

## KONINKRIJK BELGIË

[DATUM] – VOORONTWERP VAN WET TOT 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

### MEMORIE VAN TOELICHTING

Het Europees Parlement en de Raad van de Europese Unie hebben op 15 maart 2006 Richtlijn 2006/24/EG aangenomen 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.

Deze richtlijn heeft, zoals dat in het eerste artikel ervan wordt uiteengezet, 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 stelt 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 communicatie, alsook van de gebruikte apparatuur en de locatie van de gebruikte apparatuur. Het wetsontwerp groepeert deze categorieën van gegevens onder de noemers “verkeers- en locatiegegevens” en “gegevens voor identificatie van de eindgebruikers”. Deze worden dan verder uitgewerkt in het ontwerp van koninklijk besluit. Op die manier worden de artikelen 46bis en 88bis van het Wetboek van Strafvordering, en de terminologie van de wet betreffende de elektronische communicatie gerespecteerd.

## ROYAUME DE BELGIQUE

[DATE] – AVANT-PROJET DE LOI MODIFIANT LES ARTICLES 2, 126 ET 145 DE LA LOI DU 13 JUNI 2005 RELATIVE AUX COMMUNICATIONS ELECTRONIQUES ET DE L'ARTICLE 90DECIES DU CODE D'INSTRUCTION CRIMINELLE

### EXPOSE DES MOTIFS

Le Parlement européen et le Conseil de l'Union européenne ont adopté, le 15 mars 2006, la directive 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.

Cette directive a pour objectif, ainsi que cela est explicité dans son article premier, d'harmoniser les dispositions des Etats 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 Etat membre dans son droit interne.

La directive 2006/24/CE établit la liste des données à conserver en les regroupant par 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. Le projet de loi regroupe ces catégories de données sous les dénominations « données de trafic et de localisation » et « données d'identification d'utilisateurs finals ». Celles-ci sont développées plus amplement dans le projet d'arrêté royal. De cette manière, les articles 46bis et 88bis du Code d'Instruction criminelle et la terminologie de la loi relative aux communications électroniques sont respectés.

De richtlijn creëert eveneens een aantal subcategorieën binnen deze verschillende gegevenscategorieën naargelang van de aard van de netwerken en diensten die zijn betrokken bij een communicatie: vaste telefonie, mobiele telefonie, internettelefonie, internettoegang en e-mail 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 opgesomde gegevens.

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.

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 politiediensten en de gerechtelijke autoriteiten.

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 in de eerste plaats 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 operatoren en aanbieders voortaan uitdrukkelijk verplicht het geheel alle bepalingen van de wet van 8 december 1992 en het bijbehorende uitvoeringsbesluit van 13 februari 2001 na te leven, wat betreft meer bepaald de kwaliteit van de gegevens (nauwkeurigheid, bewerking, 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 operatoren dienen de

De même, au sein de ces différentes catégories de données, la directive établit un certain nombre de sous catégories, en fonction de la nature des réseaux et services concernés par une communication : téléphonie fixe, téléphonie mobile, téléphonie par Internet, accès à l'Internet, et courrier électronique par Internet. Ces catégories sont également explicitement énumérées au projet de l'article 126, afin qu'il soit clair quels opérateurs sont soumis à l'obligation de conservation des données énumérées ci-dessus.

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.

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 services de police et des autorités judiciaires.

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 tout d'abord 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 opérateurs et fournisseurs sont désormais 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 opérateurs de la conservation de ses données pendant une période

persoon op de hoogte te brengen van de bewaring van zijn gegevens voor strafrechtelijke doeleinden 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 Commissie voor de bescherming van de persoonlijke levenssfeer 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.

Wat straffen betreft, 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 gevormde) die artikel 4 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 van diezelfde wet mag het BIPT een administratieve boete opleggen die in het geval van rechtspersonen kan gaan tot 5% van het omzetcijfer (waarbij het totale bedrag van de boete het bedrag van 12,5 miljoen euro niet mag overschrijden).

Aangezien de Europese richtlijn 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 wetsontwerp een extra strafbepaling in, die een aanvulling is op de al bestaande strafbepalingen betreffende externe en interne hacking in het Strafwetboek. Dat wil zeggen dat niet alleen het BIPT en de Commissie voor de bescherming van de persoonlijke levenssfeer, maar ook de gerechtelijke autoriteiten toezicht kunnen

maximale de 12 mois pour des finalités pénales, elle pourra accéder à ses données et pourra, le cas échéant, les faire rectifier, le tout sans préjudice d'une plainte devant la Commission de Protection de la Vie privée 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.

En matière de sanctions, 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 de ladite loi, à savoir la qualité des données (pas de données excessives, pas de durée de conservation éternelle, pas d'utilisation incompatibles 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 de cette même loi permet à l'IBPT d'infliger une amende administrative pouvant aller, dans le cas des personnes morales, jusqu'à 5 % du chiffre d'affaire (sans que le montant total de l'amende ne puisse dépasser un montant de 12,5 millions EUR).

