exposé des motifs renvoie déjà à des dispositions existantes qui punissent l'usage abusif des données. Outre les dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée et de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, il peut encore être signalé qu'un certain nombre d'articles du Code pénal peuvent également être d'application en la matière:

- les articles 259*bis* et 314*bis* sanctionnent les écoutes, la prise de connaissance et l'enregistrement de communications privées;
- l'article 210*bis* sanctionne le faux en informatique;

- l'article 504*quater* sanctionne la fraude informatique;

- enfin, les articles 550*bis* et 550*ter* traitent des infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes.

Outre ces infractions informatiques spécifiques, certaines dispositions générales du Code pénal peuvent également s'appliquer à un environnement informatique. Pensons à des formes d'abus de confiance, d'escroquerie ou de fraude.

Toutefois, compte tenu du caractère sensible de la question et de l'atteinte à la vie privée que peut constituer la rétention de données, il peut être donné suite à la suggestion de la Commission de faire figurer dans l'avant-projet de loi une incrimination supplémentaire visant plus précisément à punir l'utilisation des données conservées à d'autres fins que celles prévues par la loi.

Les autorités de contrôle (l'IBPT, la Commission de la protection de la vie privée, la Justice, le gestionnaire de la cellule de coordination) sont mentionnées explicitement dans l'exposé des motifs.

zal in artikel 2 van het voorontwerp in doeleinde a) een expliciete verwijzing opgenomen worden naar de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering. Zo wordt duidelijk dat de toegang tot de gegevens in die artikelen geregeld wordt.

6. Strafbepalingen en toezichthoudende autoriteit (advies, § 27 en § 65)

De memorie van toelichting verwijst al naar bestaande bepalingen die misbruik van de gegevens strafbaar stellen. Naast de bepalingen van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer en van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, kan er ook nog op gewezen worden dat een aantal artikelen van het Strafwetboek hier ook van toepassing kunnen zijn:

- de artikelen 259*bis* en 314*bis* stellen het afluisteren, kennisnemen en opnemen van privécommunicatie strafbaar;
- artikel 210*bis* stelt de valsheid in informatica strafbaar;
- artikel 504*quater* stelt het informaticabedrog strafbaar;
- de artikelen 550*bis* en 550*ter* tenslotte betreffen de misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen.

Naast deze specifieke informaticamisdrijven kunnen ook een aantal algemene bepalingen van het Strafwetboek van toepassing zijn op een informaticaomgeving. Gedacht wordt aan vormen van misbruik van vertrouwen, oplichting, of bedrog.

Gezien echter de gevoeligheid en de aantasting van het privéleven van de dataretentie, kan ingegaan worden op de suggestie van de Commissie om een extra strafbaarstelling in het voorontwerp van wet op te nemen, die meer bepaald gericht is op het strafbaar stellen van de aanwending van de bewaarde gegevens voor andere dan de wettelijk voorziene doeleinden.

In de memorie van toelichting worden de toezichthoudende autoriteiten (het BIPT, de privacycommissie, justitie, de beheerder van de coördinatiecel) expliciet vermeld.

7. Sanction de nullité (point 28 de l'avis)

La présente loi ne règle pas l'obtention de la preuve. A cet égard, les articles 46*bis* et 88*bis* du Code d'Instruction criminelle sont d'application. Aucun des deux articles ne prévoit de sanction de nullité. Cela signifie que les règles générales en matière d'action publique, y compris la doctrine d'Antigone de la Cour de cassation, sont d'application.

Il serait en outre illogique de prévoir soudainement dans cet avant-projet de loi, qui ne pose que le principe de la rétention des données, une sanction de nullité pour l'obtention irrégulière de preuve.

8. Appels d'urgence et service de médiation (points 29 et 30 de l'avis)

Les points b) et c) de l'article 3 de l'avant-projet de loi figuraient déjà dans l'article 126 initial. L'avant-projet n'y déroge donc pas.

L'avant-projet de loi a pour but de régler la conservation des données par les opérateurs pour trois finalités. Cette approche a pour avantage que les opérateurs savent précisément quelles données ils doivent conserver et qu'ils ne doivent pas consulter différents textes de loi pour vérifier quelles sont leurs obligations en matière de rétention de données. En ce sens, il est logique que les finalités b) "la répression d'appels malveillants vers les services d'urgence" et c) "la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques" figurent également dans l'avant-projet de loi, d'autant que ces finalités sont contenues dans l'actuel article 126 de la LCE. La conservation en fonction des trois finalités ne doit donc pas être réglée dans des textes de loi distincts.

On ne peut évidemment pas demander aux opérateurs d'établir eux-mêmes une distinction en ce qui concerne les données à conserver et le délai de conservation en fonction de l'une des trois finalités possibles pour lesquelles les données peuvent être demandées. S'il faut à chaque fois associer aux trois finalités différentes un délai de conservation différent, cela impliquera concrètement pour l'opérateur que le délai de conservation pour la finalité à laquelle est associé le délai de conservation le plus long sera déterminant. En effet, l'opérateur ne peut pas "prévoir" la finalité pour laquelle l'accès sera demandé et ne peut donc savoir à l'avance s'il peut ou non supprimer plus tôt les données. Par conséquent, il devra tenir compte du délai de conservation le plus long pour pouvoir accéder à la

7. Nietigheidssanctie (advies, § 28)

Het verkrijgen van bewijs wordt niet geregeld door deze wet, daarvoor zijn de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering van toepassing. Geen van beide artikelen voorziet in een nietigheidssanctie. Dat wil zeggen dat de algemene regels van strafvordering, inclusief de Antigoonleer van het Hof van Cassatie, van toepassing zijn.

Het zou bovendien ook onlogisch zijn om in dit voorontwerp van wet, dat enkel het principe van de dataretentie poneert, plots in een nietigheidssanctie te voorzien voor onrechtmatig bekomen bewijs.

8. Noodoproepen en de Ombudsdienst (advies, § 29-30)

De punten b) en c) van artikel 2 van het voorontwerp van wet stonden al in het oorspronkelijke artikel 126. Het voorontwerp wijkt daar dus niet van af.

Het voorontwerp van wet strekt ertoe de bewaring van de gegevens door de operatoren te regelen voor drie doeleinden. Het voordeel van deze benadering is dat de operatoren duidelijkheid hebben welke gegevens zij dienen te bewaren en geen verschillende wetteksten dienen te raadplegen om na te gaan welke verplichtingen zij hebben inzake dataretentie. In die zin is het logisch dat ook de doeleinden b) "de beteugeling van kwaadwillige oproepen naar de nooddiensten" en c) "onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van personen die kwaadwillig gebruik hebben gemaakt van een elektronisch communicatienetwerk of –dienst" worden opgenomen in het voorontwerp van wet, temeer daar ook het huidige artikel 126 WEC deze doeleinden bevat. De bewaring in functie van de drie doeleinden dient dus niet in afzonderlijke wetteksten te worden geregeld.

Uiteraard kunnen de operatoren niet gevraagd worden om zelf een onderscheid te maken in de te bewaren gegevens en de bewaartermijn in functie van één van de drie mogelijke doeleinden waarvoor de gegevens kunnen worden opgevraagd. Indien aan de drie verschillende doeleinden telkens een andere bewaartermijn moet worden verbonden, zal *in concreto* voor de operator de bewaartermijn voor het doeleinde waaraan de langste bewaartermijn wordt gekoppeld doorslaggevend zijn. De operator kan immers niet "voorspellen" voor welk doeleinde toegang zal worden gevraagd en kan dus op voorhand niet weten of hij de gegevens al dan niet eerder mag wissen. Bijgevolg zal hij moeten rekening houden met de langst mogelijke bewaartermijn om gunstig gevolg te kunnen geven aan een mogelijke opvraging

demande éventuelle des données nécessaires. Il en est de même pour les données à conserver - l'opérateur devra conserver le plus grand nombre de données possible. Le délai de conservation est un élément important pour l'opérateur en ce sens que face à une demande concrète qu'il recevra, il devra déterminer si le délai dans lequel les données peuvent être demandées n'a pas encore expiré.

Il faut une fois de plus souligner que l'avant-projet de loi ne règle donc pas l'accès aux données mais prescrit la conservation des données pour trois finalités bien précises. L'article 126 ne donne aucune base légale à qui que ce soit pour obtenir l'accès à ces données, ni aux autorités, ni au Service de Médiation, ni aux services d'urgence. Une base légale spécifique doit exister pour l'accès aux données. Au niveau des autorités judiciaires, cela est le cas dans les articles 46*bis* et 88*bis* du Code d'Instruction criminelle. L'article 43*bis* § 3, 7° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques prévoit une base légale spécifique pour le Service de Médiation. Enfin, pour les services d'urgence, l'article 107 de la loi relative aux communications électroniques s'applique.

Pour clarifier cet aspect, ces bases légales spécifiques peuvent être reprises dans les trois finalités énumérées dans l'article 126. C'est donc à ce niveau que des restrictions sont imposées dans le domaine de l'accès aux données conservées.

9. Pourquoi dans l'arrêté royal et non dans le texte même de la loi (point 32 de l'avis)

La directive européenne 2006/24/CE fixe le cadre général pour la conservation des données relatives aux communications électroniques. Seules quatre catégories de services de communications électroniques sont visées:

- téléphonie fixe;
- téléphonie mobile;
- accès à l'Internet;
- courrier électronique (e-mail) et téléphonie par Internet.

La technologie de la communication et les protocoles techniques qui régissent ces communications électroniques évoluent rapidement - essentiellement en ce qui concerne les formes de téléphonie par Internet. Pour que le cadre légal soit un instrument efficace de lutte contre la criminalité, il est indispensable qu'il puisse

van de noodzakelijke gegevens. Hetzelfde geldt voor de te bewaren gegevens – de operator zal het ruimst aantal gegevens moeten bewaren. De bewaartermijn is voor de operator van belang in die zin dat in functie van een concrete bevraging die hij ontvangt, hij zal moeten bepalen of de termijn waarbinnen de gegevens kunnen worden opgevraagd nog niet is verstreken.

Er dient nog eens benadrukt te worden dat het voorontwerp van wet dus niet de toegang tot de gegevens regelt, maar wel de bewaring van gegevens voorschrijft voor drie welbepaalde doeleinden. Artikel 126 geeft geen enkele wettelijke basis aan wie dan ook om toegang te krijgen tot deze gegevens, noch aan de gerechtelijke overheden, noch aan de Ombudsdienst, noch aan de nooddiensten. Voor de toegang tot de gegevens dient een specifieke wettelijke basis te bestaan. Op het niveau van de gerechtelijke overheden is dit het geval in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering. Voor de Ombudsdienst is een specifieke wettelijke basis voor de toegang voorzien in artikel 43*bis,* § 3, 7° van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Voor de nooddiensten tenslotte geldt artikel 107 van de wet betreffende de elektronische communicatie.

Om dit duidelijk te maken kunnen deze specifieke wettelijke basissen opgenomen worden in de drie doeleinden die opgesomd staan in artikel 126. Het is dus op dit niveau dat beperkingen worden opgelegd op het gebied van de toegang tot de bewaarde gegevens.

9. Waarom in KB en niet in de wettekst zelf (advies, § 32)

De Europese richtlijn 2006/24/CE legt het algemene kader voor de gegevensbewaring betreffende elektronische communicatie vast. Slechts vier categorieën van elektronische-communicatiediensten worden geviseerd:

- Vaste telefonie;
- Mobiele telefonie;
- Internettoegang;
- Elektronisch berichtenverkeer (e-mail) en telefonie over internet.

De communicatietechnologie en de technische protocollen die deze elektronische communicatie regelen, evolueren snel – voornamelijk de vormen van telefonie over internet. Opdat het wettelijke kader een effectief instrument voor de criminaliteitsbestrijding zou zijn, is het noodzakelijk dat dit kader de evolutie van de

suivre l'évolution des protocoles technologiques de la nouvelle téléphonie (ou des nouvelles formes de courrier électronique).

D'une part, travailler avec un arrêté royal permet une mise à jour plus rapide du cadre légal que par le biais d'une procédure législative plus lourde. D'autre part, il est clair également que les possibilités pour le roi de fixer cette liste des données à conserver restent limitées par les principes et aux services déterminés par la directive européenne et la loi relative aux communications électroniques.

En outre, cette façon de procéder ne déroge pas non plus à la volonté et à la méthode de travail du législateur qui dès 2000 établissait les principes et prescrivait que les données à conserver ainsi que les modalités de cette conservation devraient figurer dans un arrêté royal.

Ce principe était déjà clairement défini à l'article 14 de la loi du 28 novembre 2000 relative à la criminalité informatique. Il a à nouveau été confirmé à l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques venu remplacer l'article précédent.

Le travail législatif étant en cours au niveau européen depuis 2002, nous avons attendu que l'UE ait finalisé ses travaux pour élaborer l'arrêté royal. La transposition de la directive européenne donne en effet un cadre précis à l'exécution effective des dispositions légales existantes. Par conséquent, la transposition via un arrêté royal est tout à fait conforme à la volonté du législateur.

10. Délai de conservation (points 33 à 37 de l'avis)

Le délai minimum de six mois demandé par une majorité des parties qui ont réagi à la consultation réalisée par l'IBPT ne répond pas du tout aux besoins sur le terrain.

Depuis des années, un délai de conservation des données de communication de 12 mois a été arrêté pour la téléphonie fixe et la téléphonie mobile. Mais même ce délai de conservation semble dans de nombreux cas insuffisant. Dans des dossiers importants principalement, des investigations sont menées sur l'utilisation de la téléphonie. Toutefois, compte tenu de la complexité de ces dossiers, le délai d'un an s'avère souvent trop court.

technologische protocollen van de nieuwe telefonie (of e-mailvormen) kan volgen.

Enerzijds laat het werken met een KB een snellere "update" van het wettelijke kader toe dan dat dit zou gebeuren via de zwaardere wetgevende procedure. Anderzijds is het echter ook duidelijk dat de mogelijkheden van de Koning om deze lijst van te bewaren gegevens vast te leggen, afgebakend blijven door de principes en voor de diensten die zijn omschreven door de Europese richtlijn en door de wet op de elektronische communicatie.

Deze werkwijze wijkt bovendien ook niet af van de wil en de werkwijze van de wetgever die al in 2000 de principes vastlegde en voorschreef dat de te bewaren gegevens en de modaliteiten van deze bewaring zouden worden zouden worden opgenomen in een Koninklijk besluit.

Dit principe was al duidelijk beschreven in artikel 14 van de wet op de informaticacriminaliteit van 28 november 2000. Het werd nog eens bevestigd in artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicaties dat in de plaats kwam van het vorige artikel.

Gezien het wetgevende werk dat op Europees niveau aan de gang was sinds 2002 werd met de uitwerking van dit KB gewacht tot de EU haar werkzaamheden had afgerond. De omzetting van de Europese richtlijn levert immers een duidelijk kader voor de effectieve uitvoering van de al bestaande wettelijke bepalingen. De omzetting via een KB ligt dus volledig in de lijn van de wil van de wetgever.

10. De bewaartermijn (advies, § 33 tot 37)

De minimale termijn van zes maanden die wordt gevraagd door een groot deel van de partijen die reageerden op de consultatie door het BIPT vult de behoeften op het terrein helemaal niet in.

Voor vaste en mobiele telefonie houdt men sinds jaren een termijn van 12 maanden bewaring van de communicatiegegevens aan. Maar zelfs deze bewaringstermijn lijkt in vele gevallen onvoldoende te zijn. Voornamelijk in belangrijke dossiers wordt onderzoek gevoerd naar telefoniegebruik. Maar gezien de complexiteit van deze dossiers blijkt de termijn van 1 jaar vaak te kort.

Voici quelques exemples issus de dossiers qui nous ont été communiqués par les unités de recherche.

- Une personne disparaît. La demande des données de son gsm connu n'apporte aucune information. Un an après sa disparition, les enquêteurs obtiennent des renseignements selon lesquels la personne disparue avait plusieurs numéros de gsm. Les opérateurs n'ont plus été en mesure de fournir les données d'appel pour les numéros de gsm récemment découverts. La personne est toujours introuvable.

- Un pédophile est arrêté. Il s'avère qu'il abuse depuis des années de petites filles. Il les contacte par SMS à des numéros qu'il a vus à la télévision (MTV, JIM TV, …). La demande des données de communication pour son gsm a permis de retrouver les victimes de la dernière année. Les victimes qu'il avait contactées avant cette période n'ont plus pu être retrouvées.

- Un criminel est arrêté dans le cadre d'un dossier important de paris illégaux et de corruption privée. Il ressort du dossier qu'il corrompt depuis une plus longue période des sportifs afin d'influencer les résultats de compétitions. Les données d'appel disponibles montrent que non seulement des sportifs mais également des managers sont impliqués. Le délai de conservation limité des données n'a permis d'établir qu'une partie restreinte des activités de ce criminel et d'autres organisations impliquées sont passées entre les mailles du filet.

- Un dossier porte au total sur une série de 20 "home invasions" dans des quartiers de villas où les habitants sont souvent menacés et où des quantités importantes d'argent et de bijoux sont dérobées. Les faits se déroulent sur le territoire de plusieurs arrondissements. Tous les faits ne sont rassemblés en un seul dossier qu'après des mois d'enquête. Les données de téléphonie disponibles de ces dossiers sont rassemblées et à nouveau analysées. Alors que l'analyse permet finalement de retenir deux numéros de GSM suspects, il s'avère que les données de téléphonie relatives à la période des derniers faits ne sont déjà plus disponibles. Un délai de conservation de deux ans aurait pu, dans ce cas-ci, permettre de démasquer le réseau des auteurs impliqués.

- Dans des dossiers importants de corruption et de fraude, on part souvent d'un seul fait précis. Ce n'est qu'ensuite que les pièces du puzzle s'emboîtent vraiment bien. Dans son audition, un suspect communique des indices concernant des faits similaires commis par d'autres suspects. De tels dossiers exigent souvent

Hierna zijn een aantal voorbeelden opgesomd die komen uit dossiers die ons door de recherche-eenheden werden overgemaakt.

- Een persoon verdwijnt. Het opvragen van de gegevens van zijn gekende gsm leveren geen informatie op. Eén jaar na zijn verdwijning krijgen de speurders informatie dat de verdwenen persoon meerdere gsm-nummers had. De operatoren konden voor de nieuw ontdekte gsm-nummers geen oproepgegevens meer verstrekken. De persoon is nog steeds spoorloos.

