SERVICE PUBLIC FEDERAL ECONOMIE, P.M.E., CLASSES MOYENNES ET ENERGIE ET SERVICE PUBLIC FEDERAL JUSTICE

[C − 2013/11510]

19 SEPTEMBRE 2013. — Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques

RAPPORT AU ROI

Sire,

La Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 *sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques et modifiant la Directive 2002/58/CE* (ci-après « la directive ») a été publiée au *Journal officiel de l'Union européenne* du 13 avril 2006 (*J.O.C.E.*, L105, pp. 54-63).

Cette directive vise principalement à réduire les disparités législatives et techniques existant au sein des différents Etats membres de l'Union en ce qui concerne les dispositions relatives à la conservation de données en vue de la recherche, de la détection et de la poursuite d'infractions pénales graves.

Cette directive est partiellement transposée par :

- l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après « la LCE »);

- l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demande judiciaires concernant les communications électroniques.

Le présent arrêté complète et achève la transposition en portant exécution de l'article 126.

L'article 126, § 2, alinéa 1er, de la LCE prévoit cette conservation en vue de la recherche, de la détection et de la poursuite d'infractions pénales visées aux articles 46*bis* et 88*bis* du *Code d'instruction criminelle*, en vue de la répression d'appels malveillants vers les services d'urgence, en vue de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques et en vue de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

L'article 126 de la LCE habilite le Roi à fixer :

- les données à conserver (voir paragraphes 1er et 2 des articles 3 à 6);

- les données qui sont soumises à l'article 126, § 3, alinéa 1er, et celles qui sont soumises à l'alinéa 2 du même paragraphe (voir paragraphe 3 des articles 3 à 6);

- les exigences auxquelles ces données doivent répondre (article 7);

- les mesures techniques et administratives que les fournisseurs de réseaux et services concernés doivent prendre en vue garantir la protection des données à caractère personnelle (article 8);

- les statistiques que ces fournisseurs transmettent à l'Institut belge des services postaux et des télécommunications (ci-après « IBPT ») et celles que l'IBPT transmet au ministre et au ministre de la Justice (article 9).

L'article 5 de la directive établit la liste minimale des données à conserver en les regroupant par catégories selon qu'il s'agit de données nécessaires pour : *a)* retrouver et identifier la source d'une communication, *b)* identifier la destination d'une communication, *c)* déterminer la date, l'heure et la durée d'une communication, *d)* déterminer le type de communication, *e)* identifier le matériel de communication utilisé et *f)* localiser le matériel de communication mobile.

L'article 5.1. de la directive prévoit des sous-catégories au sein de chacune de ces catégories sur la base du type de service de communications électroniques visé. Les sous-catégories visent ainsi la téléphonie fixe en réseau, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet et la téléphonie par Internet.

FEDERALE OVERHEIDSDIENST ECONOMIE, K.M.O., MIDDENSTAND EN ENERGIE EN FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2013/11510]

19 SEPTEMBER 2013. — Koninklijk besluit tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie

VERSLAG AAN DE KONING

Sire,

Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 *betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische-communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG* (hierna "de richtlijn") is gepubliceerd in het *Publicatieblad van de Europese Unie* van 13 april 2006 (*PbEG*, L105, blz. 54-63).

Die richtlijn is er voornamelijk op gericht om de wetgevende en technische verschillen te verminderen die onder de verschillende lidstaten van de Unie bestaan wat betreft de bepalingen met betrekking tot de bewaring van gegevens met het oog op het onderzoek, de opsporing en vervolging van zware strafbare feiten.

Die richtlijn wordt gedeeltelijk omgezet door :

- artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna "de WEC");

- het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie.

Dit besluit vormt de aanvulling en afronding van de omzetting door uitvoering te geven aan artikel 126.

Artikel 126, § 2, eerste lid, van de WEC schrijft deze bewaring voor met het oog op het onderzoek, de opsporing en de vervolging van strafbare feiten bedoeld in de artikelen 46*bis* en 88*bis* van het *Wetboek van strafvordering*, maar ook met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, en met het oog op het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische-communicatienetwerk of -dienst en om ten slotte de inlichtingenopdrachten te vervullen waarbij gebruik wordt gemaakt van de methodes voor gegevensverzameling bedoeld in de artikelen 18/7 en 18/8 van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Artikel 126 van de WEC verleent de Koning de bevoegdheid om het volgende vast te stellen :

- de te bewaren gegevens (zie de paragrafen 1 en 2 van de artikelen 3 tot 6);

- de gegevens die onderworpen zijn aan artikel 126, § 3, eerste lid, en die welke onderworpen zijn aan het tweede lid van dezelfde paragraaf (zie paragraaf 3 van de artikelen 3 tot 6);

- de eisen waaraan deze gegevens moeten voldoen (artikel 7);

- de technische en administratieve maatregelen die de betrokken aanbieders van netten en diensten moeten nemen om de persoonsgegevens te beschermen (artikel 8);

- de statistieken die deze aanbieders bezorgen aan het Belgisch Instituut voor postdiensten en telecommunicatie (hierna "BIPT") en diegene die het BIPT overzendt aan de minister en aan de minister van Justitie (artikel 9).