Vu que la directive européenne stipule explicitement à l'article 13.2, que chaque Etat 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. Cela veut dire que non seulement l'IBPT et la Commission pour la protection de la vie privée, mais aussi les autorités judiciaires peuvent contrôler le bon déroulement de la conservation des

houden op het goede verloop van de bewaring van de gegevens.

De omzetting van Richtlijn 2006/24/EG zal ten slotte deels aan de hand van een wijziging van artikel 126 van de voornoemde wet van 13 juni 2005 geschieden 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 bewaringsvoorwaarden zullen worden vastgelegd door de Koning.

De Europese richtlijn 2006/24/EG legt het algemene kader voor de gegevensbewaring betreffende elektronische communicatie vast. Slechts vier categorieën van openbare elektronische communicatiediensten worden geïdentificeerd: vaste telefonie, mobiele telefonie, internettoegang en elektronisch berichtenverkeer (e-mail) 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. 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 opgenomen zouden worden 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 communicatie dat in de plaats kwam van het vorige artikel.

Het voorontwerp van wet werd, samen met het ontwerp van Koninklijk Besluit, twee maal voor advies voorgelegd aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. In bijlage bij deze memorie werd de nota opgenomen die aan de Commissie werd overgemaakt met de elementen van antwoord op het eerste advies nr. 24/2008.

données.

Enfin, la transposition de la directive 2006/24/CE sera effectuée 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 conditions de leur conservation seront fixés par le Roi.

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

L'avant-projet de loi et le projet d'arrêté royal ont été soumis deux fois pour avis à la Commission de la protection de la vie privée. La note transmise à la Commission et contenant les éléments de réponse au premier avis n° 24/2008, est jointe en annexe de cet exposé des motifs.

## COMMENTAAR BIJ DE ARTIKELEN

Het eerste artikel behoeft geen commentaar.

### Artikel 2

Artikel 2 vervangt de definitie van het begrip “operator” in artikel 2, 11° van de wet van 13 juni 2005 betreffende de elektronische communicatie. Doordat immers de huidige definitie het begrip beperkt tot iedere persoon die een kennisgeving heeft ingediend overeenkomstig artikel 9, schiet deze definitie te kort voor wat betreft het doel van dit wetsontwerp: voldoen aan de Europese richtlijn 2006/24/EG en ervoor zorgen dat alle aanbieders van elektronische communicatiediensten en communicatienetwerken beoogd door deze richtlijn onder de Belgische wetgeving inzake dataretentie vallen.

Artikel 9, §1 van de wet bepaalt dat het aanbieden of het doorverkopen in eigen naam en voor eigen rekening van elektronische communicatiediensten of –netwerken pas kan aangevat worden na een kennisgeving aan het BIPT. De begrippen “elektronische communicatiedienst” en “elektronisch communicatienetwerk” worden beiden gedefinieerd in artikel 2 van de wet, respectievelijk in de punten 3° en 5°. Deze definities werden bijna letterlijk overgenomen uit de Europese Richtlijn 2002/21/EG van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en elektronische communicatiediensten, een richtlijn die in Belgisch recht werd omgezet door de wet van 13 juni 2005 (zie artikel 1 van de wet).

Nu is het zo dat de richtlijn 2006/24/EG, die het voorwerp uitmaakt van huidig wetsontwerp, dezelfde terminologie gebruikt. M.a.w., de richtlijn heeft betrekking op de elektronische communicatiediensten en elektronische communicatienetwerken zoals gedefinieerd in de richtlijn van 2002. Dit wordt uitdrukkelijk bepaald door artikel 2 van de richtlijn. Precies de aanbieders van deze diensten en netwerken worden door artikel 9 van de wet van 13 juni 2005 opgelegd een kennisgeving te doen aan het BIPT. Omdat de regelgeving inzake dataretentie betrekking heeft op al deze diensten en netwerken is het noodzakelijk om de definitie van het begrip “operator” in de Belgische wetgeving aan te passen. De operatoren zijn de gehele groep van aanbieders van elektronische communicatienetwerken en elektronische communicatiediensten die onder de dataretentiewetgeving dienen te vallen, volgens de Europese richtlijn. De huidige definitie van het

## COMMENTAIRE DES ARTICLES

L'article premier n'appelle pas de commentaire.

### Article 2

L'article 2 remplace la définition de la notion d'“opérateur” à l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques. En effet, la définition actuelle limitant la notion à toute personne ayant introduit une notification conformément à l'article 9, elle se révèle insuffisante pour l'objet du présent projet de loi : satisfaire à la directive européenne 2006/24/CE et veiller à ce que tous les fournisseurs de services et de réseaux de communications électroniques visés par cette directive tombent sous la législation belge en matière de rétention de données.