- Een pedofiel wordt opgepakt en blijkt al jaren jonge meisje te misbruiken. Hij contacteert ze per SMS op nummers die hij zag op televisie (MTV, JIM TV, ...). Op basis van de bevraging van de communicatiegegevens voor zijn gsm konden de slachtoffers van het laatste jaar worden opgespoord. De slachtoffers die hij voor die periode contacteerde, konden niet meer worden opgespoord.

- In een belangrijk dossier van illegaal gokken en private omkoping wordt een crimineel opgepakt. Uit het dossier blijkt dat hij sinds langere periode sportmensen omkoopt om wedstrijden te beïnvloeden. De beschikbare oproepgegevens tonen aan dat niet alleen sportlui maar ook managers betrokken zijn. Door de beperkte bewaringstermijn van gegevens kan slechts een beperkt deel van zijn activiteit worden aangetoond en ontspringen anderen betrokken organisaties de dans.

- Een dossier omvat in totaal een serie van 20 "home-invasions" in villawijken waarbij de bewoners vaak worden bedreigd en aanzienlijke hoeveelheden geld en juwelen worden buitgemaakt. De feiten situeren zich op het grondgebied van verschillende arrondissementen. Het samenvoegen van alle feiten in één dossier gebeurt pas na maanden onderzoekswerk. De beschikbare telefoniegegevens uit deze dossiers worden samengevoegd en opnieuw geanalyseerd. Als men uiteindelijk uit de analyse 2 verdachte GSM-nummers kan weerhouden, blijken de telefoniegegevens ten tijde van de laatste feiten al niet meer beschikbaar te zijn. Een bewaringstermijn van 2 jaar had hier het netwerk van de betrokken daders kunnen blootleggen.

- In belangrijke dossiers van corruptie en fraude vertrekt men vaak vanuit één bepaald feit waarna de bal pas echt goed aan het rollen gaat. De ene verdachte geeft in zijn verhoor aanwijzingen over soortgelijke feiten door andere verdachten. Dergelijke dossiers vergen vaak jaren onderzoekswerk waarbij de achterliggende

des années d'enquête, les organisations sous-jacentes n'étant mises au jour qu'après que leur comptabilité a été épluchée. Souvent, les données concernant les contacts téléphoniques entre les personnes véritablement impliquées de ces sociétés ne peuvent alors plus être demandées. De ce fait, certaines personnes échappent à la justice parce que les éléments de preuve qui auraient pu être fournis par les données de téléphonie font défaut.

- Dans le cadre d'un trafic de drogue, l'Allemagne demande l'identification d'un certain nombre de numéros de gsm belges appartenant à des personnes qui fournissent de la drogue en Allemagne. Cette investigation donne des résultats positifs pour l'enquête allemande. Toutefois, un certain nombre de numéros de téléphone ne peuvent être directement utilisés dans l'enquête. Plus d'un an plus tard, l'unité belge concernée ouvre un nouveau dossier concernant un trafic de drogue. Un des numéros figurant dans ce dossier s'avère être lié au dossier allemand. Le lien est par la suite établi entre ces deux dossiers. L'analyse des données de téléphonie de ces deux dossiers conjoints a permis d'identifier au total une dizaine de suspects. Les données de téléphonie disponibles couvraient par chance une période de 2,5 ans. Si les données n'avaient pas été disponibles pour l'ensemble de cette période, seuls deux auteurs auraient pu être mis sous les verrous. Dans des dossiers d'une telle ampleur, un délai de conservation plus long représente une plus-value décisive.

- Souvent, les données de téléphonies sont également utilisées pour pouvoir étayer certaines déclarations et prouver l'existence de contacts entre les différents coauteurs dans un dossier. Dans le dossier DUTROUX et dans le dossier André COOLS, certaines allégations n'ont pu être vérifiées parce que les déclarations avaient été faites au-delà du délai d'un an.

- Une femme est retrouvée à l'état de momie près d'un an après être décédée de mort violente. Plus aucune donnée de téléphonie n'a pu être demandée.

- La police reçoit de l'étranger des informations selon lesquelles une personne fabriquerait des explosifs à la demande d'un terroriste qui voudrait commettre avec ceux-ci un attentat dans une grande ville en Belgique. Le fabriquant de ces explosifs, sans avoir été identifié comme tel, commet peu de temps après l'ouverture de l'enquête un hold-up et est incarcéré pendant un an et deux mois. Ce n'est qu'après sa libération que le lien est établi avec le suspect. Celui-ci ne veut toutefois pas donner d'informations concernant le commanditaire. Les données de téléphonie n'ont plus pu être consultées en raison du délai de rétention trop court.

organisatie pas na uitpluizen van boekhoudingen wordt blootgelegd. De telefonische contacten tussen de effectieve betrokkenen uit die firma's kunnen dan vaak niet meer worden opgevraagd waardoor sommige personen uit de handen van het gerecht blijven wegens ontbreken van bewijsmateriaal dat had kunnen geleverd worden met telefoniegegevens.

- In kader van een drugstrafiek vraagt Duitsland om een aantal Belgische gsm-nummers te identificeren van drugleveranciers naar Duitsland. Het resultaat van dit onderzoek levert positieve resultaten op voor het Duits onderzoek. Een aantal telefoonnummers kan echter niet dadelijk worden geplaatst in het onderzoek. Meer dan een jaar later wordt in de betrokken Belgische eenheid een nieuw dossier betreffende drugstrafiek opgestart. Eén van de nummers die in dit dossier voorkomen, blijkt een link te hebben met het Duitse dossier waarna deze dossiers met elkaar worden gelinkt. Uit de analyse van de telefoniegegevens uit deze twee dossiers samen konden in totaal een tiental verdachten worden geïdentificeerd. De beschikbare telefoniegegevens omvatten door dit toeval een periode van 2,5 jaar. Zonder de beschikking over de gegevens voor deze gehele periode hadden slechts 2 daders kunnen worden ingerekend. De meerwaarde van de langere bewaartermijn in dergelijke grote dossiers van cruciaal belang.

- Vaak worden de telefoniegegevens ook gebruikt om bepaalde verklaringen te kunnen staven en contacten tussen de verschillende mededaders in een dossier te kunnen aantonen. In het dossier DUTROUX en het dossier André COOLS konden bepaalde beweringen niet meer worden geverifieerd omdat de verklaringen pas na het verlopen van een jaar werden afgelegd.

- Een vrouw wordt als gemummificeerd lijk gevonden bijna een jaar na haar gewelddadig overlijden. Er konden geen telefoniegegevens meer worden opgevraagd.

- De politie krijgt uit het buitenland informatie dat een persoon springstoffen zou aanmaken op vraag van een terrorist die hiermee een aanslag wilde plegen in een drukke stad in België. De springstofaanmaker, zonder alszodanig geïdentificeerd geweest te zijn, pleegt kort na de start van het onderzoek echter een overval waardoor hij voor een jaar en twee maand in de cel beland. Pas na zijn vrijlating wordt de link gelegd met de vrijgekomen verdachte. Deze wil echter geen informatie verstrekken over de opdrachtgever. Telefoniegegevens konden niet meer worden geraadpleegd wegens de te korte retentietermijn.

Progressivement toutefois, les communications se font via Internet. A la complexité de l'enquête mentionnée ci-dessus s'ajoute la difficulté que pose sur un plan technique l'identification sur Internet. L'identification d'un utilisateur internet nécessite généralement plusieurs réquisitions successives auprès de différents opérateurs. En outre, certains de ces opérateurs sont établis à l'étranger.

Dans des dossiers du parquet fédéral, la FCCU trace sur réquisition des suspects qui ont utilisé Internet. Les CCU régionales fournissent un appui similaire aux parquets d'arrondissement. Concernant le traitement des réquisitions adressées à la FCCU, il existe des chiffres qui montrent clairement qu'un délai de conservation de 12 mois est absolument insuffisant pour couvrir les besoins.

Il ressort des chiffres de la FCCU relatifs à l'identification des adresses IP en 2007 qu'un délai de conservation de 6 mois ne permet de répondre qu'à 15 % des demandes. (voir tableau en annexe).

A cet égard, il ne faut pas perdre de vue que le parquet fédéral demande généralement l'intervention de la FCCU dans des dossiers de terrorisme, de traite des êtres humains, de pornographie enfantine ou dans le cadre d'une demande d'entraide judiciaire. Il s'agit donc toujours de criminalité grave.

Si le délai devait être limité à une seule année, les opérateurs ne pourront donner une réponse que dans 66 % des cas, soit 2 cas sur 3.

Si le délai de conservation est porté à 18 mois, 84 % des demandes trouveront une réponse.

Au total, 83 % des demandes adressées aux opérateurs ont permis une identification effective.

Le tableau ci-dessus nous apprend en outre que les opérateurs peuvent actuellement fournir une identification dans 46 % des cas où les données datent de plus de 18 mois.

Au vu de ce qui précède et de l'analyse des exemples et des statistiques, nous pouvons conclure qu'un délai de conservation de 6 ou 12 mois est trop court et qu'un délai de 24 mois, prévu également dans la directive, est certainement justifié si l'on se base sur les besoins de la justice et de la police.

Stilaan verschuift het communicatiegebeuren echter naar het Internet. Daar komt naast de hierboven aangehaalde complexiteit van het onderzoek nog eens de technische complexiteit van de internetidentificatie. Het identificeren van een internetgebruiker noodzaakt meestal de uitvoering van verschillende opeenvolgende vorderingen bij verschillende operatoren. Bovendien situeren een aantal van deze operatoren zich in het buitenland.

In dossiers van het Federaal Parket spoort de FCCU op vordering verdachten op die gebruik maakten van internet. Een soortgelijke steun wordt door de regionale CCU's geleverd aan de arrondissementele parketten. Voor wat de verwerking van de vorderingen bij de FCCU betreft, zijn er cijfers beschikbaar die duidelijk aantonen dat de bewaringstermijn van 12 maanden absoluut onvoldoende is om de behoefte in te dekken.

Uit de FCCU-cijfers voor de identificatie van IP-adressen in 2007, leren we dat we met een bewaringstermijn van 6 maand slechts 15 % van de gestelde vragen kan worden beantwoord (zie tabel in bijlage).

Hierbij mogen we niet uit het oog verliezen dat het Federaal Parket in het algemeen de FCCU tussenkomst vraagt in dossiers van terrorisme, mensenhandel, kinderpornografie of in het kader van een rechtshulpverzoek. Het betreft dus steeds ernstige criminaliteit.

Indien de termijn zou worden beperkt tot één jaar dan zal door de operatoren slechts in 66 % van de gevallen kunnen worden geantwoord: 2/3 gevallen.

Wordt de bewaartermijn opgetrokken tot 18 maand dan kunnen 84 % van de gestelde vragen worden opgelost.

In totaal leverde 83 % van de vragen aan de operatoren een effectieve identificatie op.

Uit de bovenstaande tabel leren we bovendien dat de operatoren vandaag al in 46 % van de gevallen waarbij de gegevens ouder zijn dan 18 maand, een identificatie kunnen leveren.

Gezien het bovenstaande, en uit analyse van de voorbeelden en de statistieken kunnen we besluiten dat een bewaringstermijn 6 of 12 maanden te kort is en dat een termijn van 24 maanden zoals dit ook in de richtlijn is voorzien zeker gerechtvaardigd is vanuit de behoeften van justitie en politie.

11. “Circonstances particulières” dans lesquelles le roi peut prolonger le délai de conservation (points 38-40 de l’avis).

La Commission estime que les termes “circonstances particulières” n’offrent pas suffisamment de sécurité juridique, sont vagues et sujets à une trop grande interprétation.

Afin de répondre à cette préoccupation, les mots “circonstances particulières” sont définis en renvoyant à l’article 4, § 1er, de la LCE: les circonstances particulières sont donc présentes “lorsque la sécurité publique, la santé publique, l’ordre public ou la défense du Royaume l’exigent”.

La contradiction entre les textes français et néerlandais a également été corrigée: comme prescrit dans la directive européenne, il s’agit d’une période limitée.

12. Remarques générales concernant le projet d’arrêté royal (points 41-43 de l’avis)

Concernant les délais de conservation, il peut être renvoyé à l’explication donnée au point 9.

Base légale pour une extension limitée de la liste des données définie par la directive européenne.

Comme indiqué précédemment, la directive européenne 2006/24/CE définit le cadre général de la conservation des données. La directive comble ainsi un besoin généré par l’exécution de la directive européenne 2002/58/CE qui prévoit que les données issues de communications électroniques doivent en principe être supprimées ou rendues anonymes si elles ne sont plus utilisées pour la facturation, le marketing ou la fourniture de services basés sur ces données. L’article 15 de la directive européenne 2002/58/CE permettait et permet toujours aux États membres d’imposer la conservation des données de communication de communications électroniques pour autant que cette conservation soit prévue par la loi et soit justifiée.

La plupart des États membres se sont servis de cette dérogation au principe de base afin de développer leur propre cadre en matière de rétention de données. Toutefois, les divergences étaient telles entre les différents développements qu’une harmonisation entre les États membres s’imposait. C’est vers cette harmonisation que tend la directive de 2006. L’article 15 de la directive de 2002 n’a pas été supprimé par la directive de 2006 bien que la question ait fait débat. La volonté

11. De “uitzonderlijke omstandigheden” waarbij de Koning de bewaartermijn kan verlengen (advies § 38-40).

De Commissie meent dat de term “uitzonderlijke omstandigheden” niet voldoende rechtszekerheid biedt, vaag is en te ruim interpreteerbaar.

Om aan deze bezorgdheid tegemoet te komen worden de uitzonderlijke omstandigheden gedefinieerd door te verwijzen naar artikel 4, § 1 van de WEC: de uitzonderlijke omstandigheden zijn hier dus “wanneer de openbare veiligheid, de volksgezondheid, de openbare orde of de verdediging van het Rijk dit eisen”.

Ook de tegenstelling tussen de Franse en de Nederlandse tekst wordt verbeterd: zoals de Europese richtlijn voorschrijft gaat het om een beperkte periode.

12. Algemene opmerkingen bij het ontwerp van KB (advies, § 41-43)

Op het gebied van de bewaartermijnen kan verwezen worden naar de uitleg onder punt 9.

Rechtsgrond voor een beperkte uitbreiding van de lijst van gegevens die door de Europese richtlijn werd bepaald.

De Europese richtlijn 2006/24/CE legt, zoals eerder vermeld, het algemene kader voor de gegevensbewaring vast. De richtlijn vult hiermee een behoefte in die was ontstaan bij de uitvoering van de eerdere Europese richtlijn 2002/58/CE die bepaalt dat de gegevens die voorkomen uit elektronische communicaties in principe gewist of geanonimiseerd dienen te worden indien ze niet langer dienen voor facturatie, marketing of voor het aanbieden van diensten die op deze gegevens zijn gebaseerd. Artikel 15 van de Europese richtlijn 2002/58/CE liet en laat nog steeds aan de lidstaten toe om een verplichte bewaring van communicatiegegevens van elektronische communicatie op te leggen mits deze bewaring wettelijk wordt voorzien en wordt gerechtvaardigd.

Deze afwijking op het basisprincipe werd door de meeste lidstaten gebruikt om een eigen kader voor dataretentie uit te werken. De diverse uitwerkingen verschilden echter zo erg van elkaar dat een harmonisatie tussen de lidstaten zich opdrong. Deze harmonisatie wordt beoogd met de richtlijn van 2006. Artikel 15 van de richtlijn van 2002 is door de richtlijn van 2006 niet afgeschaft hoewel daarover debat is gevoerd. Heel duidelijk was dus de wil op Europees niveau om de mogelijkheid

au niveau européen de laisser ouverte la possibilité d'imposer au plan national la conservation d'autres données en plus de celles mentionnées dans la directive 2006/24/CE était par conséquent très claire.

Le gouvernement souhaite faire usage de cette possibilité afin de combler un certain nombre de lacunes dans le cadre européen. La directive européenne a en effet été élaborée rapidement, de sorte que certaines questions n'ont pas été prises en considération. Si la liste de la directive n'est pas complétée par un nombre limité de données supplémentaires, l'efficacité de la rétention de données s'en trouvera sapée. Il s'agit principalement des données d'identification (voir plus loin).

Enfin, la Commission fait observer au point 42 que la durée de conservation des données va à l'encontre du texte de la directive. Le texte du projet d'arrêté royal sera adapté de manière à ce que les données soient conservées pendant 24 mois à compter de la date de la dernière communication enregistrée (données d'identification) ou de la date de la communication (données de trafic et de localisation). En ce qui concerne la fin de la période de conservation des données d'identification, nous nous écartons légèrement de la directive. En effet, l'identification d'un service utilisé ou d'un abonnement est nécessaire pour donner un sens à toutes les communications dont la conservation des données de trafic a été ordonnée. Sans données d'identification, il est impossible de demander les données de trafic d'une communication. Les données d'identification doivent par conséquent rester disponibles dans les 24 mois qui suivent la dernière utilisation de ce service de communication.

13. Commentaire relatif à l'extension limitée de la liste des données définie par la directive européenne (points 44, 46, 47, 50, 53, 54, 57, 58 et 59 de l'avis)

La série de données suivante, absente de la directive, figure dans le projet:

1. Téléphonie fixe

1.1. Données d'identification
- la date de commencement de l'abonnement;
- le cas échéant, l'identité de l'opérateur d'origine de l'abonné en cas de transfert de son numéro auprès d'un autre opérateur;
- les services annexes auxquels l'abonné à souscrit;
- les données relatives au type de paiement ainsi qu'à l'identification et à la date du paiement.

1.2. Données de trafic et de localisation - article 2, § 2
Pas de données supplémentaires.

op nationaal niveau open te laten om bovenop de gegevens die vermeld zijn in de richtlijn 2006/24/CE ook nog de bewaring van andere gegevens op te leggen.

De regering wenst van deze mogelijkheid gebruik te maken om een aantal lacunes in het Europese kader in te vullen. De Europese richtlijn werd immers in een spoedtempo uitgewerkt waarbij een aantal zaken over het hoofd werden gezien. Indien de lijst van de richtlijn zelf niet verder wordt aangevuld met een beperkt aantal bijkomende gegevens, wordt de effectiviteit van de dataretentie ondergraven. De bijkomende gegevens betreffen voornamelijk de identificatiegegevens (zie verder).