Artikel 5 van de richtlijn stelt de minimumlijst op van de te bewaren gegevens, onderverdeeld in categorieën naargelang het gaat om gegevens die nodig zijn om : *a)* de bron van een communicatie te vinden en te identificeren, *b)* de bestemming van een communicatie te identificeren, *c)* de datum, het tijdstip en de duur te bepalen van een communicatie, *d)* het type communicatie te bepalen, *e)* de gebruikte communicatieapparatuur te identificeren en *f)* de locatie te bepalen van de mobiele-communicatieapparatuur.

Artikel 5.1. van de richtlijn voorziet in subcategorieën binnen elk van deze categorieën op basis van het bedoelde type van elektronische-communicatiedienst. De subcategorieën zijn aldus gericht op telefonie over een vast netwerk, de mobiele telefonie, internettoegang, e-mail over internet en internettelefonie.

Le présent arrêté présente les données à conserver autrement que dans l'article 5 de la directive.

En effet, il fait d'abord une distinction par type de services et réseaux publics de communications électroniques. Ainsi, l'arrêté distingue :

- les fournisseurs au public de services de téléphonie fixe, à l'exception de la téléphonie par internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 3);

- les fournisseurs au public de services de téléphonie mobile, à l'exception de la téléphonie par internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 4);

- les fournisseurs au public de services d'accès à l'internet, à l'exception du courrier électronique par internet accessible au public et de la téléphonie par l'internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 5);

- les fournisseurs au public de services de courrier électronique par internet et de téléphonie par l'internet accessibles au public, à l'exception de l'accès à l'internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 6).

Deux sous-catégories sont prévues selon le type de données à conserver pour chacune des catégories de fournisseurs susvisées.

Il s'agit d'une part des données qui sont liées à l'abonnement, à l'inscription au service ou à l'utilisation du service et qui permettent d'identifier l'utilisateur final, le service de communications utilisé et l'équipement terminal qui est présumé avoir été utilisé (ci-après la première catégorie de données). Ces données sont visées au paragraphe 1er des articles 3, 4, 5 et 6 de l'arrêté. Comme ces données ne varient pas ou peu, elles sont relativement « statiques ».

Il s'agit d'autre part des données de trafic et de localisation au sens des articles 2, 6° (données de trafic) et 2, 7° (données de la localisation) de la LCE (ci-après la seconde catégorie de données). Ces données sont visées au paragraphe 2 des articles 3, 4, 5 et 6 de l'arrêté. Ces données fluctuent constamment selon les communications et ont donc une nature « dynamique ».

L'article 1.2 de la directive prévoit d'ailleurs *« qu'elle s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré »*. Le présent arrêté vise les données de localisation et de trafic (§ 2 des articles 3 à 6) ainsi que les données d'identification des utilisateurs finals, du service de communications électroniques utilisé et de l'équipement terminal qui est présumé avoir été utilisé (§ 1er des articles 3 à 6). Le but ultime de l'identification de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé est de pouvoir identifier les utilisateurs finals participant à la communication électronique.

Les données devraient être conservées de manière à éviter qu'elles ne soient conservées plus d'une fois. Le fournisseur de réseau ou de service concerné se chargera de conserver, pour chaque communication, le numéro ou l'identifiant attribué à l'utilisateur final afin de pouvoir mettre en relation les données de trafic et de localisation avec les données d'identification.

Par ailleurs, le présent arrêté dépasse quelque peu le cadre minimum fixé par la directive pour les raisons suivantes.

Il s'agit d'abord 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.

Ensuite, le cadre européen ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de prévention, de recherche, de détection et de poursuite d'infractions pénales. Ainsi, le présent arrêté vise par exemple certaines données indispensables en vue de l'identification des personnes concernées par une communication pertinente dans le cadre d'une enquête en matière répressive - telles que les données relatives au paiement – qui ne figurent pas à la liste établie par la directive.

Il faut enfin souligner que la directive a été adoptée le 15 mars 2006. Entretemps, des évolutions technologiques et économiques ont eu lieu et ont été prises en compte dans le présent arrêté. On pense à cet égard

Het onderhavige besluit stelt de gegevens voor die anders moeten worden bewaard dan in artikel 5 van de richtlijn.