L'article 9, § 1<sup>er</sup>, de la loi prévoit que la fourniture ou la revente en nom propre et pour son propre compte de services ou de réseaux de communications électroniques ne peut débuter qu'après une notification à l'IBPT. Les notions de “service de communications électroniques” et “réseau de communications électroniques” sont toutes deux définies à l'article 2 de la loi, respectivement aux 3° et 5°. Ces définitions ont été reprises quasi littéralement de la directive européenne 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, directive transposée en droit belge par la loi du 13 juin 2005 (voir article 1<sup>er</sup> de la loi).

Il se fait que la directive 2006/24/CE, qui fait l'objet du présent projet de loi, utilise la même terminologie. En d'autres termes, la directive se rapporte aux services et réseaux de communications électroniques définis dans la directive de 2002. L'article 2 de la directive le prévoit expressément. L'article 9 de la loi du 13 juin 2005 impose précisément aux fournisseurs de ces services et réseaux d'introduire une notification à l'IBPT. La réglementation relative à la rétention de données s'appliquant à tous ces services et réseaux, il y a lieu d'adapter la définition de la notion d'“opérateur” dans la législation belge. Par opérateurs, il convient d'entendre tous les fournisseurs de réseaux et services de communications électroniques qui, aux termes de la directive européenne, sont tenus de se soumettre à la réglementation relative à la rétention de données. La définition actuelle de la notion n'est pas acceptable dans la pratique car elle offre une

begrip is niet werkbaar in de praktijk doordat zij een ontsnapingsmogelijkheid biedt: operatoren die geen kennisgeving doen aan het BIPt zouden zo niet onder de regelgeving inzake dataretentie vallen. De richtlijn bepaalt uitdrukkelijk dat vaste telefonie, mobiele telefonie, internettoegang, emaildiensten en internettelefoniediensten onderworpen zijn aan de regelgeving inzake dataretentie. Deze categorieën worden expliciet opgesomd in artikel 3 van huidig wetsontwerp (cfr. Infra). In de huidige stand van de wetgeving zou dit betekenen dat de dataretentie van toepassing is op de operatoren zoals gedefinieerd door artikel 2, 11° van de wet, maar ook op operatoren die aan de verplichting van artikel 9 niet voldaan hebben.

Wetgeving die mogelijk een inbreuk inhouden op de persoonlijke levenssfeer dient duidelijk en voorzienbaar te zijn voor de rechtsonderhorigen. Omdat dit in de huidige omstandigheden niet het geval is, verdient het dan ook aanbeveling om de definitie van het begrip “operatoren” te wijzigen. Daarmee komt het voorontwerp overigens tegemoet aan het advies nr. 24/2008 van 2 juli 2008 van de Commissie voor de bescherming van de persoonlijke levenssfeer.

### **Artikel 3**

Artikel 3 vervangt het artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

De doeleinden voor opsporing en beteugeling van strafbare feiten wordt in het nieuwe artikel 126 vervangen door “het onderzoek, de opsporing en de vervolging” van strafbare feiten teneinde in overeenstemming te zijn met artikel 1 van Richtlijn 2006/24/EG.

Zo werden ook de bepalingen betreffende de bewaringstermijn van de gegevens herzien op basis van artikel 6 van Richtlijn 2006/24/EG. Dit artikel voorziet een minimale bewaringstermijn van de gegevens van zes maanden en een maximale bewaringstermijn van de gegevens van vierentwintig maanden. In overeenstemming met het advies 20/2009 van de Commissie voor de Bescherming van de persoonlijke levenssfeer voorziet het voorontwerp van wet nu een bewaringstermijn van 12 maanden, en bepaalt het expliciet dat na afloop van deze termijn de bewaarde gegevens onverwijld vernietigd worden, tenzij voor de normale bedrijfsvoering overige wettelijke termijnen van toepassing zijn.

Bovendien heeft de Koning de mogelijkheid

échappatoire, en ce sens que les opérateurs qui n'introduiraient pas de notification à l'IBPT ne seraient pas soumis à la réglementation relative à la rétention de données. La directive prévoit expressément que la téléphonie fixe, la téléphonie mobile, les services d'accès à l'Internet, les services de courrier électronique et les services de téléphonie par Internet sont soumis à la réglementation relative à la rétention de données. Ces catégories sont explicitement énumérées à l'article 3 du présent projet de loi (cf. infra). En l'état actuel de la législation, la rétention de données s'appliquerait aux opérateurs définis à l'article 2, 11°, de la loi mais également aux opérateurs n'ayant pas satisfait à l'obligation de l'article 9.

Toute législation susceptible de porter préjudice au droit au respect de la vie privée doit être claire et prévisible pour les justiciables. Comme ce n'est pas le cas dans les circonstances actuelles, il est recommandé de modifier la définition de la notion d'“opérateur”. Ce faisant, l'avant-projet rencontre d'ailleurs l'avis n° 24/2008 du 2 juillet 2008 de la Commission de la protection de la vie privée.