Tot slot, de Commissie merkt in randnummer 42 op dat de bewaarduur van de gegevens ingaat tegen de tekst van de richtlijn. De tekst van het ontwerp van Koninklijk Besluit zal aangepast worden zodat gegevens bewaard worden 24 maand vanaf de datum van de laatst geregistreerde communicatie (identificatiegegevens) of vanaf de datum van de communicatie (verkeers- en locatiegegevens). Wat betreft het einde van de bewaarperiode van de identificatiegegevens wordt licht afgeweken van de richtlijn. Identificatie van een gebruikte dienst of van een abonnement is immers noodzakelijk om zin te geven aan alle communicaties waarvan de bewaring van de verkeersgegevens is voorgeschreven. Zonder identificatiegegevens is het onmogelijk om verkeersgegevens van een communicatie op te vragen. Bijgevolg dienen de identificatiegegevens beschikbaar te blijven gedurende 24 maand na het laatste gebruik van deze communicatiedienst.

13. Toelichting bij de beperkte uitbreiding van de lijst van gegevens die door de Europese richtlijn werd bepaald (advies, §§ 44, 46, 47, 50, 53, 54, 57, 58, 59)

Volgende reeks van gegevens worden in het ontwerp opgenomen en staan niet in de richtlijn:

1. Vaste telefonie

1.1. Identificatiegegevens
- datum van aanvang van het abonnement;
- in voorkomend geval: de operator vanwaar de klant komt bij nummeroverdraging;
- de bijhorende diensten waarbij de abonnee geregistreerd is;
- de gegevens inzake type, identificatie en tijdstip van betaling.

1.2. Verkeers- en locatiegegevens – Art 2 § 2
Geen bijkomende gegevens.

2. Téléphonie mobile - article 3

2.1. Données d'identification - article 3, § 1er

- la date et le lieu de la souscription du service;
- le cas échéant, l'identité de l'opérateur d'origine de l'abonné en cas de transfert de son numéro auprès d'un autre opérateur;
- les services annexes auxquels l'abonné à souscrit;
- les données relatives au type de paiement ainsi qu'à l'identification et à la date du paiement.

2.2. Données de trafic et de localisation - article 3, § 2
- la localisation du point de terminaison du réseau à la fin de chaque communication.

3. Accès à l'Internet - article 4

3.1. Données d'identification - article 4, § 1er

- la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur;
- l'adresse IP ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur;
- l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu'utilisateur enregistré si celle-ci est disponible;
- les services annexes auxquels l'abonné à souscrit;

- les données relatives au type de paiement ainsi qu'à l'identification et à la date du paiement

3.2. Données de trafic et de localisation - article 4, § 2

- le volume de données uploadé et downloadé pendant la durée de la session ou autre unité de temps demandée;
- la localisation du point de terminaison du réseau au début et à la fin de chaque communication;
- le cas échéant, les données de localisation géographique au moyen de l'identifiant cellulaire.

4. Service de courrier électronique et téléphonie par Internet - article 5

4.1. Données d'identification - article 5, § 1er
— la date et l'heure de la création du compte de courrier électronique ou de téléphonie par Internet
— l'adresse IP ayant servi à la création du compte de courrier électronique ou de téléphonie par Internet
— les données relatives au type de paiement ainsi qu'à l'identification et à la date du paiement des 24 derniers mois

2. Mobiele telefonie – Art 3

2.1. Identificatiegegevens – Art 3 § 1

- Datum en de plaats van de registratie bij de dienst;
- In voorkomend geval: de operator vanwaar de klant komt bij nummeroverdraging;
- de bijhorende diensten waarop de abonnee geregistreerd is;
- de gegevens inzake type, identificatie en tijdstip van betaling.

2.2. Verkeers- en locatiegegevens – Art 3, § 2
- de locatie van het netwerkaansluitpunt bij het einde van elke verbinding.

3. Internettoegang – Art 4

3.1. Identificatiegegevens – Art 4 § 1

- Datum en het tijdstip van het nemen van het abonnement of de registratie van de gebruiker
- IP-adres dat gediend heeft voor het nemen van het abonnement of voor de registratie van de gebruiker;
- Identificatie van het netwerkaansluitpunt dat gediend heeft voor het nemen van het abonnement of voor de inschrijving als geregistreerde gebruiker als deze laatste mogelijkheid beschikbaar is
- de bijhorende diensten waarbij de abonnee geregistreerd is;
- de gegevens inzake type, identificatie en tijdstip van betaling.

3.2. Verkeers- en locatiegegevens – Art 4, § 2

- het volume van gegevens die tijdens de sessie of gevraagde tijdseenheid geüpload en gedownload werden;

- Lokalisatie van het netwerkaansluitpunt bij aanvang en einde van elke verbinding;
- In voorkomend geval, de geografische lokatiegegevens middels de celidentiteit.

4. E-maildienst & internettelefonie – Art 5

4.1. Identificatiegegevens – Art 5, § 1
— Datum en het tijdstip van de creatie van e-mail of internettelefonieaccount
— IP-adres dat gediend heeft voor de creatie van e-mail of internettelefonieaccount
— de gegevens inzake type, identificatie en tijdstip van betaling van de laatste 24 maanden

4.2. Données de trafic et de localisation - article 5, § 2

Pas de données supplémentaires.

Justification des données d'identification supplémentaires

1. Caractère nécessaire, raisonnable et proportionnel de l'extension des données d'identification

Les données demandées en plus de celles figurant sur la liste de la directive portent principalement sur l'identification des parties concernées, sur la source de la communication.

L'objectif de l'identification par une autorité compétente est de retrouver le véritable utilisateur d'un service de communication. Cette identification implique évidemment la nécessité de conserver les données personnelles de l'utilisateur enregistré. Toutefois, l'utilisation fréquente de fausses données d'identité impose également de recourir à d'autres données administratives et techniques disponibles chez les opérateurs:

- les différentes adresses disponibles;
- les données techniques de la connexion utilisées pour s'enregistrer;
- les données relatives au paiement du service de communication électronique.

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

La quantité des données supplémentaires demandées est limitée car elles concernent l'utilisateur et non les données de trafic. La conservation de ces données est toutefois nécessaire pour permettre une utilisation judicieuse des données de trafic conservées. Les données dont la conservation est demandée sont déjà conservées par les opérateurs comme données client.

La police et la justice s'en servent déjà et ont pu dans plusieurs cas dépister des criminels qui, dans le cadre de la criminalité organisée, faisaient usage de connexions mobiles ou Internet apparemment anonymes.

4.2. verkeers- en locatiegegevens – Art 5, § 2

Geen bijkomende gegevens.

Rechtvaardiging van de bijkomende identificatiegegevens

1. Noodzaak, redelijkheid en proportionaliteit van de uitbreiding van de identificatiegegevens

De gegevens die gevraagd worden bovenop de lijst van de richtlijn, hebben voornamelijk te maken met de identificatie van de betrokken partijen, voornamelijk met de bron van de communicatie.

Het doel van een identificatie door een bevoegde overheid is het achterhalen van de reële gebruiker van een communicatiedienst. Deze identificatie houdt vanzelfsprekend in dat men de persoonsgegevens van de geregistreerde gebruiker dient te bewaren. Gezien echter vaak gebruik wordt gemaakt van valse identiteitsgegevens, is het tevens noodzakelijk om andere administratieve en technische gegevens te gebruiken die beschikbaar zijn bij de operatoren:

- verschillende beschikbare adressen;
- technische informatie van de verbinding die diende om zich te registreren;
- de gegevens omtrent de betaling van de elektronische communicatiedienst.

Niet alleen zetten die bijkomende gegevens ons op het spoor van de effectieve gebruiker maar we kunnen er tevens mee uitsluiten dat slachtoffers van identiteitsfraude onterecht worden betrokken als dader in een gerechtelijk dossier waar zij geen uitstaans mee hebben. De bijkomende gegevens voorkomen zo ook dat de privacy van deze onschuldige personen verder zou worden geschonden door meer indringende, navolgende onderzoeksmaatregelen zoals een interceptie van hun communicatie of een huiszoeking.

De gevraagde bijkomende gegevens zijn beperkt in omvang omdat ze betrekking hebben op de gebruiker en niet op de verkeersgegevens. De bewaring van deze gegevens is echter noodzakelijk om de bewaarde verkeersgegevens zinvol te kunnen aanwenden. De gegevens waarvan de bewaring wordt gevraagd, worden vandaag al door de operatoren bijgehouden als klantengegevens.

Politie en justitie maken er ook vandaag al gebruik van en konden in verschillende gevallen toch op het spoor komen van criminelen die binnen het kader van georganiseerde criminaliteit gebruik maakten van schijnbaar anonieme mobiele of internetverbindingen.

Certaines données supplémentaires concernant l'abonnement au service de communication électronique considéré doivent fournir à la police et à la justice des indices complémentaires quant à l'utilité d'une demande d'information auprès d'un opérateur: les services supplémentaires auquel l'utilisateur est abonné, le commencement et la fin de l'abonnement, l'opérateur précédent en cas de portabilité du numéro.

Ces données sont également limitées en nombre et sont elles aussi déjà conservées chez les opérateurs.

Vous trouverez ci-dessous des explications complémentaires concernant ces différentes données présentées une à une.

2. Données personnelles (point 44 de l'avis)

En ce qui concerne l'abonné ou l'utilisateur enregistré, nous demandons les différentes adresses enregistrées auprès d'un opérateur: adresse(s) de livraison et de facturation.

Les adresses de livraison et de facturation ne sont pas toujours les mêmes. L'adresse de livraison (point de terminaison du réseau) est évidemment primordiale et indispensable. L'adresse de facturation est tout aussi essentielle car elle permet également de dépister la personne ou l'organisation qui paie l'abonnement. Nous avons constaté dans différents dossiers qu'une personne morale se chargeait de régler les factures des connexions téléphoniques ou internet utilisées par des criminels. L'adresse de facturation nous a conduits à cette personne morale.

3. Données de paiement (point 46 de l'avis)

Les données de paiement liées à l'abonnement sont un autre élément qui actuellement aide les services de police à identifier l'utilisateur réel d'un service de communication

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

Les termes "données bancaires" du projet précédent sont remplacés par les "données de paiement" suivantes:

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

Ook deze gegevens zijn beperkt in omvang en worden nu ook bijgehouden bij de operatoren.

Hierna worden de verschillende gegevens één voor één verder toegelicht.

2. Persoonsgegevens (advies, § 44)

Voor de abonnee of de geregistreerde gebruiker vragen we de verschillende adressen die bij een operator zijn geregistreerd: leveringsadres en facturatieadres.

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

3. Betalingsgegevens (advies, § 46)

Een ander element dat actueel de politiediensten helpt bij de identificatie van de reële gebruiker van een communicatiedienst, zijn de betalingsgegevens verbonden aan het abonnement.

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

De term "bankgegevens" uit het vorige ontwerp wordt vervangen door de volgende betalingsgegevens:

- type de paiement (virement, ATM, paiement par carte de crédit, …);
- identification du moyen de paiement (numéro de compte, numéro de carte de paiement, …);
- date et heure du paiement.

Nous demandons que les opérateurs conservent les données de paiement des 24 derniers mois afin de pouvoir également analyser l'unique trace éventuelle pouvant conduire à l'utilisateur réel durant la période où les données de trafic sont conservées.

Les données demandées sont actuellement disponibles chez les opérateurs et sont régulièrement demandées par les autorités judiciaires. C'est essentiellement le cas lorsque des cartes prépayées sont utilisées.

Ces données de paiement constituent donc pour le magistrat une trace susceptible de le mener à l'utilisateur pour lequel il pourra ensuite ouvrir une enquête auprès des organismes bancaires concernés.

4. Données techniques relatives à la création d'un compte auprès d'un service internet

Différents services liés à Internet permettent de s'enregistrer en ligne en tant que nouvel utilisateur.

En l'absence de contact réel entre l'opérateur ou le fournisseur de service et le client, il est de plus en plus fréquent de voir l'utilisateur encoder de fausses données d'identité. Pour permettre l'identification réelle de l'utilisateur, il faut en pareils cas conserver les traces laissées sur Internet (adresse IP et point de terminaison du réseau lors de la création du compte).

Par exemple, si un utilisateur d'Internet crée une boîte à messages internet sur mail.be au nom de Mickey Mouse habitant à Disneyland, les "données personnelles" enregistrées ne sont d'aucune utilité. L'adresse IP de cet utilisateur ainsi que la date et l'heure de la création de son "abonnement" sont les seules données fiables pouvant nous conduire au véritable utilisateur.

Cela doit contribuer à éviter qu'une "identification" basée sur les "données personnelles" nous mène à la mauvaise personne. En effet, si l'enregistrement n'était pas fait au nom de Mickey Mouse mais au nom d'une personne existante et à son insu, il ne serait pas évident de repérer le caractère erroné de ces données personnelles.

- type betaling (overschrijving, ATM, kredietkaartbetaling, ...);
- identificatie van het betalingsmiddel (rekeningnummer, betaalkaartnummer, ...);
- datum en tijdstip van de betaling.

We vragen dat de operator de betalingsgegevens van de laatste vierentwintig maanden bijhoudt om over de periode waarin de verkeersgegevens worden bijgehouden ook het mogelijk enige spoor naar de reële gebruiker te kunnen onderzoeken

De gegevens die worden gevraagd zijn vandaag beschikbaar bij de operatoren en worden regelmatig opgevraagd door de gerechtelijke overheden. Dit is voornamelijk het geval wanneer prepaid kaarten worden gebruikt.

Deze betalingsgegevens vormen voor de magistraat dus het spoor naar de gebruiker waarvoor hij dan een navolgend onderzoek kan instellen bij de betrokken bankinstellingen.

4. Technische gegevens van de aanmaak van een account bij een internetdienst

Verschillende internetgebonden diensten laten toe om zich online te registreren als nieuwe gebruiker.

Bij gebrek aan reëel contact tussen de operator of dienstenverstrekker en de klant, is het steeds vaker zo dat de gebruiker valse identiteitsgegevens invoert. Om tot een reële identificatie van de gebruiker te kunnen komen, is het in deze gevallen dan noodzakelijk om de internetsporen (IP-adres en netwerkaansluitingspunt bij creatie van het account) te bewaren.

Bvb. indien een internetgebruiker een webmailbox aanmaakt bij mail.be onder de naam Mickey Mouse wonende in Disneyland, dan zijn de geregistreerde "persoonsgegevens" helemaal van geen nut. Het IP-adres van deze internetgebruiker en de datum en het tijdstip van de creatie van zijn "abonnement" zijn de enige betrouwbare gegevens die ons kunnen leiden naar de echte gebruiker

Dit moet helpen voorkomen dat een "identificatie" op basis van de "persoonsgegevens" ons zou leiden naar de verkeerde persoon. Immers, indien de registratie niet zou genomen zijn op naam van Mickey Mouse maar op naam van een onwetende, bestaande persoon, is de detectie van het valse karakter van deze persoonsgegevens niet voor de hand liggend.

5. Informations concernant le transfert de numéro - début de l'abonnement/du service

Grâce à la libéralisation du marché des télécommunications, il est beaucoup plus facile pour les utilisateurs de téléphonie de changer d'opérateur tout en conservant leur numéro. Pour pouvoir s'informer auprès du bon opérateur, il importe que la police et la justice sachent précisément depuis quand l'utilisateur est affilié à son opérateur actuel et quel était son opérateur d'origine en cas de transfert de numéro. Grâce à ces informations, le juge d'instruction ou, le cas échéant, le procureur du roi peut adresser des réquisitions supplémentaires aux bons opérateurs. Demander des informations à un mauvais opérateur n'a, en effet, aucun sens. Ces données permettront donc d'interroger plus efficacement et de manière plus ciblée les opérateurs. Elles éviteront en outre des demandes inutiles auprès des opérateurs et les frais de justice plus élevés générés par celles-ci.

Justification de l'extension des données de trafic

1. Caractère nécessaire, raisonnable et proportionnel de l'extension des données de trafic

L'extension des données de trafic demandées est très limitée et entend correspondre en fait à la situation existante.

Les données supplémentaires demandées sont déjà conservées et fournies par les opérateurs.

2. Localisation du point de terminaison du réseau à la fin de chaque communication

La directive prévoit la conservation du point de terminaison au début de la communication. Nous souhaitons l'étendre à la terminaison du réseau à la fin de la communication lorsque cette information est disponible.

En téléphonie mobile, il est courant que les gens se déplacent pendant la communication. Etant donné que la localisation de l'appel est souvent utilisée comme ébauche de preuve, il importe d'avoir une idée précise de l'endroit où cette communication a eu lieu. Si le point de terminaison à la fin de l'appel est disponible, il est important pour la justice de savoir où il se trouve.

Dans le passé, certains opérateurs belges ont adapté leur système pour pouvoir communiquer cette

5. Informatie omtrent nummeroverdraging – begin abonnement/dienstverlening

Met de liberalisering van de telecommunicatiemarkt is het voor telefoniegebruikers heel gemakkelijk om over te schakelen van één operator naar een andere met behoud van zijn nummer. Om bij de juiste operator een bevraging te doen is het van belang voor politie en justitie om precies te weten sinds wanneer de gebruiker bij zijn huidige operator is aangesloten en van welke operator hij bij nummeroverdraging afkomstig was. Met deze informatie kan de onderzoeksrechter of in voorkomend geval de procureur bijkomende vorderingen gericht naar de correcte operatoren zenden. Het heeft immers geen zin om gegevens bij een verkeerde operator te gaan opvragen. Deze gegevens zullen dus mee zorgen voor een efficiënter en gerichter vraagstelling aan de operatoren. Ze zullen bijkomend voorkomen dat onnodige vraagstellingen de operatoren belasten en dat hierdoor hogere gerechtskosten worden gegenereerd.

Rechtvaardiging voor de uitbreiding van de verkeersgegevens

1. Noodzaak, redelijkheid en proportionaliteit van de uitbreiding van de verkeersgegevens

De uitbreiding van de gevraagde verkeersgegevens is zeer beperkt en wil eigenlijk aansluiten op de bestaande situatie.

De gegevens die bijkomend worden gevraagd, worden vandaag al bewaard en aangeleverd door de operatoren.