Het maakt immers eerst een onderscheid per soort van openbare dienst en openbaar netwerk voor elektronische communicatie. Zo onderscheidt het besluit :

- de aanbieders van openbare diensten voor vaste telefonie, met uitzondering van openbare internettelefonie, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie (artikel 3);

- de aanbieders van openbare diensten voor mobiele telefonie, met uitzondering van openbare internettelefonie, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie (artikel 4);

- de aanbieders van openbare diensten voor internettoegang, met uitzondering van openbare e-mail via het internet en openbare internettelefonie, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie (artikel 5);

- de aanbieders van openbare diensten voor e-mail via het internet en openbare internettelefonie, met uitzondering van openbare internettoegang, en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie (artikel 6).

Er worden twee subcategorieën gemaakt volgens het soort van te bewaren gegevens voor elke categorie van de hierboven bedoelde aanbieders.

Het gaat enerzijds om de gegevens die verband houden met het abonnement, de inschrijving op de dienst of het gebruik van de dienst en die het mogelijk maken om de eindgebruiker, de gebruikte communicatiedienst en de eindapparatuur die vermoed wordt te zijn gebruikt te identificeren (hierna de eerste categorie van gegevens). Deze gegevens worden bedoeld in paragraaf 1 van de artikelen 3, 4, 5 en 6 van het besluit. Aangezien deze gegevens niet of weinig variëren, zijn ze "statisch".

Anderzijds gaat het om verkeers- en locatiegegevens in de zin van de artikelen 2, 6° (verkeersgegevens) en 2, 7° (locatiegegevens) van de WEC (hierna de tweede categorie van gegevens). Deze gegevens worden bedoeld in paragraaf 2 van de artikelen 3, 4, 5 en 6 van het besluit. Deze gegevens fluctueren constant volgens de communicatie en zijn dus "dynamisch" van aard.

Artikel 1.2 van de richtlijn luidt trouwens : *"Deze richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren"*. Het onderhavige besluit is gericht op de locatie- en verkeersgegevens (§ 2 van de artikelen 3 tot 6) alsook op de gegevens voor de identificatie van de eindgebruikers, van de gebruikte elektronische-communicatiedienst en van de eindapparatuur die vermoed wordt te zijn gebruikt (§ 1 van de artikelen 3 tot 6). Het uiteindelijke doel van de identificatie van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst bestaat erin om de eindgebruikers die deelnemen aan de elektronische communicatie, te kunnen identificeren.

De identificatiegegevens zouden op zo'n manier moeten worden bewaard dat ze maar één keer meer worden bewaard. De aanbieder van het betrokken netwerk of de betrokken dienst zal de taak op zich nemen om voor elke communicatie het toegewezen nummer of de toegewezen eindgebruikersidentificatie te bewaren, om het verband te kunnen leggen tussen de verkeers- of locatiegegevens en de identificatiegegevens.

Overigens overstijgt het onderhavige besluit enigszins het minimale kader dat vastgelegd is door de richtlijn om de volgende redenen.

Allereerst komt het erop aan een aantal lacunes in het Europese kader in te vullen. De Europese richtlijn werd immers in een spoedtempo uitgewerkt waardoor een aantal zaken over het hoofd werden gezien.

Het Europese kader voldoet bovendien niet noodzakelijk aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor de preventie, het onderzoek, de opsporing en de vervolging van strafbare feiten. Zo beoogt het onderhavige besluit bijvoorbeeld bepaalde gegevens die onmisbaar zijn bij de identificatie van personen betrokken bij een relevante communicatie in het kader van een strafrechtelijk onderzoek - zoals gegevens inzake betaling - die ontbreken in de door de richtlijn opgestelde lijst.

Ten slotte moet worden benadrukt dat de richtlijn aangenomen is op 15 maart 2006. Ondertussen hebben er zich technologische en economische ontwikkelingen voorgedaan, waarmee in het onderhavige

en particulier à la conservation des ports source suite au partage d'une adresse IP entre plusieurs utilisateurs finals.

Si le présent arrêté ne complètait pas la liste de la directive par un nombre limité de données supplémentaires, l'efficacité de la rétention de données s'en trouverait diminuée.

La directive a été prise sur base de l'article 95 (et non 94) du Traité instituant la Communauté européenne (actuellement l'article 114 du Traité sur le fonctionnement de l'Union européenne), ce qui permet d'aller plus loin que ce que prévoit la directive. Par ailleurs, l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques* (ci-après « directive vie privée et communications électroniques ») permet aux Etats membres d'adopter des mesures réglementaires prévoyant la conservation de données pendant une durée limitée lorsque c'est justifié par un des motifs énumérés dans cet article. A cet égard, le considérant 12 de la directive prévoit que « *l'article 15, paragraphe 1er, de la Directive 2002/58/CE continue à s'appliquer aux données, y compris à celles relatives aux appels téléphoniques infructueux, dont la conservation n'est pas expressément requise par la présente directive et qui ne relèvent donc pas de son champ d'application, ainsi qu'à la conservation de données à d'autres fins que celles prévues par la présente directive, notamment à des fins judiciaires.* » Le présent arrêté royal s'appuye sur l'article 15.1 de la directive « vie privée et communications électroniques » pour ce qui concerne les données non prévues dans la directive.