### **Article 3**

L'article 3 remplace l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.

Les finalités relatives à la poursuite et à la répression d'infractions pénales, sont remplacés dans le nouvel article 126 par « la recherche, la détection et la poursuite » d'infractions pénales, et ce pour correspondre au libellé de l'article 1er de la directive 2006/24/CE.

De même, les dispositions relatives à la durée de conservation des données ont été revues en fonction de l'articles 6 de la directive 2006/24/CE. Cet article prévoit un délai minimum de conservation des données de six mois et un délai maximum de conservation des données de vingt-quatre mois. Conformément à l'avis n° 20/2009 de la Commission de la protection de la vie privée, l'avant-projet de loi prévoit maintenant un délai de conservation de douze mois, et il prescrit qu'après l'expiration de ce délai, les données conservées sont détruites sans délai, sauf si pour la gestion habituelle de l'entreprise, d'autres délais légaux sont d'application.

De plus, la possibilité est donnée au Roi de fixer

gekregen om een langere termijn dan het wettelijke maximum te bepalen in uitzonderlijke omstandigheden. Deze uitzonderlijke omstandigheden worden opgesomd in artikel 4, §1 van de wet: *”wanneer de openbare veiligheid, de volksgezondheid, de openbare orde of de verdediging van het Rijk dit eisen”*. Men kan bij wijze van voorbeeld denken aan oorlogssituaties of terroristische aanslagen. In ieder geval moeten de omstandigheden zwaarwegend genoeg zijn. In deze gevallen voorziet paragraaf 2 van artikel 126, conform artikel 12 van de richtlijn, in een procedure voor kennisgeving aan de Europese Commissie. Aangezien de richtlijn echter voorziet in bewaartermijnen van minimum zes maanden tot maximum vierentwintig maanden, en artikel 12 slechts in deze uitzonderlijke procedure voorziet als lidstaten de intentie hebben om de bewaringstermijn langer dan 24 maanden te verlengen, dient de kennisgeving aan de Commissie slechts gedaan te worden indien de Koning een bewaringstermijn langer dan 24 maanden wil vastleggen. (...)

De paragrafen 3 en 4 van artikel 126 nemen een suggestie over van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer en voorzien in een tweevoudige evaluatie van de wet en het erop gestoelde Koninklijk Besluit. Enerzijds moet er twee jaar na de inwerkingtreding van het Koninklijk Besluit een grote eenmalige evaluatie komen waarbij de verantwoordelijke ministers verslag uitbrengen aan het Parlement over de toepassing van de wet en van het Koninklijk Besluit, en waarbij eventueel inhoudelijke aanbevelingen gedaan kunnen worden omtrent bewaartermijnen, inhoud van de bewaarde gegevens, praktische toepassing, etc. Deze evaluatie kan in voorkomend geval tot passende initiatieven leiden. Anderzijds voorziet het voorontwerp ook in een jaarlijkse rapportering aan het parlement. Het gaat hier eerder om de statistische rapportering zoals die voor een aantal onderzoeksmaatregelen ook is opgenomen in artikel 90decies van het Wetboek van Strafvordering.

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

#### **Artikel 4**

un délai supérieur au maximum légal en cas de circonstances exceptionnelles. Ces circonstances exceptionnelles sont énumérées à l'article 4, §1<sup>er</sup> de la loi : *« lorsque la sécurité publique, la santé public, 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. En tout cas, il faut que les circonstances sont très sérieuses. Dans ces cas, une procédure de notification à la Commission européenne est prévue au paragraphe 2 de l'article 126, conformément à l'article 12 de la directive. Etant donné que la directive prévoit des délais de conservation de minimum six mois à maximum vingt-quatre mois, et que l'article 12 ne prévoit cette procédure exceptionnelle que lorsque des Etats membres ont l'intention de prolonger le délai au-delà de 24 mois, la notification à la Commission ne doit être faite que si le Roi fixe un délai de conservation qui est supérieur à 24 mois. (...)

Les paragraphes 3 et 4 de l'article 126 reprennent une suggestion de la Commission de la protection de la vie privée et prévoient une double évaluation de la loi et de son arrêté royal. D'une part, deux ans après l'entrée en vigueur de l'arrêté royal, une grande évaluation unique devra être menée ; les ministres responsables feront rapport au Parlement sur l'application de la loi et de l'arrêté royal, 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, l'avant-projet de loi prévoit également un rapport annuel au Parlement. Il s'agit ici plutôt d'un rapportage statistique, comme cela est déjà prévu pour quelques mesures d'instruction à l'article 90decies du Code d'instruction criminelle.