2. De locatie van het netwerkaansluitpunt bij het einde van elke verbinding

De richtlijn voorziet dat het netwerkaansluitpunt bij het begin van de verbinding wordt bijgehouden. We wensen dit uit te breiden met het netwerkaansluitpunt bij het einde van de verbinding waar dit beschikbaar is.

Bij mobiele telefonie is het niet ongewoon dat mensen zich tijdens de communicatie verplaatsen. Gezien de locatie van de oproep vaak als aanzet van bewijs wordt aangewend, is het belangrijk een goed beeld te hebben van de plaats waar deze communicatie is gevoerd. Indien het netwerkaansluitpunt bij het einde van de oproep beschikbaar is, is het voor justitie van belang te kennen waar dit is gelegen.

Sommige Belgische operatoren hebben in het verleden hun systemen aangepast om dit gegeven te kunnen

information, ce qu'ils font actuellement à la demande des autorités judiciaires.

3. Volume de données uploadé et downloadé pendant une session internet

Depuis l'apparition des connexions à large bande avec tarif mensuel fixe et des réseaux WiFi pour utilisateurs à domicile, les utilisateurs restent de plus en plus souvent connectés à Internet 24 heures sur 24. Pour pouvoir fournir les données de connexion et procéder à une évaluation de la faisabilité technique d'une interception internet, il est important pour les enquêteurs de pouvoir se faire une idée de l'activité effective de la connexion internet concernée.

Celle-ci peut, en partie, être déduite des volumes de données uploadés et downloadés. Ces données sont actuellement conservées systématiquement par les opérateurs dans leurs données clients.

14. Article 7 de l'arrêté royal: accès aux données - sanctions pénales - conservation (points 63-66 de l'avis)

En ce qui concerne les "mesures techniques et organisationnelles appropriées" visées à l'article 7, 2°, l'exposé des motifs contiendra un renvoi aux mesures de référence établies par la Commission et applicables au traitement des données à caractère personnel.

La Commission fait judicieusement observer que seul l'accès aux données auprès des opérateurs mêmes est régi. D'autres pouvoirs d'accès sont en effet régis par d'autres dispositions légales. C'est le cas des articles 46*bis* et 88*bis* du Code d'Instruction criminelle précités qui confèrent certaines compétences au procureur du roi et au juge d'instruction. En ce qui concerne le service de médiation et les services d'urgence, ces pouvoirs d'accès doivent dès lors être régis dans d'autres lois. La Commission a elle-même déjà fait remarquer qu'en ce qui concerne le service de médiation, l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 est d'application (voir le point 29 de l'avis).

Concernant les remarques de la Commission aux points 64-65 relatifs aux fournisseurs et revendeurs mentionnés à l'article 9, §§ 5 et 6, de la loi relative aux communications électroniques, ainsi qu'aux sanctions pénales, il peut être renvoyé aux commentaires antérieurs.

La Commission fait en outre observer, à juste titre, que les données consultées seront conservées par les

aanleveren en leveren deze gegevens nu aan op vraag van de gerechtelijke overheden.

3. Het upload en downloadvolume tijdens een internetsessie

Sinds de komst van breedband verbindingen met een vast maandelijks tarief en van WiFi-netwerken voor thuisgebruikers, gebeurt het steeds vaker dat de gebruikers hun internetverbinding 24u op 24 laten opstaan. Om de verbindingsgegevens zin te kunnen geven en om een inschatting te kunnen maken van de technische haalbaarheid van een internetinterceptie, is het van belang dat de onderzoekers beeld krijgen van de effectieve activiteit over de betreffende internetverbinding.

Dit kan voor een deel worden afgeleid uit de volumes van geuploade en gedownloade gegevens. Deze gegevens worden door de operatoren thans ook steeds bijgehouden in hun klantengegevens.

14. Artikel 7 KB: toegang tot de gegevens – strafsancties - bewaring (advies § 63-66)

Wat betreft de passende technische en organisatorische maatregelen" in artikel 7, 2° zal in de memorie van toelichting een verwijzing opgenomen worden naar de door de Commissie opgestelde referentiemaatregelen die toepasbaar zijn op de verwerking van persoonsgegevens.

De Commissie merkt terecht op dat enkel de toegang tot de gegevens bij de operatoren zelf wordt geregeld. Andere toegangsbevoegdheden worden immers geregeld door andere wettelijke bepalingen. Zo zijn er de al eerder vermelde artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering waar aan de PK en de onderzoeksrechter bepaalde bevoegdheden gegeven worden. Voor wat betreft de Ombudsman en de nooddiensten dienen deze toegangsbevoegdheden dan ook geregeld te worden in andere wetten. De Commissie merkte zelf al op dat wat de Ombudsman betreft, artikel 43*bis*, § 3, 7° van de wet van 21 maart 1991 van toepassing is (zie § 29 van het advies).

Wat betreft opmerkingen van de Commissie in §§ 64-65 betreffende de aanbieders en doorverkopers vermeld in artikel 9, §§ 5 en 6 van de wet betreffende de elektronische communicaties, en de strafrechtelijke sancties kan verwezen worden naar eerdere toelichtingen.

De Commissie merkt verder terecht op dat de geraadpleegde gegevens bewaard zullen worden door

autorités judiciaires et ne devront plus être conservées par les opérateurs.

15. Communications n'ayant pas abouti (points 6869 de l'avis)

La Commission fait remarquer que la formulation de "communication n'ayant pas abouti" de l'article 10 ne correspond pas à la définition de la directive européenne. Etant donné que l'article 1er contient déjà une définition de la notion qui, elle, correspond à la directive, la définition de l'article 10 peut être supprimée. Il est ainsi donné suite à l'avis de la Commission.

16. Préposé à la protection des données (points 7073 de l'avis)

A cet égard, il peut être donné suite aux suggestions formulées par la Commission afin de préciser dans l'arrêté royal le statut du préposé à la protection des données.

17. Article 12 de l'arrêté royal (point 74 de l'avis)

L'article 12 a été adapté en ce sens que l'obligation visée par celui-ci vaut pour chaque opérateur.

de bevoegde gerechtelijke autoriteiten en niet langer bewaard dienen te worden door de operatoren.

15. Mislukte oproeppogingen (advies § 6869)

De Commissie merkt op dat de verwoording in artikel 10 van het begrip "mislukte oproeppoging" niet aansluit bij de definiëring van de Europese richtlijn. Aangezien in artikel 1 al een definitie is opgenomen van het begrip die wél aansluit bij de richtlijn, kan in artikel 10 de definitie geschrapt worden, en wordt aldus ingegaan op het advies van de Commissie.

16. Aangestelde gegevensbescherming (advies § 7073)

Hier kan ingegaan worden op de suggesties van de Commissie om het statuut van de aangestelde voor de gegevensbescherming wat te verduidelijken in het KB.

17. Artikel 12 KB (advies § 74).

Artikel 12 werd aangepast in die zin dat de daarin beoogde verplichting geldt voor elke operator.

ANNEXE 5

BIJLAGE 5

Avis n° 20/2009 du 1er juillet 2009

Objet: demande d'avis relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration (A/09/012)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la demande d'avis du Ministre de la Justice, Monsieur Stefaan De Clerck, reçue le 23/04/2009;

Vu le rapport de Monsieur le Président ;

Émet, le 1er juillet 2009, l'avis suivant :

A. INTRODUCTION

1. Le 23 avril 2009, le Ministre de la Justice a demandé à la Commission d'émettre un avis d'urgence concernant l'avant-projet de loi et le projet d'arrêté royal en matière de rétention de données (ci-après "l'avant-projet de loi et le projet d'arrêté royal"), et le projet d'arrêté royal relatif à l'obligation de collaboration (ci-après "le deuxième projet d'arrêté royal").

2. L'urgence est suffisamment motivée. La Commission émet dès lors ci-après un avis urgent concernant les projets précités, en tenant compte des informations dont elle dispose.

B. LÉGISLATION APPLICABLE

3. L'on peut tout d'abord se référer à la Directive 2006/24/CE. Étant donné que des données à caractère personnel sont traitées, la LVP est d'application, de même que la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après la "LCE"). Il faut enfin mentionner l'arrêté royal du 9 janvier 2003 *portant exécution des articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3, du code d'instruction criminelle ainsi que de l'article 109ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques* (ci-après "l'arrêté royal du 9 janvier 2003").

C. ANTÉCÉDENTS

4. Le 2 juillet 2008, la Commission a déjà rendu un avis (n° 24/2008) *relatif à l'avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques et au projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données*. Son avis était à l'époque défavorable. C'est pourquoi le Ministre de la Justice soumet à présent à la Commission l'avant-projet de loi et le projet d'arrêté royal adaptés.

5. Le 3 septembre 2008, la Commission a émis l'avis n° 29/2008 *relatif au projet d'arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques*. Cet avis était également défavorable. Le deuxième projet d'arrêté royal est donc également soumis à présent à la Commission.

D. EXAMEN DE LA DEMANDE D'AVIS

6. La Commission examine ci-après dans quelle mesure ses remarques, telles que formulées dans les conclusions des avis précités, ont été respectées par les projets en question. Par commodité, l'ordre des remarques des avis a été maintenu ci-après, en mentionnant pour chaque point les modifications éventuellement apportées par le demandeur.

D.1. AVANT-PROJET DE LOI ET PROJET D'ARRÊTÉ ROYAL EN MATIÈRE DE RÉTENTION DE DONNÉES

7. *- (Avis n° 24/2008) - vu le principe de légalité, les éléments essentiels en matière de conservation de données doivent être définis clairement dans l'avant-projet de loi. Dans cette optique, la durée de conservation devrait être définie dans l'avant-projet de loi, de même que les données à conserver.*

8. En ce qui concerne la *durée de conservation*, aucune modification n'a été apportée dans l'avant-projet de loi : la durée de conservation ne peut pas être inférieure à 6 mois et ne peut dépasser 24 mois. Il appartient au Roi de fixer la durée de conservation exacte. La Commission maintient son point de vue selon lequel la durée de conservation exacte doit être fixée dans l'avant-projet de loi, vu l'importance de la matière. En ce qui concerne la durée de conservation, elle estime qu'une durée de 12 mois devrait suffire, cf. ci-après aux points 19 à 22 inclus. Il faudrait également stipuler dans l'avant-projet de loi que les données conservées doivent être détruites immédiatement au terme de ce délai.

9. L'Exposé des motifs mentionne toutefois une modification importante au commentaire de l'article 3 de l'avant-projet de loi. Celle-ci consiste à ce que deux ans après l'entrée en vigueur de cet arrêté royal, une évaluation de son application devra être réalisée, afin de pouvoir faire le point sur la nécessité et/ou la suffisance des délais impartis pour les besoins des autorités judiciaires. Le bénéfice de cette disposition réside dans le fait que l'on prévoit la possibilité d'adapter le délai de conservation, le cas échéant à la baisse, s'il ne correspondait plus à la réalité. Comme exposé ci-dessus, la Commission estime que la durée de conservation doit être fixée dans la loi. Il faudrait également inscrire dans la loi même, et non uniquement dans l'Exposé des motifs, qu'une évaluation aura lieu, et de quelle manière. D'après la Commission, cette évaluation devrait être double : *d'une part*, une grande évaluation unique, qui se ferait idéalement après l'évaluation européenne de la Directive 2006/24 qui est prévue, lors de laquelle on devrait fixer définitivement les critères ainsi que la durée de conservation. À titre d'exemple, on peut se référer à cet égard à la loi relative à l'institution et à l'organisation de la plate-forme eHealth, plus particulièrement à l'article 36,

qui fait mention d'une évaluation après deux ans. *D'autre part*, on devrait prévoir un rapport annuel au Parlement par le ministre responsable, par analogie avec ce que stipule l'article 90*decies* du Code d'instruction criminelle. Le rapport annuel en matière de rétention de données peut éventuellement être repris dans le rapport précité, conformément à l'article 90*decies* du Code d'instruction criminelle. La Commission suivra de près l'évaluation et le rapport susmentionnés.

10. Les *données à conserver* sont à présent définies comme suit dans l'avant-projet de loi (article 3, § 1) : "… *les opérateurs fournissant un service de téléphonie fixe accessible au public, un service de téléphonie mobile accessible au public, un service d'accès à l'Internet, un service de courrier électronique ou un service de téléphonie par Internet, conservent les données de trafic, de localisation et les données d'identification d'utilisateurs finals qui sont générées ou traitées par eux lors de la fourniture respective de réseaux ou de services de communications électroniques* …". Conformément à l'Exposé des motifs (partie générale, alinéas 3 et 4), la Directive 2006/24/CE établit la liste des données à conserver, subdivisée en catégories : identification de l'origine d'une communication, identification de la destination d'une communication, détermination des caractéristiques temporelles d'une communication, détermination du type de communication, ainsi que du matériel utilisé, et localisation du matériel utilisé. L'avant-projet de loi regroupe ces catégories de données sous les intitulés "données de trafic et de localisation" et "données d'identification d'utilisateurs finals". Ceux-ci sont ensuite développés davantage dans le projet d'arrêté royal. Les articles 88*bis* et 46*bis* du Code d'instruction criminelle et la terminologie de la LCE sont ainsi respectés. Par ailleurs, l'Exposé des motifs mentionne que la Directive crée également plusieurs sous-catégories au sein de ces différentes catégories de données, selon la nature des réseaux et services impliqués dans une communication : téléphonie fixe, téléphonie mobile, téléphonie par Internet, accès à l'Internet, et courrier électronique par Internet. Ces catégories sont également énumérées explicitement dans le projet d'article 126, de sorte que l'on sait clairement quels opérateurs sont soumis à l'obligation de conservation des données précitées.

11. L'Exposé des motifs stipule enfin (trois derniers alinéas de la partie générale) que la Directive 2006/24/CE établit le cadre général de la conservation des données relative aux communications électroniques. Seules quatre catégories de services de communications électroniques sont visées : la téléphonie fixe, la téléphonie mobile, l'accès à l'Internet et la messagerie électronique et la téléphonie via l'Internet. La technologie de la communication et les protocoles techniques qui règlent cette communication électronique se développent rapidement, en particulier en ce qui concerne les formes de la téléphonie via l'Internet. Pour que le cadre légal soit un instrument efficace dans la lutte contre la criminalité, il est

nécessaire que ce cadre puisse suivre l'évolution de ces protocoles techniques. Un arrêté royal permet une mise à jour rapide du cadre légal.

12. La Commission constate que dans l'avant-projet de loi, les catégories de données à conserver sont définies plus clairement. Leur élaboration via un arrêté royal peut être suivie, en tenant compte du fait que l'effet de l'avant-projet de loi et du projet d'arrêté royal sera évalué (cf. ci-avant, point 9), et qu'une éventuelle modification de l'arrêté royal doit être fixée après une concertation en Conseil des ministres, et ce après avis de la Commission et de l'Institut.

13. *- (Avis n° 24/2008) - la nécessité de conserver certaines données qui ne sont pas prévues dans la directive doit être justifiée, conformément aux principes de l'article 8 de la CEDH.*

14. Le Rapport au Roi du projet d'arrêté royal mentionne que le cadre minimum fixé par la directive pour la conservation des données en matière de communications électroniques ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de détection et de poursuite d'infractions pénales. Ainsi, par exemple, certaines données indispensables en vue de l'identification des personnes concernées par une communication pertinente dans le cadre d'une enquête en matière répressive — telles que les données relatives au paiement — manquent à la liste établie par la directive. Le commentaire des articles du Rapport au Roi précise ensuite, par catégorie de données, quelles données doivent être conservées complémentairement, et pourquoi. Le demandeur a encore fourni des informations complémentaires à ce sujet à la Commission. Sur la base des données précitées, la Commission estime pouvoir conclure au caractère justifié du traitement envisagé, ce toutefois à condition qu'une évaluation ait lieu prochainement (cf. ci-dessus), la nécessité du traitement de ces données devant de nouveau être évaluée.

15. *- (Avis n° 24/2008) - l'avant-projet de loi devrait préciser pour la recherche, la poursuite et la répression de quelles infractions pénales (graves) les données conservées peuvent être utilisées.*

16. Dans sa version modifiée, l'avant-projet de loi prévoit à l'article 3, § 1, a) "la recherche, la détection et la poursuite d'infractions pénales *visées aux articles 46bis et 88bis du Code d'Instruction criminelle*". Le demandeur a précisé à la Commission que sa remarque avait été prise en compte grâce à cet ajout. L'article 46*bis* prévoit notamment la réclamation par le procureur du Roi de données d'identification relatives aux services de télécommunication,

l'article 88*bis* prévoit le repérage et la localisation de communications par le juge d'instruction. C'est en vue de l'applicabilité pratique de ces articles que les données d'identification, données d'appels et données de localisation qui sont visées doivent être conservées. Les deux articles prévoient également des conditions telles que la subsidiarité et la proportionnalité de la mesure. L'article 46*bis* est une compétence du procureur du Roi, l'article 88*bis* du juge d'instruction. Dans les deux cas, les mesures doivent être motivées par écrit et il y a donc des garanties que quiconque ne puisse pas accéder aux données conservées pour quelque raison ou infraction que ce soit. Les deux articles ne prévoient pas de liste des infractions mais un certain seuil est établi pour que ces articles limitent les mesures aux contraventions et crimes. Une énumération exhaustive des infractions graves n'est pas possible selon le demandeur, vu les diverses dispositions pénales particulières. En outre, une modification législative serait chaque fois nécessaire si une infraction devait être ajoutée.

17. La Commission peut être d'accord avec l'argumentation précitée, d'autant plus en raison de la précision apportée par le renvoi explicite aux articles 46*bis* et 88*bis* du Code d'instruction criminelle. L'article 46*bis* prévoit une motivation explicite par le procureur du Roi, laquelle doit refléter la proportionnalité en respectant la vie privée et la subsidiarité à l'égard de tout autre acte d'investigation. L'article 88*bis* prévoit une même disposition pour le juge d'instruction. Elle rappelle en outre que les données demandées par le magistrat qui ne sont pas utiles à l'enquête doivent être détruites.