Les données demandées en plus de celles figurant sur la liste de la directive portent principalement sur l'identification des parties concernées, en particulier sur la source de la communication.

L'objectif de l'identification par une autorité compétente est de retrouver le véritable utilisateur final d'un service de communication. Cette identification implique évidemment la nécessité de conserver les données personnelles de l'utilisateur final. 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 communications électroniques.

Ces données supplémentaires mettent les autorités non seulement sur la piste de l'utilisateur final effectif mais elles leur 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 principalement l'utilisateur final et non les données de trafic. La conservation de ces données est toutefois nécessaire pour permettre une utilisation judicieuse des données de trafic conservées. Les données dont la conservation est demandée sont pour la plupart 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 communications électroniques considéré doivent fournir aux autorités des indices complémentaires quant à l'utilité d'une demande d'information auprès d'un opérateur : les services supplémentaires auquel l'utilisateur final est abonné, le commencement et la fin de l'abonnement, l'opérateur précédent en cas de portabilité du numéro.

Ces données sont également limitées en nombre et sont, elles aussi, déjà conservées chez les opérateurs.

Par ailleurs, le considérant 23 de la directive prévoit qu' « *étant donné que les obligations incombant aux fournisseurs de services de communications électroniques devraient être proportionnées, la présente directive leur prescrit de ne conserver que les données qui sont générées ou traitées lors de la fourniture de services de communication. Dans les cas où ces données ne sont pas générées ou traitées par ces fournisseurs, il n'y a pas d'obligation de les conserver.* ». De la même manière, les fournisseurs de réseaux de communications électroniques publics ne sont tenus de conserver les

besluit rekening wordt gehouden. Daarbij wordt in het bijzonder gedacht aan de bewaring van de bronpoorten na het delen van een IP-adres onder verschillende eindgebruikers.

Indien dit besluit de lijst van de richtlijn zelf niet verder zou aanvullen met een beperkt aantal bijkomende gegevens, zou de effectiviteit van de dataretentie ondergraven worden.

De richtlijn is aangenomen op basis van artikel 95 (en niet 94) van het Verdrag tot oprichting van de Europese Gemeenschap (nu artikel 114 van het Verdrag betreffende de werking van de Europese Unie), wat het mogelijk maakt verder te gaan dan wat de richtlijn voorschrijft. Overigens stelt artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 *betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie* (hierna "richtlijn betreffende privacy en elektronische communicatie") de lidstaten in staat om bestuursrechtelijke bepalingen aan te nemen die voorzien in de bewaring van gegevens gedurende een beperkte periode, wanneer dat gerechtvaardigd is door één van de redenen die in dat artikel worden opgesomd. In dat opzicht luidt considerans 12 van de richtlijn als volgt : "*Artikel 15, lid 1, van Richtlijn 2002/58/EG blijft van toepassing op gegevens, met inbegrip van gegevens met betrekking tot oproeppogingen zonder resultaat, die ingevolge de huidige richtlijn niet specifiek moeten worden bewaard en derhalve niet onder het toepassingsgebied daarvan, alsook voor bewaring van gegevens voor doelstellingen, inclusief van justitiële aard, andere dan die welke onder deze richtlijn vallen.*" Dit koninklijk besluit berust op artikel 15.1 van de Richtlijn "privacy en elektronische communicatie" wat betreft de gegevens waarin deze richtlijn niet voorziet.

De gegevens die gevraagd worden bovenop de lijst van de richtlijn, hebben voornamelijk te maken met de identificatie van de betrokken partijen, in het bijzonder met de bron van de communicatie.

Het doel van een identificatie door een bevoegde overheid is het achterhalen van de reële eindgebruiker van een communicatiedienst. Deze identificatie houdt vanzelfsprekend in dat men de persoonsgegevens van de eindgebruiker 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 de autoriteiten op het spoor van de daadwerkelijke eindgebruiker maar ze kunnen tevens uitsluiten dat slachtoffers van identiteitsfraude onterecht worden betrokken als dader in een gerechtelijk dossier dat geen betrekking heeft op hen. 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 voornamelijk betrekking hebben op de eindgebruiker 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 voor het merendeel door de operatoren bijgehouden als klantengegevens.

Politie en justitie maken er ook vandaag al gebruik van en konden in verschillende gevallen toch op het spoor komen van criminelen die, binnen het kader van georganiseerde criminaliteit, gebruik maakten van schijnbaar anonieme mobiele of internetverbindingen.