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

#### **Article 4**

Artikel 4 bevat de strafbaarstelling vernoemd in het algemene gedeelte van deze memorie. Het voorontwerp wijkt daarbij af van het advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, omdat na analyse gebleken is dat de tekst die aan de Commissie werd voorgelegd incoherent is met de al bestaande strafbepalingen in het Strafwetboek. Niettemin blijft de doelstelling van het artikel, die gedeeld wordt door de Commissie, dezelfde: de vertrouwelijkheid van de gegevens beschermen en waarborgen dat de toegang tot, het gebruik van en het bezit van deze gegevens conform zijn aan de wettelijke voorziene 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 zijn, om slechts een nieuwe strafbepaling te creëren voor de gevallen die nog niet gedekt zijn.

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

Wanneer een persoon gemachtigd is om toegang te hebben tot het systeem zijn toegangsbevoegdheid overschrijdt, kan er verwezen worden naar de interne hacking (artikel 550bis, §2 van het Strafwetboek + §§3 en 7). Dit zal bijvoorbeeld het geval zijn voor de persoon die in de Cel Justitie van een operator werkt maar zich toegang verschafte tot de gegevens zonder gerechtelijke vordering. Niettemin, de persoon die zijn toegangsbevoegdheid niet overschrijdt, maar later gebruik maakt van de gegevens die hij uit het systeem heeft gehaald op een wettelijke en gerechtvaardigde manier, is een hypothese die niet gedekt is door de wet.

Dit is dan ook de reden waarom in het voorontwerp van wet een nieuwe strafbepaling ingevoegd wordt die de elementen herneemt 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

L'article 4 contient la disposition pénale mentionnée dans la partie générale de cet exposé. L'avant-projet de loi s'écarte ici de l'avis de la Commission de la protection de la vie privée, parce qu'il est apparu, après analyse, que le texte soumis à la Commission est incohérent avec les dispositions pénales déjà existantes dans le Code pénal. Néanmoins, le but de l'article, qui est partagé par la Commission, rest 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 adéquates au cas présent.

Il est donc nécessaire de distinguer différents cas de figure et de voir quelles sont les dispositions existantes qui pourraient s'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, nous renvoyons ici à l'article 550bis, §1<sup>er</sup> 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 outrepassa son pouvoir d'accès, il peut être renvoyé à le hacking interne (article 550bis, §2 Code pénal + §§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'outrepassa pas son pouvoir d'accès, mais fait ultérieurement un usage non autorisés par la loi des données qu'elle a 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 l'avant-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

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 ander persoon onthult of verspreidt, of er enig gebruik van maakt.

#### **Artikel 5**

Dit artikel vervolledigt artikel 90decies van het Wetboek van Strafvordering. De jaarlijkse rapportering van de minister van Justitie voorzien door dit artikel zal voortaan ook statistische informatie bevatten over de bewaring van gegevens zoals voorzien door artikel 126 van de wet betreffende de elektronische communicatie.

De Minister voor Ondernemingen en  
Vereenvoudigen,

Vincent Van Quickenborne

De Minister van Justitie,

Stefaan De Clerck

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.

#### **Article 5**

Cet article complète l'article 90decies du Code d'instruction criminelle. Le rapportage 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 pour l'Entreprise et la  
Simplification,

Vincent Van Quickenborne

Le Ministre de la Justice,

Stefaan De Clerck

**Bijlage: 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 facturatie doeleinden, 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 46bis Wsv) en de oproepgegevens (art 88bis 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

**Annexe: 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. 46bis du Code d'Instruction criminelle) et les données d'appel (art. 88bis 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 du Code

bovendien een zo vergaande onderzoeksmaatregel dat de onderzoeksrechter en in uitzonderlijke 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

d'Instruction criminelle) est en outre une mesure d'instruction à ce point extrême que le juge d'instruction et, dans des cas exceptionnels, le procureur du roi ne peuvent 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. Élément 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

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.

Dit valt echter eenvoudig te verklaren:

De vergoedingen per vordering op basis van artikel 46bis of 88bis 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 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.

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 tarifiering voor de mededeling van de gegevens aan de bevoegde autoriteiten. Dit is ook het

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.

Cela s'explique toutefois simplement :

Les indemnités par réquisition sur la base de l'article 46bis ou 88bis du Code d'Instruction criminelle figurent actuellement à l'annexe de l'arrêté royal portant exécution des articles 46bis, § 2, alinéa 1<sup>er</sup>, 88bis, § 2, alinéas 1<sup>er</sup> 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.

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 du 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

geval in Portugal, Spanje, Zweden, Estland en Hongarije. Slechts Finland en Frankrijk voorzien in compensatie van de bewaringskosten via overheidsfinanciering.

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 46bis en 88bis van het Wetboek van Strafvordering en het KB van 9 januari 2003 (advies §16)

Artikel 46bis voorziet in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot telecommunicatiediensten, artikel 88bis 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 46bis en 88bis.