18. *-(Avis n° 24/2008) - la durée de conservation de 24 mois doit être davantage fondée et justifiée et, le cas échéant, reconsidérée au vu des délais de conservation prévus dans la plupart des pays européens.*

19. Le projet d'arrêté royal a repris la durée de conservation de 24 mois du premier projet. Le Rapport au Roi stipule à ce sujet que sur la base de la pratique observée auprès des différents services de police décentralisés et auprès du Parquet fédéral en matière de demandes d'informations aux opérateurs et aux fournisseurs de réseaux ou de services de communications électroniques, ont peut considérer qu'un délai uniforme de 24 mois pour la conservation des différents types de données visés à l'article 126 de la loi constitue le mécanisme le plus approprié. Le demandeur a fourni à la Commission des exemples de situations dont il devrait ressortir qu'un délai de 24 mois est justifié, et que cela répond à un besoin réel de la police et de la justice.

20. Le demandeur a également informé la Commission d'une étude de l'IBPT relative aux délais de conservation à l'étranger, datant de juillet 2008. Il en ressort que différents pays (parmi lesquels l'Italie, la Slovénie, l'Irlande, le Portugal et les Pays-Bas) prévoient aussi un long délai (18 à 24 mois). D'autres pays (notamment la France, l'Allemagne et le Royaume-Uni) opteraient pour un délai plus court (12 mois). Selon le demandeur, cela serait davantage dicté par des raisons économiques et financières (frais pour les opérateurs).

21. La Commission a également pu prendre connaissance des points de vue de l'industrie des télécoms (ISPA). D'après les chiffres communiqués par cette dernière (étude d'octobre 2008), il apparaît que la durée prévue est, dans la plupart des pays (Danemark, France, Finlande, Espagne, Portugal), de 12 mois ; l'Allemagne a fixé une période de 6-7 mois. Dans d'autres pays, le délai proposé est souvent de 12 mois aussi (Royaume-Uni, Pays-Bas, Suède) ou de 6 mois (Autriche, Luxembourg). Elle fournit également des statistiques dont il devrait ressortir que la plupart des demandes de la justice adressées aux opérateurs de télécommunications belges ont lieu dans les six mois à compter du début de la conservation des données et que le nombre de demandes après 12 mois ne représente pas plus de 5 % du nombre total des demandes.

22. La Commission a pris note des arguments précités. Du point de vue de la justice, il est évident qu'une durée de conservation de 24 mois est nécessaire. L'industrie souhaite par contre limiter autant que possible cette durée de conservation, ce pour diverses raisons. La Commission estime qu'il est important, dans cette discussion, d'observer la finalité initiale de la directive, qui consiste en *l'harmonisation* de la législation dans les États membres en ce qui concerne la conservation de données de télécommunications par les opérateurs. Dans cette optique, le délai de 24 mois semble en ce moment être exagéré, vu le délai de 12 mois ou moins qui est d'application dans nos pays voisins (France, Pays-Bas, Allemagne, Luxembourg). La Commission estime dès lors qu'un délai de conservation de 12 mois est momentanément suffisant. Dans cette optique, l'évaluation envisagée est également importante, le délai pouvant être revu vers le haut ou vers le bas, si nécessaire. L'avant-projet de loi devrait enfin prévoir explicitement qu'au terme de cette durée de conservation, les données doivent être détruites immédiatement par l'opérateur.

23. *-(Avis n° 24/2008) - l'application de l'avant-projet de loi et du projet d'arrêté royal aux fournisseurs et aux revendeurs prévus à l'article 9, §§ 5 et 6 doit être réexaminée et doit éventuellement être prévue pour eux dans une autre disposition.*

24. Dans la version actuelle de l'avant-projet de loi, il n'est plus question des fournisseurs et revendeurs prévus à l'article 9, §§ 5 et 6 de la LCE. La Commission avait insisté sur ce point dans son avis précédent étant donné que l'on doit par exemple entendre par fournisseurs et revendeurs le réseau interne d'un groupe d'entreprises. Ceux-ci ne sont toutefois pas visés par la Directive 2006/24/CE, qui, conformément à l'article 3, s'applique exclusivement aux fournisseurs de services de communication électronique publics ou d'un réseau de communication public pour la fourniture des services de communication en question. D'où la demande de la Commission de supprimer les fournisseurs et revendeurs.

25. Étant donné que l'article 3 de la Directive 2006/24 prévoit que la directive ne s'applique qu'aux fournisseurs de services publics de communications électroniques ou d'un réseau public de télécommunications lors de la fourniture du service de communication en question, l'article 3, § 1 de l'avant-projet de loi doit être adapté. Le mot 'public' ne doit pas uniquement être utilisé dans l'article précité pour un service de téléphonie fixe et un service de téléphonie mobile, mais aussi pour un service d'accès à Internet, un service d'e-mail et un service de téléphonie par Internet. Cela doit donc devenir : un service public d'accès à Internet, un service public d'e-mail et un service public de téléphonie par Internet

26. L'avant-projet de loi prévoit à l'article 2 une adaptation de la notion d'opérateur dans la LCE (article 2, 11°) : "toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9." Version actuelle de l'article 2, 11° de la LCE : "toute personne ayant introduit une notification conformément à l'article 9". Cette version offre toutefois une possibilité d'échappatoire : les opérateurs qui ne font pas de notification ne seraient ainsi pas soumis à la réglementation en matière de rétention de données. D'où l'adaptation de la définition. La Commission n'a pas de remarque à ce sujet.

27. *-(Avis n° 24/2008) - la conservation des données pour les finalités prévues à l'article 2, § 1, b) et c) (les appels malveillants vers les services d'urgence et le Service de médiation pour les télécommunications) doit être retirée de l'application de l'avant-projet de loi, et qu'il faut prévoir à cet égard une réglementation distincte.*

28. Dans sa version modifiée, l'avant-projet de loi prévoit à l'article 3, § 1, b) et c) : "*la répression d'appels malveillants vers les services d'urgence, visée à l'article 107 de cette loi*" et "la recherche par le Service de médiation pour les télécommunications de l'identité des *personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43bis, § 3, 7° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques*". Le demandeur estime que les deux finalités doivent être maintenues en vertu de l'article 126 de la LCE. Toutefois,

compte tenu des remarques de la Commission et par analogie avec la modification apportée au point a), il a été précisé de quels articles de loi il s'agissait, offrant ainsi davantage de clarté quant à l'application de l'obligation de conservation et aux modalités d'accès aux données, dont on reparlera plus en détail ci-après au point 32.

29. *-(Avis n° 24/2008) - des exceptions ne peuvent pas être régies par un arrêté royal, mais que le principe de base de l'exception doit au moins être réglé dans la loi. La notion de "circonstances particulières" de l'article 2, § 2 de l'avant-projet de loi est trop vague.*

30. La Directive permet dans certains cas de dépasser la durée de conservation maximale prévue (24 mois). Cette possibilité est prévue dans l'avant-projet de loi à l'article 3, § 2 : "(…) *dans les circonstances exceptionnelles comme visées à l'article 4, § 2, le Roi peut* (…) *fixer un délai de conservation des données supérieur à 24 mois*". Dans la version précédente du projet de loi, seule l'expression "circonstances exceptionnelles" était mentionnée, laquelle n'offrait pas suffisamment de sécurité juridique aux yeux de la Commission, était extrêmement vague et de ce fait susceptible d'une interprétation trop large. Pour répondre à cette préoccupation, le demandeur a prévu de se référer, dans une définition, à l'article 4, § 1 de la LCE : les circonstances exceptionnelles sont donc ici "*lorsque la sécurité publique, la santé publique, l'ordre public ou la défense du Royaume l'exigent*". La Commission prend note de cette définition et demande que le demandeur donne, dans l'Exposé des motifs, les exemples utiles de ce que l'on entend par là. Ces exemples devraient être suffisamment importants.

31. *-(Avis n° 24/2008) - la désignation des personnes ou instances qui ont accès aux données conservées via la Cellule de coordination de la Justice doit être faite explicitement dans l'avant-projet de loi, en mentionnant également qui a accès à quelles données.*

32. Comme indiqué ci-dessus aux points 13 et 19, le renvoi explicite aux dispositions légales pertinentes dans l'avant-projet de loi (par exemple les articles 46*bis* et 88*bis* du Code pénal et l'article 107 de la LCE) doit fournir plus de clarté selon le demandeur, notamment en matière d'accès. Ainsi, l'article 46*bis* du Code pénal prévoit, d'après le demandeur, une compétence du procureur du Roi et l'article 88*bis* du Code d'instruction criminelle la compétence du juge d'instruction. Dans les deux cas, les mesures doivent être motivées par écrit et il y a donc des garanties que quiconque ne puisse pas accéder aux données conservées pour quelque raison ou infraction que ce soit.

33. *-(Avis n° 24/2008) - le non-respect des exigences en matière d'accès et d'utilisation des données collectées doit être sanctionné.*

34. Suite à sa remarque précédente (désigner explicitement qui a accès à quelles données), la Commission a demandé de criminaliser le non-respect des exigences d'accès et d'utilisation. Le demandeur y a satisfait, étant donné que l'avant-projet de loi prévoit désormais ce qui suit à l'article 4 : "*Est puni d'une amende de 50 à 50 000 EUR et d'une peine d'emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui, sachant qu'elle n'y est pas autorisée, accède aux données visées à l'article 126 ou fait usage des données à des fins autres que celles prévues dans cet article".* Cette criminalisation supplémentaire vise plus particulièrement à criminaliser l'utilisation des données conservées pour une finalité autre que celle prévue légalement. Ainsi, d'après l'Exposé des motifs, les autorités judiciaires peuvent également contrôler le bon déroulement de la conservation des données. La Commission recommande d'adapter le texte comme suit afin d'éviter les malentendus : "(…) *sachant qu'elle n'y est pas autorisée, accède aux données visées à l'article 126 ou,* ***si elle est autorisée à y accéder****, fait usage des données à des fins autres que celles prévues à* ***l'article 126****".*

D.2. LE PROJET D'ARRÊTÉ ROYAL RELATIF À L'OBLIGATION DE COLLABORATION

35. *- (Avis n° 29/2008) le projet d'arrêté royal fixant les données à conserver en application de l'article 126 LCE, ainsi que les conditions et la durée de conservation de ces données (arrêté royal "conservation"), pour lequel la Commission a émis un avis défavorable, est intimement lié au projet d'Arrêté Royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques (arrêté royal "collaboration") ;*

36. À ce sujet, le demandeur a communiqué à la Commission que si le lien étroit entre les deux arrêtés royaux était clair, il n'était quand même pas recommandé de régler les deux matières dans un seul texte. Avant tout, les deux textes ont une base légale différente (LCE et Code d'instruction criminelle). Le demandeur souligne également que l'obligation de conservation des données et l'obligation de collaboration ne se chevauchent pas forcément intégralement (différence du concept "opérateur" dans la LCE et le Code d'instruction criminelle). L'obligation de collaboration est plus large. Par ailleurs, l'obligation de collaboration est déjà régie dans l'arrêté royal du 9 janvier 2003, qui est abrogé par le deuxième projet d'arrêté royal.

37. *-(Avis n° 29/2008) les mêmes défauts, pointés dans l'avis 24/2008, entachent l'arrêté royal "collaboration", à savoir l'application des règles de collaboration aux fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6 LCE, ainsi que l'absence d'une sanction attachée au non-respect des exigences en matière d'accès et d'utilisation des données ;*

38. Dans le deuxième projet d'arrêté royal, la définition du secteur Internet est maintenue. Conformément au Rapport au Roi, il faut tenir compte, en ce qui concerne cette définition, de l'article 2 de la LCE, qui définit les notions de "point de terminaison du réseau", "utilisateur", "utilisateur final" et "service de communications électroniques". L'on a tenté de suivre autant que possible la terminologie de cette loi. En principe, il faut entendre par là tous les niveaux du secteur Internet : les opérateurs qui mettent leur infrastructure à disposition pour le transport des signaux Internet (connexion physique), les fournisseurs d'accès à Internet qui donnent accès à Internet à l'utilisateur final et les fournisseurs de services Internet qui offrent sur Internet des services de communication. Le demandeur a pu confirmer à la Commission que l'on n'entendait pas par là les fournisseurs et revendeurs prévus à l'article 9, §§ 5 et 6 de la LCE. Un règlement distinct sera prévu pour ces derniers.

39. Dans son avis, la Commission avait proposé de souligner dans le texte de l'article 2, § 2, premier alinéa du projet d'arrêté royal que les membres du personnel et les préposés des opérateurs, en vertu des articles 46*bis*, § 2, troisième alinéa, 88*bis*, § 2, deuxième alinéa et 90*quater*, deuxième alinéa du Code d'instruction criminelle, devaient respecter le secret professionnel conformément à l'article 458 du Code pénal. Le Rapport au Roi relatif au deuxième projet d'arrêté royal mentionne ce qui suit dans le commentaire de l'article 2 : "*Il est extrêmement important que les membres du personnel de la Cellule de coordination soient fiables. Ils doivent en effet traiter des informations sensibles. C'est important également dès lors que l'article 90quater, § 2, alinéa 2, du Code d'instruction criminelle prévoit des sanctions pénales en cas de violation de l'obligation de secret, conformément à l'article 458 du Code pénal*." La Commission recommande de se référer également dans ce cadre aux articles 46*bis* et 88*bis* du Code d'instruction criminelle.

40. *-(Avis n° 29/2008) le service NTSU-CTIF, désigné pour accéder directement à ces bases de données, doit être, vu le principe de légalité, plus clairement défini ;*

41. L'article 1er du deuxième projet d'arrêté royal définit le service NTSU-CTIF : le système central d'interception technique du service de police intégrée, structuré à deux niveaux. Le demandeur a notamment transmis à la Commission un organigramme afin de mieux comprendre ce service. Selon la Commission, il est recommandé de rendre ces informations

publiques, de sorte que quiconque puisse retrouver ce service au sein des services de la police fédérale.

42. *-(Avis n° 29/2008) le changement de pratique, à savoir l'accès direct, par un service de police, aux bases de données "clients" des opérateurs télécom doit être davantage justifié, et si elle s'impose, cette pratique devrait être entourée de garanties (règles d'accès, log, journalisation des accès et consultations, accès authentifié,…) dans le corps du texte du projet d'arrêté royal ;*

43. Le deuxième projet d'arrêté royal fait une distinction entre d'une part les opérateurs à qui une capacité de numérotation a été attribuée dans le plan national de numérotation et d'autre part les autres opérateurs. Ce n'est que dans le premier cas que les opérateurs sont tenus d'accorder au service NTSU-CTIF un accès à la banque de données contenant le fichier clients. Conformément à l'article 3, cet accès sera implémenté par une application Internet sécurisée, sur la base d'une requête électronique à laquelle l'opérateur sera tenu de répondre de manière automatique. Le service NTSU-CTIF fixe les détails techniques complémentaires de cette procédure. Le service NTSU-CTIF conserve un log et fait un journal de chaque accès et consultation de la banque de données. Conformément au Rapport au Roi, cela ne signifie pas pour autant que le service NTSU-CTIF pourra consulter sans condition cette base de données à n'importe quel moment. Il y a lieu bien entendu d'observer les règles du Code d'instruction criminelle et ce n'est qu'à la réception de la requête visée à l'article 466*bis* par le service NTSU-CTIF qu'il pourra consulter la base de données. Les opérateurs peuvent par ailleurs voir quand ce service accède aux fichiers des clients et dénoncer l'accès qui ne s'effectue pas sur la base de la procédure décrite dans l'arrêté royal : une requête électronique du service NTSU-CTIF est requise.

44. D'après le demandeur, le but était que le NTSU/CTIF puisse consulter plus facilement un fichier reprenant les données des clients des opérateurs, ce en particulier grâce à une requête traitée électroniquement par le NTSU/CTIF (et plus des consultations manuelles ou téléphoniques et encore moins par fax). L'automatisation des processus accroît la rapidité avec laquelle les informations sont mises à disposition des demandeurs, réduit la charge de travail manuel et les risques d'erreurs lors du traitement (faute de frappe par exemple) et permet le contrôle a posteriori de toutes les requêtes introduites (en particulier grâce à un logging). Toujours d'après le demandeur, ce processus automatisé est plus respectueux de la vie privée que les consultations manuelles, téléphoniques ou par fax, qui ne permettent pas par exemple le contrôle via des loggings, et n'empêchent pas le risque de perte de données et les éventuelles fautes lors du traitement de données. Il est également important que seules les requêtes passent via le NTSU/CTIF et y soient contrôlées. Les réponses sont

par contre transmises directement au demandeur initial sans passer de nouveau par le NTSU/CTIF. C'est également favorable à la protection de la vie privée. D'après le demandeur, le NTSU prend deux types de mesures pour protéger les données relatives aux mesures pour lesquelles il est responsable :

- mesures physiques : accès limité, accès contrôlé par un badge, bâtiment protégé physiquement, occupation permanente, caméras, logging des personnes qui entrent et sortent ;

- mesures logicielles : octroi de droits sur la base de profils spécifiques, contrôle de logging de chaque acte posé sur le réseau, accès octroyé par dossier (pas d'accès général) lorsque le nom de la personne concernée est mentionné spécifiquement sur le réquisitoire du juge d'instruction, transfert sécurisé.

45. La Commission propose d'ajouter le passage suivant à l'article 3, premier alinéa du deuxième projet d'arrêté royal : "(…) Le service NTSU-CTIF conserve un log et fait un journal de chaque accès et consultation de la banque de données. *Il prend également les mesures physiques et logicielles nécessaires pour prévoir un niveau de protection adéquat*."

46. *-(Avis n° 29/2008) le principe de proportionnalité n'est pas respecté en ce qui concerne la transmission des coordonnées personnelles des membres des Cellules Coordination de la Justice.*

47. Le deuxième projet d'arrêté royal prévoit à l'article 2, § 3 qu'un gsm de service est mis à la disposition de la Cellule de coordination. Il a ainsi été satisfait à la remarque formulée par la Commission dans son avis, et la mise à disposition des données privées des membres de la cellule a été supprimée.

PAR CES MOTIFS,

la Commission émet un avis *favorable*, uniquement à la condition qu'il soit tenu compte des remarques formulées concernant :

- la détermination de la durée de conservation de 12 mois dans l'avant-projet de loi (point 8) ;
- l'évaluation parlementaire de l'avant-projet de loi et du projet d'arrêté royal ainsi que le rapport annuel au parlement par le ministre compétent (point 9) ;
- la durée de conservation de 12 mois et la destruction immédiate des données conservées au terme de ce délai (points 19 à 22 inclus) ;
- l'utilisation du terme 'public' pour un service d'accès à Internet, un service d'e-mail et un service de téléphonie par Internet (point 25) ;
- la définition de la notion de 'circonstances exceptionnelles' (point 30) ;

- l'incrimination des exigences d'accès et d'utilisation (point 34) ;
- le service NTSU-CTIF (points 41-45).