Een aantal bijkomende gegevens over het abonnement voor de beschouwde elektronische-communicatiedienst moeten de autoriteiten bijkomende aanwijzingen geven over het nut van een bevraging bij een operator : de bijkomende diensten waarop de eindgebruiker is geabonneerd, het begin en einde van een abonnement, de vorige operator bij nummeroverdraagbaarheid.

Ook deze gegevens zijn beperkt in omvang en worden nu ook bijgehouden bij de operatoren.

Bovendien bepaalt considerans 23 van de richtlijn : "*Aangezien de verplichtingen voor aanbieders van elektronische-communicatiediensten evenredig dienen te zijn, eist deze richtlijn dat zij alleen gegevens bewaren die gegenereerd of verwerkt worden in het kader van het aanbieden van hun communicatiediensten. Wanneer dergelijke gegevens niet worden gegenereerd bij of verwerkt door deze aanbieders, is er geen verplichting ze te bewaren.*". Op dezelfde manier zijn de aanbieders van openbare elektronische-communicatienetwerken maar verplicht om de gegevens te bewaren in

données que dans la mesure où ils les génèrent ou les traitent. Ce principe est rappelé à l'article 126, § 1er, alinéa 1er, de la loi du 13 juin 2005, tel que modifié par la loi du 30 juillet 2013, qui impose à certains fournisseurs de conserver uniquement certaines données qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications électroniques. Par conséquent, les données à conserver en vertu des articles 3 à 6 du présent arrêté ne doivent être conservées par un fournisseur de réseau ou de service que s'il traite ou génère cette donnée.

A titre d'illustration : le présent arrêté royal prévoit la conservation par les fournisseurs non seulement des données concernant leurs abonnés mais également des données concernant le destinataire de la communication (voir article 3, § 2, 2°, pour la téléphonie fixe, l'article 4, § 2, 4°, pour la téléphonie mobile et l'article 6, § 2, 3°, b, pour l'e-mail). A part le numéro de téléphone ou l'adresse électronique que l'auteur de la communication a utilisé pour atteindre le destinataire de la communication, un fournisseur d'un abonné (ci-après le fournisseur *A)* ne connaît pas les données concernant le destinataire de la communication lorsque ce dernier est l'abonné d'un autre fournisseur (ci-après le fournisseur *B)*. Dès lors qu'il ne connaît pas ces données, il ne les traite pas ni ne les génère. Par conséquent, il ne doit pas les conserver. Par contre, comme le fournisseur A connaît tout de même le numéro de téléphone et l'adresse électronique susmentionné et les traite, il devra les conserver. Par ailleurs, il reviendra au fournisseur B de conserver les données relatives au destinataire de la communication ainsi que le numéro de téléphone de l'appelant ou l'adresse électronique de l'auteur de la communication. Ces différentes données (numéros de téléphone de l'appelant et de l'appelé et adresses électroniques de l'auteur et du destinaire de la communication) permettent aux autorités d'établir le lien entre les participants à la communication.

Lorsqu'une donnée n'est pas disponible ou n'existe pas, il n'y a pas d'obligation de la conserver, dès que le fournisseur ne la traite pas ni ne la génère. Ainsi, à titre d'illustration, l'article 5, § 2, 6°, du présent arrêté oblige les fournisseurs à conserver « les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée. » Si ces données n'existent pas ou ne sont pas disponibles, les fournisseurs ne doivent pas les conserver. Si c'est le fournisseur du service concerné qui traite ou génère une donnée mais non le fournisseur du réseau sous-jacent, ce dernier fournisseur ne sera pas tenu de conserver la donnée en question.

L'avis 53.841/2/V du 26 août 2013 du Conseil d'Etat a été globalement suivi. La prise en compte de cet avis appelle les explications suivantes :

1) Le Conseil d'Etat estime qu'il ne ressort pas du dossier qui lui a été transmis que l'examen préalable de la nécessité de procéder à une évaluation d'incidence au sens de l'article 19/1 de la loi du 5 mai 1997 relative à la coordination de la politique fédérale de développement durable (dit test « EIDD ») a bien été réalisé.

L'article 2, 3°, de l'arrêté royal du 20 septembre 2012 portant exécution de l'article 19/1, § 1er, deuxième alinéa, du chapitre V/1 de la loi du 5 mai 1997 précitée dispense d'un examen préalable « la réglementation envisagée portant transposition d'une directive de l'Union européenne qui a fait l'objet d'une analyse d'impact similaire à une évaluation d'incidence, visée à l'article 2, 9°, de la loi ». C'est le cas pour le présent arrêté royal, dès lors que le texte de la directive avait été soumis à une évaluation de qualité sur les impacts sur le développement durable (avis du 19 janvier 2006 du Comité économique et social européen).