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 46bis en 88bis 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 datartentie. Een KB op basis van het huidige artikel 126, §2 WEC dat de te bewaren gegevens alsook de bewaartermijn had

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.

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 46bis et 88bis du Code d'Instruction criminelle et l'arrêté royal du 9 janvier 2003 (point 16 de l'avis)

L'article 46bis prévoit la demande de données d'identification concernant des services de télécommunication par le procureur du roi et l'article 88bis, 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 46bis et 88bis.

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 46bis et 88bis 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,

moeten bepalen is er nooit gekomen. Deze lacune wordt nu ingevuld door het voorontwerp van wet en het ontwerp van KB.

#### 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

§ 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.

#### 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, § 1<sup>er</sup>, 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, § 1<sup>er</sup>, 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

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.

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 46bis en 88bis van het Wetboek van Strafvordering.

Artikel 46bis voorziet in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot telecommunicatiediensten, artikel 88bis 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 46bis is een bevoegdheid van de procureur des Konings, artikel 88bis 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

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.

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 46bis et 88bis du Code d'Instruction criminelle.

L'article 46bis prévoit la demande des données d'identification relatives aux services de télécommunication par le procureur du roi et l'article 88bis, 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 46bis règle une compétence du procureur du roi, l'article 88bis, 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

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, zal in artikel 2 van het voorontwerp in doeleinde a) een expliciete verwijzing opgenomen worden naar de artikelen 46bis en 88bis 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 259bis en 314bis stellen het af luisteren, kennismaken en opnemen van privé-communicatie strafbaar;
- artikel 210bis stelt de valsheid in informatica strafbaar;
- artikel 504ter stelt het informaticabedrog strafbaar;
- de artikelen 550bis en 550ter 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.

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 sera renvoyé explicitement aux articles 46bis et 88bis du Code d'Instruction criminelle dans l'article 3, § 1<sup>er</sup>, 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 259bis et 314bis sanctionnent les écoutes, la prise de connaissance et l'enregistrement de communications privées ;
- l'article 210bis sanctionne le faux en informatique ;
- l'article 504quater sanctionne la fraude informatique ;
- enfin, les articles 550bis et 550ter 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

In de memorie van toelichting worden de toezichthoudende autoriteiten (het BIPT, de privacycommissie, justitie, de beheerder van de coördinatieceel) expliciet vermeld.

#### 7. Nietigheidssanctie (advies, §28)

Het verkrijgen van bewijs wordt niet geregeld door deze wet, daarvoor zijn de artikelen 46bis en 88bis 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

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.

#### 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 46bis et 88bis 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

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 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 opvraging 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 46bis en 88bis van het Wetboek van Strafvordering. Voor de Ombudsdienst is een specifieke wettelijke basis voor de toegang voorzien in artikel 43bis, §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

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 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 46bis et 88bis du Code d'Instruction criminelle. L'article 43bis §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 ;

- 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 technologische protocollen van de nieuwe telefonie (of e-mailvormen) kan volgen.

Eenzijds 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 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 reagerden op de consultatie door het BIPT vult de behoeften op het terrein helemaal niet in.

- 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 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.

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 tekort.**

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 opvraging 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

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.

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 arrondissementes. 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

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 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.

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 des années d'enquête, les organisations sous-jacentes n'étant mises au jour qu'après que leur comptabilité a été épiluchée. 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.

- 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 als zodanig geïdentificeerd geweest te zijn, pleegt kort na de start van het onderzoek echter een overval waardoor hij voor een jaar en twee maanden 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.

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 arrondissementale 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 maanden 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 maanden dan kunnen 84 % van de gestelde vragen worden opgelost.

- 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 fabricant 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.

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.

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 bewaaringstermijn 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. 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

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.

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, § 1<sup>er</sup>, 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.

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 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.

L'article 15 de la directive européenne 2002/58/CE permettait et permet toujours aux Etats 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 Etats 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 Etats 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 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. 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. 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

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.

2. Téléphonie mobile - article 3

*2.1. Données d'identification - article 3, § 1<sup>er</sup>*

- 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, § 1<sup>er</sup>*

- la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur

- 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 locatiegegevens 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. 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

- 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 a 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, § 1<sup>er</sup>*

- 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

*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.

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 klantgegevens.

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.

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

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 judiciaire 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.

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

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 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.

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 :

- 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.

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 dienstverstreker 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 de 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. 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 opvraging 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

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.

#### **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

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 gerichtere 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 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

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 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

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 geuploadede en gedownloadede gegevens. Deze gegevens worden door de operatoren thans ook steeds bijgehouden in hun klantgegevens.

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 46bis en 88bis 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 43bis, §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 de bevoegde gerechtelijke autoriteiten en niet langer bewaard dienen te worden door de operatoren.

15. Mislukte oproepingen (advies § 68-69)

De Commissie merkt op dat de verwoording in artikel 10 van het begrip “mislukte oproeping” niet aansluit bij de definiëring van de Europese

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 46bis et 88bis 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 43bis, § 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 autorités judiciaires et ne devront plus être conservées par les opérateurs.