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere

Advies nr 20/2009 van 1 juli 2009

Betreft: Adviesaanvraag inzake het voorontwerp van wet en het ontwerp van koninklijk besluit inzake dataretentie, en het ontwerp van koninklijk besluit inzake de medewerkingsplicht (A/09/012)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de Minister van Justitie, dhr. Stefaan De Clerck ontvangen op 23/04/2009;

Gelet op het verslag van dhr. Voorzitter;

Brengt op 1 juli 2009 het volgend advies uit:

A. INLEIDING

1. Op 23 april 2009 heeft de Minister van Justitie de Commissie verzocht om bij hoogdringendheid advies uit te brengen inzake het voorontwerp van wet en het ontwerp van koninklijk besluit inzake dataretentie (hierna 'het voorontwerp van wet en het ontwerp kb'), en het ontwerp van koninklijk besluit inzake de medewerkingsplicht (hierna 'het tweede ontwerp kb).

2. De hoogdringendheid wordt afdoende gemotiveerd. De Commissie zal hiernavolgend dan ook bij hoogdringendheid advies uitbrengen inzake de voormelde ontwerpen, rekening houdend met de informatie waarover ze beschikt.

B. TOEPASSELIJKE WETGEVING

3. Vooreerst kan worden verwezen naar de Richtlijn 2006/24/EG. Aangezien er persoonsgegevens worden verwerkt is verder de WVP van toepassing, evenals de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna 'WEC'). Tenslotte dient het koninklijk besluit vermeld van 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid, en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109ter, E, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (hierna 'het kb van 9 januari 2003').

C. VOORGESCHIEDENIS

4. De Commissie bracht reeds op 2 juli 2008 advies uit (advies nr. 24/2008) betreffende het voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, en betreffende het ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van bewaring van de gegevens. Haar toenmalig advies was ongunstig, vandaar dat de Minister van Justitie heden het aangepaste voorontwerp van wet en ontwerp van kb aan de Commissie voorlegt.

5. Op 3 september 2008 verleende de Commissie haar advies (advies nr. 29/2008) over het ontwerp van koninklijk besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie. Ook dit advies was ongunstig, en dus wordt heden ook het tweede ontwerp kb opnieuw aan de Commissie voorgelegd.

D. ONDERZOEK VAN DE ADVIESAANVRAAG

6. Hiernavolgend zal de Commissie nagaan in hoeverre aan haar opmerkingen, zoals weergegeven in de conclusies van de voormelde adviezen, door de voorliggende ontwerpen wordt tegemoetgekomen. Gemakkelijkheidshalve wordt hierna dan ook de volgorde van de opmerkingen in de adviezen aangehouden, met voor elk punt de eventueel door de aanvrager aangebrachte wijzigingen.

D.1. VOORONTWERP VAN WET EN HET ONTWERP KB INZAKE DATARETENTIE

7. *- (Advies nr. 24/2008) gelet op het legaliteitsbeginsel, de essentiële elementen inzake de bewaring van gegevens in het voorontwerp van wet duidelijker dienen te worden bepaald. In dit opzicht zou de bewaarduur in het voorontwerp van wet moeten worden bepaald, en eveneens de te bewaren gegevens.*

8. Voor wat de *bewaarduur* betreft, werden er geen wijzigingen aangebracht aan het voorontwerp van wet : de bewaarduur mag niet korter zijn dan 6 maanden, en niet langer dan 24 maanden. Het is aan de Koning om de exacte bewaarduur vast te leggen. De Commissie blijft bij haar standpunt dat de exacte bewaarduur in het voorontwerp van wet moet worden bepaald, gezien het belang van de materie. Wat de bewaarduur betreft, meent zij dat een bewaarduur van 12 maanden zou moeten volstaan, cfr. infra, punten 19 tot en met 22. Tevens zou in het voorontwerp van wet moeten worden bepaald dat de bewaarde gegevens na het verstrijken van deze termijn onverwijld dienen te worden vernietigd.

9. In de Memorie van Toelichting maakt men bij de bespreking van artikel 3 van het voorontwerp van wet evenwel melding van een belangrijke wijziging. Deze bestaat erin dat er twee jaar na de inwerkingtreding van het Koninklijk Besluit, een evaluatie zal worden uitgevoerd over de toepassing ervan, zodat kan bekeken worden in hoeverre de vastgelegde termijnen noodzakelijk en/of voldoende zijn voor de behoeften van de gerechtelijke autoriteiten. De verdienste van deze bepaling bestaat erin dat men de mogelijkheid voorziet om de bewaartermijn aan te passen, desgevallend naar onder toe, indien deze niet meer met de werkelijkheid zou stroken. Zoals hierboven uiteengezet, meent de Commissie dat de bewaarduur in de wet dient te worden bepaald. Daarbij zou dan tevens in de wet zelf, en niet enkel in de memorie van toelichting, moeten worden uitgeschreven dat er een evaluatie zal plaatsvinden, en op welke wijze. Deze evaluatie zou volgens de Commissie tweevoudig moeten zijn : *enerzijds* een grote eenmalige evaluatie, welk idealiter zou kunnen doorgaan na de voorziene Europese evaluatie van de Richtlijn 2006/24, waarbij men definitief de

criteria en de bewaarduur zou moeten bepalen. Ten titel van voorbeeld kan hieromtrent worden verwezen naar de wet houdende oprichting en organisatie van het e-Health platform, meer bepaald artikel 36, waar sprake is van een evaluatie na twee jaar. *Anderzijds* zou men moeten voorzien in een jaarlijkse rapportering door de verantwoordelijke minister aan het parlement, naar analogie met hetgeen wordt bepaald in artikel 90 decies van het wetboek van strafvordering. Eventueel kan de jaarlijkse rapportering inzake dataretentie worden opgenomen in voormelde rapportering overeenkomstig artikel 90 decies van het wetboek van strafvordering. De Commissie zal voormelde evaluatie en rapportering nauwgezet opvolgen.

10. De *te bewaren gegevens* worden nu als volgt gedefinieerd in het voorontwerp van wet (artikel 3, §1) : '…bewaren de operatoren die een openbare vaste telefoniedienst, een openbare mobiele telefoniedienst, een internettoegangsdienst, een emaildienst, of een internettelefoniedienst aanbieden, de verkeers –en localisatiegegevens en de gegevens voor identificatie van de eindgebruikers die door hen worden gegenereerd of verwerkt bij het aanbieden van hun respectievelijke elektronische communicatienetwerken –en diensten…' . Overeenkomstig de Memorie van Toelichting (algemene gedeelte, alinea's 3 en 4) stelt de Richtlijn 2006/24 de lijst op van de te bewaren gegevens, onderverdeeld in categorieën ; identificatie van de bron van een communicatie, identificatie van de bestemming van een communicatie, bepaling van de datum, het tijdstip en de duur van een communicatie, bepaling van het type van communicatie, alsook van de gebruikte apparatuur en de locatie van de gebruikte apparatuur. Het voorontwerp van wet groepeert deze categorieën van gegevens onder de noemers "verkeers –en locatiegegevens" en "gegevens voor de identificatie van de eindgebruikers". Deze worden dan verder uitgewerkt in het ontwerp kb. Op die manier worden de artikelen 88bis en 46bis van het Wetboek van Strafvordering, en de terminologie van de wet betreffende de elektronische communicatie gerespecteerd. Verder stelt de Memorie van Toelichting dat de Richtlijn tevens een aantal subcategorieën creëert binnen deze verschillende gegevenscategorieën, naargelang van de aard van de netwerken en diensten die betrokken zijn bij een communicatie : vaste telefonie, mobiele telefonie, internettelefonie, internettoegang en email over het internet. Deze categorieën worden ook uitdrukkelijk in het ontwerp van artikel 126 opgesomd, zodat duidelijk is welke operatoren onderworpen zijn aan de verplichting tot bewaring van de hierboven vermelde gegevens.

11. De Memorie van Toelichting bepaalt tenslotte (drie laatste alinea's van het algemene gedeelte) dat de Richtlijn 2006/24 het algemene kader voor gegevensbewaring betreffende elektronische communicatie vastlegt. Slechts vier categorieën van elektronische communicatiediensten worden geviseerd : vaste telefonie, mobiele telefonie,

internettoegang en elektronisch berichtenverkeer en telefonie via internet. De communicatietechnologie en de technische protocollen die deze elektronische communicatie regelen evolueren snel, voornamelijk voor wat betreft de vormen van telefonie over internet. Opdat het wettelijk kader een effectief instrument voor de bestrijding van criminaliteit zou zijn, is het noodzakelijk dat dit kader de evolutie van deze technische protocollen kan volgen. Een Koninklijk Besluit laat dan ook een snelle update van het wettelijke kader toe.

12. De Commissie stelt vast dat in het voorontwerp van wet de categorieën van te bewaren gegevens duidelijker worden gedefinieerd. De uitwerking ervan via kb, kan worden gevolgd, ermee rekening houdend dat de werking van het voorontwerp van wet en het ontwerp kb zullen worden geëvalueerd (cfr. supra, punt 9), en dat een eventuele wijziging van het kb moet worden vastgesteld na overleg in de Ministerraad, en na advies van de Commissie en van het Instituut.

13. *- (Advies nr. 24/2008) de noodzaak voor het bewaren van bepaalde gegevens, die niet voorzien zijn in de richtlijn, dient gerechtvaardigd overeenkomstig de principes van artikel 8 EVRM.*

14. Het verslag aan de Koning bij het ontwerp kb stelt dat het minimale kader voor de bewaring van gegevens op het vlak van elektronische communicatie, zoals vastgelegd door de Richtlijn, niet noodzakelijk aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de opsporing en de vervolging van strafbare feiten voldoet. Zo ontbreken in de door de Richtlijn opgestelde lijst bijvoorbeeld bepaalde gegevens die onmisbaar zijn bij de identificatie van personen betrokken bij een relevante communicatie in het kader van een strafrechtelijk onderzoek - zoals gegevens inzake betaling. In het commentaar bij de artikelen van het verslag aan de Koning wordt vervolgens per categorie van gegevens verduidelijkt welke gegevens bijkomend dienen te worden bewaard, en waarom. De aanvrager heeft hieromtrent nog bijkomende informatie aan de Commissie verschaft. Op basis van de voormelde gegevens, meent de Commissie dan ook te kunnen besluiten tot het gerechtvaardigd karakter van de voorgenomen verwerking. Dit evenwel op voorwaarde dat binnen afzienbare tijd een evaluatie doorgaat (cfr. supra), waarbij de noodzaak voor de verwerking van deze gegevens opnieuw dient te worden geëvalueerd.

15. - (Advies nr. 24/2008) het voorontwerp van wet zou dienen te verduidelijken voor het onderzoek, de vervolging en de beteugeling van welke (zware) criminele feiten de bewaarde gegevens kunnen worden gebruikt.

16. Het voorontwerp van wet voorziet in haar gewijzigde versie onder artikel 3, §1, a) 'het onderzoek, de opsporing en de vervolging van strafbare feiten *zoals bedoeld in de artikelen 46 bis en 88 bis van het Wetboek van Strafvordering'.* De aanvrager heeft aan de Commissie verduidelijkt dat door deze toevoeging aan haar opmerking werd voldaan. Artikel 46bis voorziet namelijk in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot telecommunicatiediensten, artikel 88bis voorziet in de opsporing en lokalisatie van communicatie door de onderzoeksrechter. Het is met het oog op de praktische toepasbaarheid van deze artikelen dat de beoogde identificatiegegevens, oproepgegevens en locatiegegevens bewaard dienen te worden. Beide artikelen voorzien ook in voorwaarden zoals subsidiariteit en proportionaliteit van de maatregel. Artikel 46bis is een bevoegdheid van de procureur des Konings, artikel 88bis van de onderzoeksrechter. In beide gevallen moeten de maatregelen schriftelijk gemotiveerd worden, en zijn er dus garanties dat niet om het even wie toegang kan hebben tot de bewaarde gegevens voor om het even welke reden of misdrijf. Beide artikelen voorzien dan wel niet in een lijst van misdrijven, maar er is een zekere drempel ingebouwd doordat deze artikelen de maatregelen beperken tot wanbedrijven en misdaden. Een exhaustieve opsomming van de zware misdrijven is volgens de aanvrager niet haalbaar, gelet op de diverse bijzondere strafbepalingen. Bovendien zou er telkens een wetswijziging nodig zijn indien een misdrijf zou moeten worden toegevoegd.

17. De Commissie kan met bovenstaande argumentatie instemmen, temeer gelet op de aangebrachte verduidelijking door expliciet te verwijzen naar de artikelen 46bis en 88bis van het Wetboek van Strafvordering. Artikel 46 bis voorziet in een uitdrukkelijke motivering door de procureur des Konings, waarbij deze motivering de proportionaliteit moet weerspiegelen met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad. Artikel 88 bis voorziet eenzelfde bepaling voor de onderzoeksrechter. Zij brengt tenslotte in herinnering dat de door de magistraat opgevraagde gegevens, welke niet dienstig zijn voor het onderzoek, dienen te worden vernietigd.

18. -(Advies nr. 24/2008) de bewaarduur van 24 maanden meer dient te worden gefundeerd en gerechtvaardigd, en desgevallend heroverwogen met het oog op de voorziene bewaartermijnen in de meeste andere Europese landen.

19. Het ontwerp kb heeft de bewaarduur van 24 maanden uit het eerste ontwerp overgenomen. Het Verslag aan de Koning bepaalt daaromtrent dat op basis van de praktijk die is waargenomen bij de verschillende gedecentraliseerde politiediensten en bij het federale parket inzake verzoeken om inlichtingen aan de operatoren en aan de aanbieders van

netwerken of diensten voor elektronische communicatie, mag worden aangenomen dat een uniforme termijn van 24 maanden voor de bewaring van de verschillende, in artikel 126 van de wet bedoelde soorten van gegevens, het meest geschikte mechanisme vormt. De aanvrager heeft aan de Commissie voorbeelden verstrekt van situaties waaruit zou moeten blijken dat een termijn van 24 maanden gerechtvaardigd is, en dat zulks beantwoordt aan een reële behoefte bij de politie en bij justitie.

20. De aanvrager heeft de Commissie tevens ingelicht over een studie van het BIPT d.d. juli 2008 aangaande de bewaartermijnen in het buitenland. Hieruit blijkt dat verschillende landen (waaronder Italië, Slovenië, Ierland, Portugal, Nederland) ook een lange termijn (18 tot 24 maanden) zouden voorzien. Andere landen (waaronder Frankrijk, Duitsland en het VK) zouden voor een kortere termijn (12 maanden) opteren. Dit zou volgens de aanvrager veeleer ingegeven zijn omwille van economische en financiële redenen (kosten voor de operatoren).

21. De Commissie mocht eveneens kennis nemen van de standpunten van de telecom industrie (ISPA). Uit de door hen meegedeelde cijfers (studie d.d. oktober 2008) blijkt dat de voorziene duur in de meeste landen 12 maanden bedraagt (Denemarken, Frankrijk, Finland, Spanje, Portugal), Duitsland heeft een periode van 6-7 maanden bepaalt. In andere landen bedraagt de voorgestelde termijn ook vaak 12 maanden (VK, Nederland, Zweden), dan wel 6 maanden (Oostenrijk, Luxemburg). Verder brengen zij statistieken bij waaruit zou moeten blijken dat de meeste aanvragen door justitie bij de Belgische telecomoperatoren gebeuren binnen de zes maanden na de aanvang van het bewaren van gegevens, en dat het aantal aanvragen na 12 maanden niet meer dan 5% van het totaal aantal aanvragen bedraagt.

22. De Commissie heeft nota genomen van de voormelde argumenten. Vanuit het standpunt van justitie is het uiteraard zo dat een bewaarduur van 24 maanden noodzakelijk is. De industrie wil daarentegen om diverse redenen deze bewaarduur zoveel mogelijk beperkt zien. De Commissie meent dat het in deze discussie niet onbelangrijk is om te kijken naar de initiële doelstelling van de richtlijn, welke bestaat in de *harmonisatie* van de wetgeving in de lidstaten met betrekking tot het bewaren van telecommunicatiegegevens door operatoren. In dit opzicht lijkt de termijn van 24 maanden op dit moment overdreven te zijn, gezien de in onze buurlanden (Frankrijk, Nederland, Duitsland, Luxemburg) gangbare termijn van 12 maanden of minder. De commissie meent dan ook dat een bewaartermijn van 12 maanden momenteel voldoende is. In dit opzicht is ook de voorgestelde evaluatie van belang, waarbij de termijn in plus of in min zou kunnen worden aangepast, indien daartoe noodzaak zou bestaan. Tenslotte zou het voorontwerp van wet ook expliciet moeten voorzien dat na het

verstrijken van deze bewaarduur, de gegevens onverwijld moeten worden vernietigd door de operator.

23. -(Advies nr. 24/2008) de toepassing van het voorontwerp van wet en ontwerp kb op de aanbieders en doorverkopers voorzien in artikel 9, §§ 5 en 6 dient te worden herbekeken, en voor hen eventueel in een andere bepaling te voorzien.

24. In de huidige versie van het voorontwerp van wet is er geen sprake meer van de aanbieders en doorverkopers voorzien in artikel 9, §§5 en 6 WEC. De Commissie had hierop aangedrongen in haar voormeld advies, aangezien onder aanbieders en doorverkopers bijvoorbeeld moet worden begrepen het interne netwerk van een bedrijvengroep. Deze worden evenwel niet geviseerd door de richtlijn 2006/24/EG, welke overeenkomstig artikel 3 enkel en alleen van toepassing is op aanbieders van openbare elektronische communicatiediensten of een openbaar communicatienetwerk bij het leveren van de betreffende communicatiediensten. Vandaar de vraag vanwege de Commissie om de aanbieders en doorverkopers te schrappen.