2) Selon le Conseil d'Etat, les articles 4, § 3, 5, § 3, 6, § 3, et 7, § 3, (actuellement les articles 3, § 3, 4, § 3, 5, § 3 et 6, § 3) paraphrasent l'article 126, § 3, alinéas 1er et 2 et doivent donc être omis.

Les articles 4, § 3, 5, § 3, 6, § 3, et 7, § 3, actuellement les articles 3, § 3, 4, § 3, 5, § 3 et 6, § 3) ont été modifiés pour ne plus paraphraser l'article 126, § 3, alinéas 1er et 2 de la LCE. Cependant ces articles ne peuvent pas être simplement omis. En effet, l'article 126, § 3, alinéa 3, de la LCE prévoit : « Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises à l'alinéa 1er et celles qui le sont à l'alinéa 2. ».

3) Selon le Conseil d'Etat, l'article 126 de la LCE se réfère à l'identification des utilisateurs finals alors que le projet d'arrêté royal se réfère à l'identification des abonnés et des utilisateurs.

de mate waarin ze deze genereren of verwerken. Aan dit principe wordt herinnerd door artikel 126, § 1, eerste lid, van de wet van 13 juni 2005, zoals gewijzigd door de wet van 30 juli 2013, dat aan sommige aanbieders de verplichting oplegt om enkel bepaalde gegevens te bewaren die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de elektronische-communicatiediensten. Bijgevolg moeten de krachtens de artikelen 3 tot 6 van het onderhavige besluit te bewaren gegevens, slechts worden bewaard door een netwerk- of dienstenaanbieder als hij dat gegeven verwerkt of genereert.

Ter illustratie : het onderhavige koninklijk besluit voorziet in de bewaring door de aanbieders van niet alleen gegevens betreffende hun abonnees maar ook van gegevens over de bestemmeling van de communicatie (zie artikel 3, § 2, 2°, voor vaste telefonie, artikel 4, § 2, 4°, voor mobiele telefonie en artikel 6, § 2, 3°, b, voor e-mail). Behalve het telefoonnummer of elektronisch adres die de initiatiefnemer van de communicatie heeft gebruikt om de bestemmeling van de communicatie te bereiken, kent een aanbieder van een abonnee (hierna aanbieder A genoemd) niet de gegevens over de bestemmeling van de communicatie wanneer deze laatste bij een andere aanbieder (hierna aanbieder *B)* geabonneerd is. Daar hij deze gegevens niet kent, worden deze door hem noch verwerkt noch gegenereerd. Bijgevolg hoeft hij ze niet te bewaren. Wanneer aanbieder A daarentegen toch het telefoonnummer en het voormelde elektronische adres kent en ze verwerkt, zal hij ze moeten bewaren. Bovendien is het de taak van aanbieder B om de gegevens over de bestemmeling van de communicatie te bewaren, alsook het telefoonnummer van de oproeper of het elektronische adres van de initiatiefnemer van de communicatie. Deze verschillende gegevens (telefoonnummers van de oproeper en van de opgeroepene en elektronische adressen van de initiatiefnemer en van de bestemmeling van de communicatie) stellen de autoriteiten in staat om de link te leggen tussen de partijen die bij de communicatie betrokken zijn.

Wanneer een gegeven niet beschikbaar is of niet bestaat, is er geen verplichting om het te bewaren, zodra de aanbieder het niet verwerkt noch genereert. Ter illustratie : artikel 5, § 2, 6°, van het onderhavige besluit verplicht de aanbieders om "de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt" te bewaren. Als deze gegevens niet bestaan of onbeschikbaar zijn, moeten de aanbieders ze niet bewaren. Als een gegeven wordt verwerkt of gegenereerd door de aanbieder van de betreffende dienst, maar niet door de aanbieder van het onderliggende netwerk, dan is deze laatste aanbieder niet verplicht om het gegeven in kwestie te bewaren.

Het advies 53.841/2/V van 26 augustus 2013 van de Raad van State is volledig gevolgd. Het rekening houden met dit advies geeft aanleiding tot de volgende verklaringen :

1) De Raad van State oordeelt dat uit het dossier dat hem werd bezorgd niet blijkt dat voorafgaand de noodzaak is onderzocht om over te gaan tot een impactanalyse in de zin van artikel 19/1 van de wet van 5 mei 1997 betreffende de coördinatie van het federale beleid inzake duurzame ontwikkeling ("DOEB"-test genoemd).

Artikel 2, 3°, van het koninklijk besluit van 20 september 2012 houdende uitvoering van artikel 19/1, § 1, tweede lid, van hoofdstuk V/1 van de genoemde wet van 5 mei 1997, stelt de "voorgenomen regelgeving houdende omzetting van een richtlijn van de Europese Unie die al aan een impactanalyse onderworpen werd gelijkaardig aan de effectbeoordeling, bedoeld in artikel 2, 9°, van de wet" van een voorafgaand onderzoek vrij. Dat is het geval voor het huidige koninklijk besluit aangezien de tekst van de richtlijn aan een kwaliteitsanalyse over de impact op de duurzame ontwikkeling (advies van 19 januari 2006 van het Europese Economische en Sociale Comité) is onderworpen.