15. Communications n'ayant pas abouti (points 68-69 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

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 § 70-73)

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.

\* \* \*

définition de la directive européenne. Etant donné que l'article 1<sup>er</sup> 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 70-73 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.

\* \* \*

**Vorderingen Federaal Parket tot identificatie van IP-adressen in 2007**

Leeftijd van de opgevraagde gegevens	% van de vragen	Gecumuleerd % van de vragen	Positieve identificatie
Leeftijd < 6 maanden	15 %	15 %	
6 mnd < leeftijd < 1 jaar	51 %	66 %	76 %
12 mnd < leeftijd < 18 mnd	18 %	84 %	76 %
18 maand < leeftijd	16 %	100 %	46 %

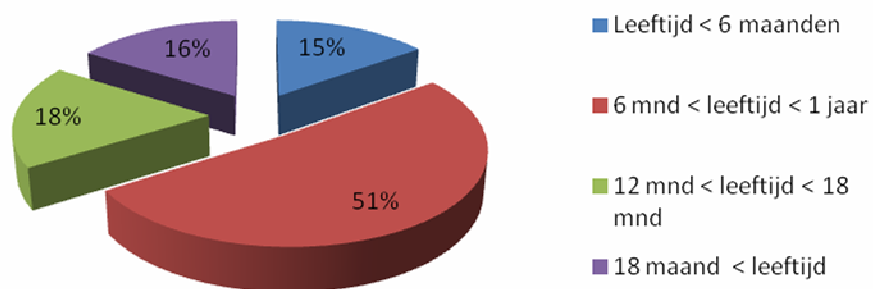
Gegevens : Federale gerechtelijke politie, DJF / FCCU

**Réquisitions du parquet fédéral concernant l'identification d'adresses IP en 2007**

Age des données demandées	Pourcentage des demandes	Pourcentage cumulé des demandes	Identification positive
Moins de 6 mois	15 %	15 %	
Entre 6 mois et 12 mois	51 %	66 %	76 %
Entre 12 mois et 18 mois	18 %	84 %	76 %
Plus de 18 mois	16 %	100 %	46 %

Données : police judiciaire fédérale, DJF / FCCU

## Ouderdom opgevraagde gegevens IP-adressen in 2007



## VOORONTWERP VAN WET

ALBERT II, Koning der Belgen,

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

Op de voordracht van Onze Minister voor Ondernemingen en Vereenvoudigen, en op het advies van Onze in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij:

Onze Minister voor Ondernemingen en Vereenvoudigen 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:

**Artikel 1.** Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

**Artikel 2.** Artikel 2, 11° van de wet van 13 juni 2005 betreffende de elektronische communicatie wordt vervangen als volgt:

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

**Artikel 3.** Artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie wordt vervangen als volgt:

“§ 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de operatoren die een openbare vaste telefoniedienst, een openbare mobiele telefoniedienst, een openbare internettoegangsdienst, een openbare emaildienst, of een openbare internettelefoniedienst aanbieden, de verkeers- en locatiegegevens 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, met het oog op:

## AVANT-PROJET DE LOI

ALBERT II, Roi des Belges,

A tous, présents et à venir, Salut.

Sur la proposition de Notre Ministre pour l'Entreprise et la Simplification, et de l'avis de Nos Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Notre Ministre pour l'Entreprise et la Simplification est chargé de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit :

**Article 1<sup>er</sup>.** La présente loi règle une matière visée à l'article 78 de la Constitution.

**Article 2.** L'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques est remplacé par ce qui suit :

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

**Article 3.** L'article 126 de la loi du 13 juin 2005 relative aux communications électroniques est remplacé par la disposition suivante :

« § 1<sup>er</sup>. 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 fournissant un service de téléphonie fixe accessible au public, un service de téléphonie mobile accessible au public, un service d'accès à l'Internet accessible au public, un service de courrier électronique accessible au public ou un service de téléphonie par Internet accessible au public, 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, et ce en vue :

- a) het onderzoek, de opsporing en de vervolging van strafbare feiten zoals bedoeld in de artikelen 46bis en 88bis van het Wetboek van strafvordering;
- b) de beteugeling van kwaadwillige oproepen naar de nooddiensten, zoals bedoeld in artikel 107 van deze wet;
- c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische 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 operatoren bedoeld in het vorige lid worden beschouwd als verantwoordelijke 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.

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 van bewaring van deze gegevens.

De bewaringstermijn voor de gegevens bedoeld in het eerste lid is twaalf maanden. Na afloop van deze termijn worden de gegevens onverwijld vernietigd, tenzij voor de normale bedrijfsvoering overige wettelijke termijnen van toepassing zijn

De operatoren zorgen ervoor dat de gegevens opgenomen in het eerste lid onbeperkt toegankelijk zijn vanuit België.