25. Gelet op het feit dat artikel 3 van de richtlijn 2006/24 voorziet dat de richtlijn enkel en alleen van toepassing is op aanbieders van openbare elektronische communicatiediensten of een openbaar communicatienetwerk bij het leveren van de betreffende communicatiediensten, dient artikel 3, §1 van het voorontwerp van wet te worden aangepast. Het woord *'openbare'* moet in voormeld artikel niet enkel worden gebruikt voor een vaste telefoniedienst en mobiele telefoniedienst, maar eveneens voor een internettoegangsdienst, emaildienst, en een internettelefoniedienst. Dit moet dus worden : een openbare internettoegangsdienst, een openbare emaildienst, en een openbare internettelefoniedienst.

26. Het voorontwerp van wet voorziet onder artikel 2 in een aanpassing van het begrip operator in de WEC (artikel 2, 11°) : 'een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9'. Huidige versie artikel 2, 11° WEC : 'een persoon die een kennisgeving heeft ingediend overeenkomstig artikel 9'. Deze versie biedt evenwel een ontsnappingsmogelijkheid : operatoren die geen kennisgeving doen, zouden zo niet onder de regelgeving inzake dataretentie vallen. Vandaar de aanpassing van de definitie. De Commissie heeft hieromtrent geen opmerkingen.

27. -(Advies nr. 24/2008) Het bewaren van de gegevens voor de doeleinden voorzien in artikel 2, §1, b) en c) (de kwaadwillige oproepen naar de nooddiensten en de ombudsdienst voor telecommunicatie) uit de toepassing van het voorontwerp van wet dienen gehaald, en hieromtrent in een separate regelgeving moet worden voorzien.

28. Het voorontwerp van wet voorziet in haar gewijzigde versie onder artikel 3, §1, b) en c) : 'de beteugeling van kwaadwillige oproepen naar de nooddiensten, *zoals bedoeld in artikel 107 van deze wet'* en 'het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk –of dienst, *zoals bedoeld in artikel 43bis, §3, 7° van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven'.* De aanvrager meent dat beide doeleinden onder artikel 126 WEC dienen te worden behouden. Evenwel werd er – rekening houdend met de opmerkingen van de Commissie, en naar analogie met de wijziging aangebracht voor punt a)- verduidelijkt over welke wetsartikelen het gaat. Hierdoor is er meer klaarheid inzake de toepassing van de bewaarplicht, en de modaliteiten van de toegang tot de gegevens, waarover meer infra onder punt 32.

29. *-(Advies nr. 24/2008) uitzonderingen niet kunnen worden geregeld via een koninklijk besluit, doch dat minstens het basisprincipe van de uitzondering in de wet dient te worden geregeld. Het begrip 'uitzonderlijke omstandigheden' in artikel 2, §2 van het voorontwerp van wet is te vaag.*

30. De Richtlijn laat toe om in bepaalde gevallen de voorziene maximum bewaarduur (24 maanden) te overschrijden. Deze mogelijkheid voorziet het voorontwerp van wet in artikel 3, §2 : '..de Koning kan in uitzonderlijke omstandigheden *zoals bedoeld in artikel 4, §1, …* een bewaringstermijn vastleggen die langer is dan 24 maanden.' In de vorige versie van het wetsontwerp werd enkel de term "uitzonderlijke omstandigheden" vermeld, welke volgens de Commissie niet voldoende rechtszekerheid bood, uitermate vaag was en hierdoor te ruim interpreteerbaar. Om aan deze bezorgdheid tegemoet te komen werd door de aanvrager voorzien in een definitie door te verwijzen naar artikel 4, §1 van de WEC: de uitzonderlijke omstandigheden zijn hier dus "w*anneer de openbare veiligheid, de volksgezondheid, de openbare orde of de verdediging van het Rijk dit eisen".* De Commissie neemt nota van deze definitie, en vraagt dat door de aanvrager in de memorie van toelichting de nodige voorbeelden worden aangebracht over wat men hieronder verstaat. Deze voorbeelden zouden voldoende zwaarwegend moeten zijn.

31. *-(Advies nr. 24/2008) de toewijzing van de personen of instanties die toegang hebben tot de bewaarde gegevens via de coördinatiecel justitie expliciet moet gebeuren in het voorontwerp van wet , waarbij tevens dient aangegeven wie toegang heeft tot welke gegevens.*

32. Zoals hierboven aangegeven onder de punten 16 en 28, dient volgens de aanvrager de expliciete verwijzing naar de relevante wettelijke bepalingen in het voorontwerp van wet

(bv. artikelen 46bis en 88bis Sv., en 107 WEC) om meer duidelijkheid te verschaffen, ondermeer inzake de toegang. Zo voorziet volgens de aanvrager artikel 46bis van het Wetboek van Strafvordering in een bevoegdheid van de procureur des Konings, en artikel 88bis van het Wetboek van Strafvordering in de bevoegdheid van de onderzoeksrechter. In beide gevallen moeten de maatregelen schriftelijk gemotiveerd worden, en zijn er dus garanties dat niet om het even wie toegang kan hebben tot de bewaarde gegevens voor om het even welke reden of misdrijf.

33. -(Advies nr. 24/2008) de niet naleving van de vereisten inzake toegang en gebruik van de verzamelde gegevens strafbaar dient gesteld.

34. Aansluitend bij haar vorige opmerking (expliciet aanduiden wie toegang heeft tot de gegevens), vroeg de Commissie om de niet naleving van de toegang -en gebruiksvereisten strafbaar te stellen. De aanvrager is hieraan tegemoet gekomen, aangezien het voorontwerp van wet nu voorziet in artikel 4 dat '*met een geldboete van 50 tot 50.000 € en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen wordt gestraft hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot de gegevens bedoeld in artikel 126 of die gegevens aanwendt voor andere doeleinden dan degene voorzien in dit artikel.'* Deze extra strafbaarstelling is meer bepaald gericht op het strafbaar stellen van de aanwending van de bewaarde gegevens voor andere dan de wettelijk voorziene doeleinden. Hierdoor kunnen overeenkomstig de Memorie van Toelichting ook de gerechtelijke autoriteiten toezicht houden op het goede verloop van de bewaring van de gegevens. De Commissie beveelt aan om de tekst, teneinde misverstanden te vermijden, als volgt aan te passen : '…*terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot de gegevens bedoeld in artikel 126 of* ***indien hij gerechtigd is zich er toegang toe te verschaffen,*** *die gegevens aanwendt voor andere doeleinden dan degene voorzien in* ***artikel 126****.'*

D.2. HET ONTWERP VAN KB INZAKE DE MEDEWERKINGSPLICHT

35. -(Advies nr. 29/2008)het ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens in toepassing van artikel 126 WEC, alsook de voorwaarden en de duur van de bewaring van de gegevens ("kb bewaring"), waarover de Commissie een ongunstig advies uitbracht, nauw verwant is met het ontwerp van koninklijk besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie ("kb medewerking");

36. De aanvrager kon hieromtrent aan de Commissie meedelen dat daar waar de nauwe band tussen beide Koninklijke besluiten duidelijk is, het toch niet aangewezen is om beide materies in één tekst te regelen. Eerst en vooral hebben beide teksten een verschillende wettelijke basis (WEC en het Wetboek van Strafvordering). Er wordt door de aanvrager ook op gewezen dat de verplichting tot dataretentie en de medewerkingsplicht elkaar niet noodzakelijk volledig overlappen (verschil begrip 'operator' in de WEC en het Wb van Sv.).De medewerkingsplicht is ruimer. Daarnaast is de medewerkingsplicht al geregeld in het kb van 9 januari 2003, dat door het tweede ontwerp kb opgeheven wordt.

37. -(Advies nr. 29/2008)in het "kb medewerking" dezelfde gebreken voorkomen die werden aangestipt in het advies 24/2008, nl. de toepassing van de regels voor medewerking van de aanbieders en doorverkopers, bedoeld in artikel 9, §§5 en 6 van de WEC, evenals het feit dat er geen strafmaatregel werd gekoppeld aan de niet-naleving van de vereisten inzake toegang tot en gebruik van de gegevens;

38. In het tweede ontwerp kb wordt de definitie van internetsector gehandhaafd. Overeenkomstig het verslag aan de Koning dient voor wat deze definitie betreft rekening gehouden met artikel 2 van de WEC, dat de begrippen "netwerkaansluitpunt", "gebruiker", "eindgebruiker", en "elektronische communicatiedienst" definieert. Er werd zoveel mogelijk getracht om aan te sluiten bij de terminologie van deze wet. In principe dienen alle niveaus van de internetsector hieronder begrepen te worden : zowel de operatoren die hun infrastructuur ter beschikking stellen voor het transport van de internetsignalen (fysieke connectie), de internet-toegangsleveranciers die aan de eindgebruiker toegang tot het internet geven, en de internetdienstenleveranciers die over het internet communicatiediensten aanbieden. De aanvrager kon aan de Commissie bevestigen dat hieronder niet de aanbieders en doorverkopers voorzien in artikel 9, §§5 en 6 WEC begrepen worden. Voor hen zal in een aparte regeling worden voorzien.

39. De Commissie had in haar advies voorgesteld om er in de tekst van artikel 2, §2 eerste lid van het ontwerp kb op te wijzen dat de personeelsleden en de aangestelden van de operatoren, krachtens de artikelen 46bis §2 derde lid, 88bis §2 tweede lid en 90 quater 2de lid Wetboek van Strafvordering, het beroepsgeheim moeten eerbiedigen overeenkomstig artikel 458 van het Strafwetboek. Het Verslag aan de Koning inzake het tweede ontwerp kb stelt onder de bespreking van artikel 2 dat 'het uitermate belangrijk is dat de personeelsleden van de Coördinatiecel betrouwbaar zijn, zij dienen immers om te gaan met gevoelige informatie. Dit is ook van belang gezien artikel 90 quater, §2, tweede lid van het Wetboek van Strafvordering strafsancties voorziet voor de schending van de geheimhoudingsplicht overeenkomstig artikel 458 van het Strafwetboek.' De Commissie

beveelt aan om hierbij tevens te verwijzen naar de artikelen 46 bis en 88bis van het Wetboek van Strafvordering.

40. -(Advies nr. 29/2008)gelet op het rechtmatigheidsbeginsel, de dienst NTSU-CTIF die werd aangeduid om rechtstreeks toegang te hebben tot de gegevensbanken, duidelijker gedefinieerd moet worden;

41. Artikel 1 van het tweede ontwerp kb definieert de dienst NTSU-CTIF : de centrale technische interceptiefaciliteit van de geïntegreerde politiedienst, gestructureerd op twee niveaus. Door de aanvrager werd aan de Commissie onder meer een organigram overhandigd teneinde deze dienst beter te kaderen. Het verdient volgens de Commissie aanbeveling om deze informatie publiek beschikbaar te maken, zodat éénieder voormelde dienst kan terugvinden binnen de diensten van de federale politie.

42. -(Advies nr. 29/2008)de verandering van methode, nl. de rechtstreekse toegang door een politiedienst tot de klantenbestanden van de telecomoperatoren uitgebreider verantwoord moet worden, en in geval deze praktijk verplicht wordt, ze gepaard dient te gaan met garanties (toegangsregels, login, toegangs- en consultatiejournaal, geauthenticeerde toegang,...) in het voornaamste tekstgedeelte van het ontwerp van kb;

43. Het tweede ontwerp kb maakt een onderscheid tussen enerzijds operatoren die nummeringscapaciteit toegewezen gekregen hebben in het nationale nummeringsplan, en anderzijds de andere operatoren. Slechts in het eerste geval dienen de operatoren de dienst NTSU-CTIF toegang te verlenen tot de databanken met het klantenbestand. Overeenkomstig artikel 3 zal deze toegang geïmplementeerd worden via een beveiligde internettoepassing, op basis van een elektronisch verzoek waarop de operator gehouden zal zijn om een geautomatiseerd antwoord te verstrekken. De dienst NTSU-CTIF bepaalt de verdere technische details van deze procedure. De dienst bewaart een log en maakt een journaal op van iedere toegang en consultatie van de databank. Overeenkomstig het verslag aan de Koning wil dit echter niet zeggen dat de dienst zomaar op gelijk welk tijdstip deze databank zal kunnen consulteren. De regels van het Wetboek van Strafvordering moeten uiteraard gevolgd worden, en het is slechts als een vordering op basis van artikel 46bis door de dienst NTSU-CTIF ontvangen wordt, dat zij de databank kunnen consulteren. De operatoren kunnen overigens zien wanneer deze dienst toegang neemt tot de klantenbestanden, en dat dan ook aanklagen als dit niet gebeurt op basis van de procedure in het Koninklijk besluit : er dient een elektronisch verzoek van de dienst NTSU-CTIF te zijn.

44. Volgens de aanvrager was het de bedoeling dat de NTSU/CTIF gemakkelijker een bestand met de gegevens van de klanten van de operatoren zou kunnen raadplegen, zulks inzonderheid dankzij een door de NTSU/CTIF elektronisch behandeld verzoek (en geen manuele of telefonische raadplegingen meer en evenmin per fax). De automatisering van de processen verhoogt de snelheid waarmee de informatie ter beschikking wordt gesteld van de verzoekers, vermindert de manuele werklast en de risico's van fouten bij de verwerking (tikfout bijvoorbeeld) en maakt de controle a posteriori mogelijk van alle verzoeken die werden gedaan (in het bijzonder dankzij een logging). Nog volgens de aanvrager is dit geautomatiseerd proces meer privacyvriendelijk dan de manuele of telefonische raadplegingen of via fax, die bijvoorbeeld niet de controle door middel van loggings toelaten, het risico van verlies van gegevens en eventuele fouten bij de gegevensverwerking. Belangrijk is ook dat enkel de verzoeken gaan via de NTSU/CTIF en daar worden gecontroleerd. De antwoorden worden daarentegen rechtstreeks aan de oorspronkelijke verzoeker bezorgd zonder opnieuw langs de NTSU/CTIF te gaan. Dit is eveneens gunstig voor de gegevensbescherming. Volgens de aanvrager neemt de NTSU twee soorten maatregelen om de gegevens met betrekking tot de maatregelen waarvoor zij verantwoordelijk is te beschermen:

- <u>fysieke maatregelen</u>: beperkte toegang, gecontroleerde toegang met badge, gebouw dat fysiek beschermd wordt, permanente bezetting, camera's, logging van personen die binnenkomen en vertrekken;

- <u>softwarematige maatregelen:</u> verlenen van rechten op grond van specifieke profielen, loggingcontrole van elke op het netwerk verrichte handeling, toegang verleend per dossier (geen algemene toegang) wanneer de naam van de betrokkene specifiek vermeld is op de vordering van de onderzoeksrechter, beveiligde overdracht.

45. De Commissie stelt voor om onder artikel 3, eerste alinea, van het tweede ontwerp kb de volgende passage toe te voegen : '…De dienst NTSU-CTIF bewaart een log en maakt een journaal op van iedere toegang en consultatie van de databank. *Zij neemt tevens de nodige fysieke -en softwarematige maatregelen om in een passend beveiligingsniveau te voorzien.*'

46. -(Advies nr. 29/2008)het proportionaliteitsbeginsel niet is nageleefd voor wat de doorgifte van de persoonlijke contactgegevens van de leden van de Coördinatiecel Justitie betreft.

47. Het tweede ontwerp kb voorziet in artikel 2, §3 dat een dienst GSM ter beschikking van de Coördinatiecel wordt gesteld. Derhalve werd voldaan aan de opmerking van de Commissie in haar advies, en werd de terbeschikkingstelling van de privégegevens van de leden van de cel geschrapt.

OM DEZE REDENEN,

adviseert de Commissie *gunstig* enkel en alleen op voorwaarde dat er rekening gehouden wordt met de opmerkingen geformuleerd m.b.t.:

- de bepaling van de bewaarduur van 12 maanden in het voorontwerp van wet : punt 8;
- de parlementaire evaluatie van het voorontwerp van wet en ontwerp kb en het jaarlijkse verslag aan het parlement door de bevoegde minister : punt 9;
- de bewaarduur van 12 maanden, en de onmiddellijke vernietiging van de bewaarde gegevens na het verstrijken van die termijn : punten 19 tot en met 22;
- het gebruik van het woord *'openbare'* voor een internettoegangsdienst, emaildienst, en een internettelefoniedienst : punt 25;
- de definitie van het begrip *'uitzonderlijke omstandigheden'* : punt 30;
- de strafbaarstelling van de toegang –en gebruiksvereisten : punt 34;
- de dienst NTSU-CTIF : punten 41-45.