2) Volgens de Raad van State moeten de artikels 4, § 3, 5, § 3, 6, § 3, en 7, § 3, (nu de artikels 3, § 3, 4, § 3, 5, § 3 en 6, § 3) weggelaten worden daar zij artikel 126, § 3, eerste en tweede lid, parafraseren.

De artikels 4, § 3, 5, § 3, 6, § 3, en 7, § 3, (nu de artikels 3, § 3, 4, § 3, 5, § 3 en 6, § 3), werden gewijzigd zodat zij het artikel 126, § 3, eerste en tweede lid, van de WEC niet meer parafraseren. Deze artikels kunnen echter niet simpelweg weggelaten worden. Artikel 126, § 3, derde lid, van de WEC luidt immers : "De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de gegevens die zijn onderworpen aan het eerste lid en deze die zijn onderworpen aan het tweede lid.".

3) Volgens de Raad van State verwijst artikel 126 van de WEC naar de identificatie van de eindgebruikers terwijl het ontwerp van koninklijk besluit verwijst naar de identificatie van abonnees en gebruikers.

La notion d'utilisateur dans le projet d'arrêté royal doit en effet être remplacée par la notion d'utilisateur final, qui est également visée par l'article 126 de la LCE. Il est vrai que la directive se réfère à la définition d'utilisateur, mais elle contient sa propre définition d'utilisateur, qui est la suivante : « toute entité juridique ou personne physique qui utilise un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service » (article 2, *b)*. Or cette définition est plus proche de la définition d'utilisateur final au sens de la LCE (article 2, 13°) que de la définition d'utilisateur au sens de cette même loi (article 2, 12°).

Il n'est pas nécessaire de viser l'utilisateur enregistré comme le mentionne à certains endroits la directive. En effet, un fournisseur ne devra conserver des données que s'il les traite ou les génère (cf. supra). Par conséquent, si un fournisseur ne dispose pas d'une donnée d'un utilisateur final, car ce dernier n'est pas enregistré, il ne doit pas conserver cette donnée.

Il n'est pas nécessaire non plus de mentionner l'utilisateur final et l'abonné car la notion d'utilisateur final (article 2, 13°, de la LCE) inclut la notion d'abonné (article 2, 15°, de la LCE).

4) Selon le Conseil d'Etat, il faut reprendre la définition de « numéro d'identifiant » inscrite à l'article 2, *d)*, de la directive.

C'est la définition en néerlandais « gebruikersidentificatie » de la directive qui a été préférée à la définition en français « numéro d'identifiant », car la définition en français semble constituer une mauvaise traduction par rapport aux autres versions linguistiques de la directive. Par ailleurs, comme indiqué ci-dessus, en droit belge, la notion « d'identifiant d'un utilisateur » utilisée par la directive doit être transposée par la notion d' « identifiant d'un utilisateur final ».

COMMENTAIRE DES ARTICLES

Article 1er.

Cet article ne nécessite pas de commentaire.

Article 2.

L'article deux définit quelques notions en vue de l'application du présent arrêté.

Les définitions d'*identifiant d'un utilisateur final* et d'*identifiant cellulaire* constituent une transposition de concepts définis dans l'article 2 de la directive.

L'identifiant cellulaire est défini comme « le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin ». Une cellule dans un réseau mobile est un secteur géographique dont la couverture radio est fournie par une station de base du réseau. Chaque cellule a une identification unique dans le réseau, appelée « Cell-ID » ou identifiant cellulaire, qui fait en sorte que chaque utilisateur final puisse être clairement localisé dans le réseau afin de router un appel vers la bonne antenne et d'ainsi établir la connexion entre l'appelant et l'appelé.

Alors que la directive vise les noms et adresse de l'abonné ou de l'utilisateur inscrit (voir article 5.1, *a)*, 1) , ii), article 5.1, *a)*, 2), iii), article 5.1., *b)*, 1), ii) et article 5.1., *b)*, 2), ii), l'article 1er, 7°, du présent arrêté définit les données personnelles comme « les nom et prénom ainsi que les adresses de facturation et de livraison de l'utilisateur final. »

La conservation des différentes adresses enregistrées auprès d'un opérateur, adresse(s) de livraison et de facturation, qui n'est pas prévue dans la directive, est demandée dans le présent arrêté pour les raisons suivantes.

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. Les autorités ont 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 a conduit les autorités à cette personne morale.

Il convient d'observer que de nombreuses notions utilisées dans le présent arrêté royal ont été définies dans la LCE.