§2. Niettegenstaande het vierde lid van paragraaf 1 kan de Koning, in de uitzonderlijke omstandigheden zoals bedoeld in artikel 4, §1, bij besluit overlegd 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 eerste lid de Koning een bewaringstermijn oplegt die langer is dan 24 maanden, stelt de minister

- a) de la recherche, de la détection et de la poursuite d'infractions pénales visées aux articles 46bis et 88bis du Code d'Instruction criminelle ;
- b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107 de cette loi ;
- 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 43bis, §3, 7° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

Les opérateurs visés à l'alinéa précédent seront 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.

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 1<sup>er</sup> ainsi que les conditions de conservation de ces données.

La délai de la conservation des données visées à l'alinéa 1<sup>er</sup> est douze mois. Après l'expiration de ce délai, les données sont détruites sans délai, sauf si pour la gestion habituelle de l'entreprise, d'autres délais légaux sont d'application.

Les opérateurs font en sorte que les données reprises à l'alinéa 1<sup>er</sup> soient accessibles de manière illimitée à partir de la Belgique.

§2. Nonobstant l'alinéa 4 du paragraphe 1<sup>er</sup>, dans les circonstances exceptionnelles comme visées à l'article 4, §2, le Roi peut, par arrêté délibéré en Conseil des Ministres, et après avis au 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 1<sup>er</sup>, le Roi fixe un délai de conservation supérieur à 24 mois, le Ministre notifie

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.

Wanneer de Europese Commissie binnen zes maanden na de in het tweede lid bedoelde kennisgeving geen besluit neemt, wordt de maatregel tot verlenging van de termijn beschouwd als goedgekeurd door de Commissie.”

§3. De minister en de minister van Justitie zorgen ervoor dat jaarlijks aan de Europese Commissie en het parlement statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of een openbaar communicatienetwerk. Die informatie heeft betrekking op:

- de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;
- 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;
- de gevallen waarin verzoeken niet konden worden ingewilligd.

De gegevens die betrekking hebben op de toepassing van §1, a) worden tevens gevoegd aan het verslag dat de minister van Justitie overeenkomstig artikel 90decies van het Wetboek van strafvordering uitbrengt aan het Parlement.

§4. Twee jaar na de inwerkingtreding van het Koninklijk Besluit bedoeld in §1, derde lid, brengen de minister en de minister van Justitie aan de wetgevende kamers een evaluatieverslag uit over de toepassing van dit artikel en het Koninklijk Besluit, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de bewaringstermijn en de te bewaren gegevens.

**Artikel 4.** In artikel 145 van dezelfde wet wordt een § 3ter ingevoegd, luidend als volgt:

immédiatement à la Commission européenne et aux autres Etats membres de l’Union européenne toute mesure prise, accompagnée de sa motivation.

En l’absence de décision de la Commission européenne dans les six mois suivant la notification visée à l’alinéa 2, la mesure de prolongation du délai est réputée approuvée par la Commission. »

§3. 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 de communications électroniques accessibles au public ou de réseaux publics de communications soient transmises annuellement à la Commission européenne et au Parlement. Ces statistiques comprennent notamment :

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;
- 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 ;
- les cas dans lesquels des demandes de données n’ont pu être satisfaites.

Les données qui concernent l’application du §1<sup>er</sup>, a) seront également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l’article 90decies du Code d’instruction criminelle.

§4. Deux ans après l’entrée en vigueur de l’arrêté royal visé au §1<sup>er</sup>, alinéa 3, le ministre et le ministre de la Justice font un rapport d’évaluation aux Chambres législatives sur la mise en œuvre de cet article et de l’arrêté royal, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne la durée de la conservation et les données à conserver.

**Article 4.** Dans l’article 145 de la même loi, il est inséré un paragraphe 3ter rédigé comme suit :

“§ 3ter. 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 ander persoon onthult of verspreidt, of er enig gebruik van maakt.

**Artikel 5.** Artikel 90decies van het Wetboek van Strafvordering wordt aangevuld met een lid, luidend als volgt:

“In dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, §3, tweede lid van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Gegeven te [Plaats], [datum].

Van Koningswege,

De Minister voor Ondernemingen en Vereenvoudigen,

Vincent Van Quickenborne

De Minister van Justitie,

Stefaan De Clerck

“§ 3ter. 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. »

**Article 5.** L'article 90decies du Code d'instruction criminelle est complété par un alinéa, libellé comme suit :

A ce rapport est joint le rapport dressé en application de l'article 126, §3, alinéa 2 de la loi du 13 juin 2005 relative aux communications électroniques.

Donné à [Lieu], le [date].

Par le Roi,

Le Ministre pour l'Entreprise et la Simplification,

Vincent Van Quickenborne

De Minister van Justitie,

Stefaan De Clerck