Voor de Administrateur m.v., De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere

ANNEXE 6

BIJLAGE 6

Version consolidée/geconsolideerde versie

Artikel 1 van de wet van 13 juin 2005 betreffende de elektronische communicatie	
Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.	Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.
Deze wet vormt de omzetting in Belgisch recht van :	Deze wet vormt de omzetting in Belgisch recht van :
- Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten ("Kaderrichtlijn") (PbEG 24 april 2002, L 108/33);	- Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten ("Kaderrichtlijn") (PbEG 24 april 2002, L 108/33);
- Richtlijn 2002/20/EG van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische communicatienetwerken en -diensten ("Machtigingsrichtlijn") (PbEG 24 april 2002, L 108/21);	- Richtlijn 2002/20/EG van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische communicatienetwerken en -diensten ("Machtigingsrichtlijn") (PbEG 24 april 2002, L 108/21);
- Richtlijn 2002/19/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de toegang tot en interconnectie van elektronische communicatienetwerken en bijbehorende faciliteiten ("Toegangsrichtlijn") (PbEG 24 april 2002, L 108/7);	- Richtlijn 2002/19/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de toegang tot en interconnectie van elektronische communicatienetwerken en bijbehorende faciliteiten ("Toegangsrichtlijn") (PbEG 24 april 2002, L 108/7);
- Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en diensten ("Universele dienstrichtlijn") (PbEG 24 april 2002, L 108/51);	- Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en diensten ("Universele dienstrichtlijn") (PbEG 24 april 2002, L 108/51);
- Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ("Privacy- en elektronische communicatierichtlijn") (PbEG 31 juli 2002, L 201/37);	- Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ("Privacy- en elektronische communicatierichtlijn") (PbEG 31 juli 2002, L 201/37);
- en Richtlijn 2002/77/EG van de Commissie van 16 september 2002 betreffende de mededinging op de markten voor elektronische communicatienetwerken en -diensten ("Mededingingsrichtlijn") (PbEG 17 september	- en Richtlijn 2002/77/EG van de Commissie van 16 september 2002 betreffende de mededinging op de markten voor elektronische communicatienetwerken en -diensten ("Mededingingsrichtlijn") (PbEG 17 september

2002, L 249/21). Deze wet voorziet in een gedeeltelijke omzetting van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en van Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronische-communicatienetwerken en -diensten.	2002, L 249/21). Deze wet voorziet in een gedeeltelijke omzetting van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en van Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronische-communicatienetwerken en -diensten. **Deze wet voorziet in een gedeeltelijke omzetting van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn genereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG ("Dataretentierichtlijn") (PB 13 april 2006, L 105/54) en van artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB, 31 juli 2002, L 201/37).**

Article 1er de la loi du 13 juin 2005 relative aux communications électroniques	
Article 1. La présente loi règle une matière visée	Article 1. La présente loi règle une matière visée

à l'article 78 de la Constitution.	à l'article 78 de la Constitution.
La présente loi constitue la transposition en droit belge de :	La présente loi constitue la transposition en droit belge de :
- la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "Cadre") (J.O.C.E. 24 avril 2002, L 108/33);	- la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "Cadre") (J.O.C.E. 24 avril 2002, L 108/33);
- la directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive "Autorisation") (J.O.C.E. 24 avril 2002, L 108/21);	- la directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive "Autorisation") (J.O.C.E. 24 avril 2002, L 108/21);
- la directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées (directive "Accès") (J.O.C.E. 24 avril 2002, L 108/7);	- la directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées (directive "Accès") (J.O.C.E. 24 avril 2002, L 108/7);
- la directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive "Service universel") (J.O.C.E. 24 avril 2002, L 108/51);	- la directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive "Service universel") (J.O.C.E. 24 avril 2002, L 108/51);
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "Vie privée et communications électroniques") (J.O.C.E. 31 juillet 2002, L 201/37);	- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "Vie privée et communications électroniques") (J.O.C.E. 31 juillet 2002, L 201/37);
- et la directive 2002/77/CE de la Commission du 16 septembre 2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques (directive "Concurrence") (J.O.C.E. 17 septembre 2002, L 249/21).	- et la directive 2002/77/CE de la Commission du 16 septembre 2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques (directive "Concurrence") (J.O.C.E. 17 septembre 2002, L 249/21).
La présente loi transpose partiellement la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard	La présente loi transpose partiellement la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard

des réseaux et services de communications électroniques, la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le Règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et la Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les Directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.	des réseaux et services de communications électroniques, la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le Règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et la Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les Directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques. **La présente loi transpose partiellement la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de donnés 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 (directive « conservation de données ») (J.O. 13 avril 2006, L 105/54) et l'article 15.1 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») (J.O. 31 juillet 2002, L 201/37).**

Artikel 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie	
Art. 2.Voor de toepassing van deze wet wordt verstaan onder :	Art. 2.Voor de toepassing van deze wet wordt verstaan onder :
[…]	[…]
11° " operator " : een persoon die een kennisgeving heeft ingediend overeenkomstig artikel 9;	11° " operator " : **een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9**;

[…]	[…]
	74° "Oproeppoging zonder resultaat" : een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord.

Article 2 de la loi du 13 juin 2005 relative aux communications électroniques	
Art.2.Pour l'application de la présente loi, il faut entendre par :	Art. 2. Pour l'application de la présente loi, il faut entendre par :
[…]	[…]
11° " opérateur " : toute personne ayant introduit une notification conformément à l'article 9;	11° "opérateur" : **toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9;**
[…]	[…]
	74° « Appels infructueux » : toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau.

Artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie	
Art. 126. § 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de Minister van Justitie en van de minister en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.	**Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, of internettelefoniediensten, en de aanbieders van de onderliggende openbare elektronische-communicatienetwerken de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische-communicatiedienst en de gegevens voor identificatie van de vermoedelijk gebruikte eindapparatuur, die door hen worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten.**

§ 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut. De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België.	**Onder aanbieders in de betekenis van dit artikel worden ook de doorverkopers in eigen naam en voor eigen rekening verstaan.**
	Onder telefoniedienst in de betekenis van dit artikel wordt verstaan: telefoonoproepen – met inbegrip van spraakoproepen, voicemail, conference call of datacommunicatie-, aanvullende diensten -met inbegrip van call forwarding en call transfer-, en de messaging- en multimediadiensten – met inbegrip van short message service (sms), enhanced media service (EMS) en multimedia service (MMS).
	De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de krachtens het eerste lid te bewaren gegevens per type dienst alsook de vereisten waaraan deze gegevens moeten beantwoorden.
	Behoudens andersluidende wettelijke bepaling, mogen geen gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, bewaard worden.
	De verplichting om de in het eerste lid bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:
	1° wat de telefoniegegevens betreft, worden gegenereerd, verwerkt en opgeslagen door de aanbieders van openbare diensten voor elektronische communicatie of van een openbaar netwerk voor elektronische

	communicatie, of;
	2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.
	§ 2. De gegevens beoogd in paragraaf 1, eerste lid, worden bewaard met het oog op:
	a) de opsporing, het onderzoek en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering;
	b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107;
	c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of –dienst, zoals bedoeld in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
	d) de vervulling van de inlichtingenopdrachten met inzet van de methoden voor het verzamelen van gegevens zoals bedoeld in de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
	De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en 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.
	§ 3. De gegevens ter identificatie van de eindgebruikers, de gebruikte elektronische-communicatiedienst en de vermoedelijk gebruikte eindapparatuur worden bewaard vanaf de inschrijving op de dienst, zolang binnenkomende of uitgaande communicatie mogelijk is door middel van de dienst waarop

	werd ingetekend en gedurende twaalf maanden vanaf de datum van de laatste geregistreerde binnenkomende of uitgaande communicatie.
	De verkeers- en localisatiegegevens worden bewaard gedurende twaalf maanden vanaf de datum van de communicatie.
	De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de gegevens die zijn onderworpen aan het eerste lid en deze die zijn onderworpen aan het tweede lid.
	§ 4. Naar aanleiding van het evaluatieverslag beoogd in paragraaf 7, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer, de bewaringstermijn van de gegevens voor bepaalde categorieën van gegevens aanpassen, zonder een termijn van meer dan 18 maanden vast te leggen.
	De Koning kan, in de omstandigheden zoals bedoeld in artikel 4, § 1, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een beperkte periode, een bewaringstermijn voor de gegevens vastleggen die langer is dan twaalf maanden.
	Wanneer in de omstandigheden bedoeld in het tweede lid de Koning een bewaringstermijn oplegt die langer is dan vierentwintig maanden, stelt de minister de Europese Commissie en de overige lidstaten van de Europese Unie onverwijld in kennis van alle genomen maatregelen, met vermelding van de redenen die eraan ten grondslag liggen.
	§ 5. Voor de bewaring van de in paragraaf 1, eerste lid, bedoelde gegevens geldt het onderstaande voor de aanbieder van een netwerk of dienst voor elektronische communicatie bedoeld in paragraaf 1, eerste

	lid:
	1° hij garandeert dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;
	2° hij zorgt ervoor dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
	3° hij garandeert dat de toegang tot de bewaarde gegevens enkel door een of meer leden van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en door het personeel en de aangestelden van deze aanbieders die specifiek door deze cel gemachtigd zijn gebeurd;
	4° hij zorgt ervoor dat de gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, worden vernietigd.
	De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die de aanbieders van diensten en netwerken beoogd in paragraaf 1, eerste lid, moeten nemen teneinde de bescherming van de bewaarde persoonsgegevens te garanderen.
	De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, worden beschouwd als verantwoordelijk voor de verwerking van deze gegevens in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

	§ 6. De minister en de minister van Justitie zorgen ervoor dat jaarlijks aan de Europese Commissie en de Kamer van volksvertegenwoordigers statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare communicatiediensten of -netwerken. Die informatie heeft onder meer betrekking op:
	1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;
	2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;
	3° de gevallen waarin verzoeken niet konden worden ingewilligd.
	Deze statistische informatie mag geen persoonsgegevens omvatten.
	De gegevens die betrekking hebben op de toepassing van paragraaf 2, a), worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van Strafvordering moet uitbrengen aan het Parlement.
	De Koning bepaalt, op voorstel van de minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders van diensten of netwerken jaarlijks moeten overzenden aan het Instituut en deze die het Instituut overzendt aan de minister en aan de minister van Justitie.
	§ 7. Onverminderd het verslag bedoeld in paragraaf 6, derde lid, brengen de minister en de minister van Justitie, twee jaar na de inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 1, derde lid, aan de Kamer van volksvertegenwoordigers een evaluatieverslag uit over de toepassing van dit artikel, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat

	betreft de te bewaren gegevens en de bewaringstermijn.

Article 126 de la loi du 13 juin 2005 relative aux communications électroniques	
Art. 126. § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.	**Art. 126. § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic, les données de localisation, les données d'identification d'utilisateurs finals, les données d'identification du service de communications électroniques utilisé et les données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.**
§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut. Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique.	**Par fournisseurs au sens du présent article, on entend également les revendeurs en nom propre et pour leur propre compte.**
	Par service de téléphonie au sens du présent article, on entend les appels téléphoniques - notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données-, les services supplémentaires - notamment le renvoi ou le transfert d'appels- et les services de messagerie et multimédias, notamment les services de messages brefs (SMS), les services de médias améliorés (EMS) et les services multimédias (MMS).

	Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de service en application de l'alinéa 1er ainsi que les exigences auxquelles ces données doivent répondre.
	Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée.
	L'obligation de conserver les données visées à l'alinéa 1er s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés:
	1° en ce qui concerne les données de la téléphonie, générées, traitées et stockées par les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou;
	2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.
	§ 2. Les données visées au paragraphe 1er , al. 1er, sont conservées en vue :
	a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle;
	b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107;
	c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;
	d) de l'accomplissement des missions de renseignement en ayant recours aux méthodes

	de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.
	Les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 1er, alinéa 1er, , soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières.
	§ 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées à partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.
	Les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication.
	Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises au premier alinéa et celles au deuxième.
	§ 4. A la suite du rapport d'évaluation visé au paragraphe 7, le Roi peut, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de la Commission de la protection de la vie privée, adapter le délai de conservation des données pour certaines catégories de données, sans ce que ce délai ne puisse dépasser 18 mois.
	Le Roi peut, dans les circonstances visées à l'article 4, § 1er, par arrêté délibéré en Conseil des ministres, et après avis de l'Institut et de la

	Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à douze mois.
	Lorsque, dans les circonstances visées à l'alinéa 2, le Roi fixe un délai de conservation supérieur à vingt-quatre mois, le ministre notifie immédiatement à la Commission européenne et aux autres Etats membres de l'Union européenne toute mesure prise, accompagnée de sa motivation.
	§ 5. Pour la conservation des données visées au paragraphe 1er, alinéa 1er, les fournisseurs de réseaux ou de services de communications électroniques visés au paragraphe 1er, alinéa 1er:
	1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;
	2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;
	3° garantissent que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et par les agents et préposés de ces fournisseurs spécifiquement autorisés par ladite Cellule;
	4° veille à ce que les données conservées soient détruites lorsqu'est expiré le délai de conservation applicable à ces données.
	Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la

	Commission de la protection de la vie privée et de l'Institut, les mesures techniques et administratives que les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, doivent prendre en vue garantir la protection des données à caractère personnelle conservées.
	Les founisseurs de services et réseaux visés paragraphe 1er, alinéa 1er, sont considérés comme responsables du traitement de ces données au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
	§ 6. Le ministre et le ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Commission européenne et à la Chambre des Représentants. Ces statistiques comprennent notamment :
	1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;
	2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;
	3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.
	Ces statistiques ne peuvent comprendre des données à caractère personnel.
	Les données qui concernent l'application du paragraphe 2, a), seront également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.
	Le Roi détermine, sur proposition du ministre de la Justice et ministre et sur avis de l'Institut, les statistiques que les fournisseurs de services

	ou de réseaux transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.
	§ 7. Sans préjudice du rapport visé au paragraphe 6, 3ième alinéa, le ministre et le ministre de la Justice font un rapport d'évaluation à la Chambre des Représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, alinéa 3, sur la mise en œuvre de cet article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation.

Artikel 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie	
Art. 145. § 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 32, 33, 35, 41, 42, 114, 124, 127 en de ter uitvoering van de artikelen 32, 39, § 3, 47 en 127 genomen besluiten overtreedt.	Art. 145. § 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen 32, 33, 35, 41, 42, 114, 124, 127 en de ter uitvoering van de artikelen 32, 39, § 3, 47 en 127 genomen besluiten overtreedt.
§ 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt gestraft de persoon die artikel 39, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt.	§ 2. Met een geldboete van 200 tot 2 000 EUR en met een gevangenisstraf van acht dagen tot één jaar of met één van die straffen alleen wordt gestraft de persoon die artikel 39, § 1, en de ter uitvoering van artikel 16 genomen besluiten overtreedt.
§ 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft:	§ 3. Met een geldboete van 500 tot 50 000 EUR en met een gevangenisstraf van één tot vier jaar of met één van die straffen alleen wordt gestraft:
1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;	1° de persoon, die op bedrieglijke wijze elektronische communicatie door middel van een elektronische communicatienetwerk tot stand brengt, teneinde zichzelf of aan een andere persoon wederrechtelijk een voordeel te verschaffen;
2° (opgeheven)	2° (opgeheven)
3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan.	3° de persoon die welk toestel dan ook opstelt dat bestemd is om een van de voorgaande inbreuken te begaan, alsook een poging om deze te begaan.

§ 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan.	§ 3bis. Met een geldboete van 50 EUR tot 300 EUR en met een gevangenisstraf van vijftien dagen tot twee jaar of met één van die straffen alleen worden gestraft de persoon, die een elektronische-communicatienetwerk of -dienst of andere elektronische communicatiemiddelen gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen alsook de persoon die welk toestel dan ook opstelt dat bestemd is om de voorgaande inbreuk te begaan, alsook een poging om deze te begaan.
	§ 3*ter*. Met een geldboete van 50 tot 50.000 EUR en met een gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:
	1° iedere persoon die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt;
	2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt.
§ 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.	§ 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikel en 32, 33, 35 en 37 wordt altijd uitgesproken.

Article 145 de la loi du 13 juin 2005 relative aux communications électroniques	
Art. 145. § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 32, 33, 35, 41, 42, 114, 124, 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47 et 127.	Art. 145. § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 32, 33, 35, 41, 42, 114, 124, 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47 et 127.
§ 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16.	§ 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16.

§ 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement :	§ 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement :
1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite;	1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite;
2° (abroge)	2° (abroge)
3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci.	3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci.
§ 3bis. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.	§ 3bis. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.
	§ 3*ter*. Est puni d'une amende de 50 à 50 000 EUR et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement :
	1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126 ;
	2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1° les détient, les révèle à une autre personne, ou les divulgue ou fait un usage quelconque des données ainsi obtenues.
§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33,	§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33,

35 et 37 est toujours prononcée.	35 et 37 est toujours prononcée.

Artikel 90*decies* van het Wetboek van strafvordering	
Art. 90decies. De Minister van Justitie brengt elk jaar verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies.	Art. 90decies. De Minister van Justitie brengt elk jaar verslag uit aan het Parlement over de toepassing van de artikelen 90ter tot en met 90novies.
Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, van de duur van die maatregelen, van het aantal betrokken personen en van de behaalde resultaten.	Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in die artikelen, van de duur van die maatregelen, van het aantal betrokken personen en van de behaalde resultaten.
Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40bis, 46ter, 46quater, 47ter tot 47decies, 56bis, 86bis, 86ter, 88sexies en 89ter.	Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 40bis, 46ter, 46quater, 47ter tot 47decies, 56bis, 86bis, 86ter, 88sexies en 89ter.
Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in deze artikelen, van het aantal betrokken personen, van de misdrijven waarop ze betrekking hadden en van de behaalde resultaten.	Hij brengt het Parlement op de hoogte van het aantal onderzoeken die aanleiding gegeven hebben tot de maatregelen bedoeld in deze artikelen, van het aantal betrokken personen, van de misdrijven waarop ze betrekking hadden en van de behaalde resultaten.
Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 102 tot 111 en 317 en stelt de federale Wetgevende Kamers in kennis van het aantal betrokken dossiers, personen en misdrijven.	Hij brengt tegelijkertijd verslag uit over de toepassing van de artikelen 102 tot 111 en 317 en stelt de federale Wetgevende Kamers in kennis van het aantal betrokken dossiers, personen en misdrijven.
	Bij dit verslag wordt tevens het verslag bijgevoegd dat werd opgesteld met toepassing van artikel 126, § 6, derde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Article 90*decies* du Code d'instruction criminelle	
Art. 90decies. Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies.	Art. 90decies. Le Ministre de la Justice fait rapport annuellement au Parlement sur l'application des articles 90ter à 90novies.

Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, de la durée de ces mesures, du nombre de personnes concernées et des résultats obtenus.	Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, de la durée de ces mesures, du nombre de personnes concernées et des résultats obtenus.
II fait en même temps rapport sur l'application des articles 40bis, 46ter, 46quater, 47ter à 47decies, 56bis, 86bis, 86ter, 88sexies et 89ter.	II fait en même temps rapport sur l'application des articles 40bis, 46ter, 46quater, 47ter à 47decies, 56bis, 86bis, 86ter, 88sexies et 89ter.
Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, du nombre de personnes concernées, des infractions concernées et des résultats obtenus.	Il informe le Parlement du nombre d'instructions ayant donné lieu à des mesures visées par ces articles, du nombre de personnes concernées, des infractions concernées et des résultats obtenus.
Il fait en même temps rapport sur l'application des articles 102 à 111 et 317 et informe les Chambres législatives fédérales du nombre de dossiers, de personnes et d'infractions concernés.	Il fait en même temps rapport sur l'application des articles 102 à 111 et 317 et informe les Chambres législatives fédérales du nombre de dossiers, de personnes et d'infractions concernés.
	A ce rapport est joint le rapport dressé en application de l'article 126, § 6, alinéa 3 de la loi du 13 juin 2005 relative aux communications électroniques.

Imprimerie centrale – Cette publication est imprimée exclusivement sur du papier certifié FSC
Centrale drukkerij – Deze publicatie wordt uitsluitend gedrukt op FSC gecertificeerd papier