La définition de service de téléphonie reprise à l'article 126 de la LCE est ainsi d'application pour le présent arrêté.

Article 3.

L'article 3 concerne les données que les fournisseurs de réseaux et services de téléphonie fixe accessibles au public, à l'exception de la téléphonie par Internet, doivent conserver.

Het begrip gebruiker in het ontwerp van koninklijk besluit moet inderdaad vervangen worden door het begrip eindgebruiker dat eveneens beoogd wordt in artikel 126 van de WEC. Het is inderdaad zo dat de richtlijn verwijst naar de definitie van gebruiker, maar zij bevat een eigen definitie van gebruiker, namelijk : "elke natuurlijke of rechtspersoon die, eventueel zonder geabonneerd te zijn op een openbare elektronische-communicatiedienst, daarvan gebruik maakt voor particuliere of zakelijke doeleinden" (artikel 2, *b)*. Nu leunt deze definitie dichter aan bij de definitie van eindgebruiker in de zin van de WEC (artikel 2, 13°) dan bij de definitie van gebruiker in de zin van dezelfde wet (artikel 2, 12°).

Het is niet nodig om de geregistreerde gebruiker te beogen zoals op sommige plaatsen in de richtlijn gebeurt. Een leverancier moet inderdaad alleen de gegevens bewaren wanneer hij ze behandelt of genereert (zie hoger). Dientengevolge, wanneer een leverancier niet over een gegeven van een eindgebruiker beschikt daar deze niet geregistreerd is, dan dient hij dat gegeven niet te bewaren.

Het is ook niet nodig de eindgebruiker en abonnee te vermelden daar het begrip eindgebruiker (artikel 2, 13°, van de WEC) het begrip abonnee (artikel 2, 15°, van de WEC) omvat.

4) Volgens de Raad van State moet de definitie "numéro d'identifiant" van artikel 2, *d)*, van de richtlijn hernomen worden.

Er werd voorkeur gegeven aan de Nederlandse definitie "gebruikersidentificatie" van de richtlijn tegenover de Franse definitie "numéro d'identifiant", daar de Franse definitie een slechte vertaling lijkt te zijn in vergelijking met de andere taalversies van de richtlijn. Zoals hierboven trouwens is aangegeven dient het begrip "gebruikersidentificatie" zoals gebruikt in de richtlijn, naar Belgisch recht omgezet te worden door het begrip "eindgebruikersidentificatie".

COMMENTAAR BIJ DE ARTIKELEN

Artikel 1

Dit artikel behoeft geen commentaar.

Artikel 2

Het tweede artikel definieert een aantal begrippen met het oog op de toepassing van het onderhavige besluit.

De definities van *eindgebruikersidentificatie* en van *celidentiteit* vormen een omzetting van begrippen die gedefinieerd zijn in artikel 2 van de richtlijn.

Celidentiteit wordt gedefinieerd als "de unieke code van een cel van waaruit een mobiele-telefonieoproep werd begonnen of beëindigd". Een cel in een mobiel netwerk is een geografische sector waarvan de radiodekking door een basisstation van het netwerk wordt verstrekt. Elke cel heeft een unieke identificatie in het netwerk, "Cell-ID" of celidentiteit genaamd, die ervoor zorgt dat elke eindgebruiker éénduidig in het netwerk kan worden gelokaliseerd zodat een oproep naar de correcte antenne kan worden gerouteerd om zo de verbinding tussen oproeper en opgeroepene te realiseren.

Terwijl de richtlijn doelt op de namen en het adres van de abonnee of van de ingeschreven gebruiker (zie artikel 5.1, *a)*, 1) , ii), artikel 5.1, *a)*, 2), iii), artikel 5.1., *b)*, 1), ii) en artikel 5.1., *b)*, 2), ii), definieert artikel 1, 7°, van het onderhavige besluit persoonsgegevens als "de naam en voornaam, en het facturatie- en het leveringsadres van de eindgebruiker."

De bewaring van de verschillende adressen die bij een operator zijn geregistreerd, leveringsadres en facturatieadres, waarin de richtlijn niet voorziet, wordt in het onderhavige besluit gevraagd om de volgende redenen.

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 stelden de autoriteiten vast dat een rechtspersoon instond voor de afhandeling van telefoon- of internetaansluitingen die werden gebruikt door criminelen. Het facturatieadres leidde de autoriteiten naar deze rechtspersoon.

Het dient opgemerkt te worden dat talrijke begrippen die gehanteerd worden door het onderhavige koninklijk besluit gedefinieerd zijn in de WEC.

Zo geldt de definitie van telefoniedienst van artikel 126 van de WEC voor het onderhavige besluit.

Artikel 3

Artikel 3 betreft de gegevens die de aanbieders van openbare vaste telefonienetwerken en -diensten, met uitzondering van internettelefonie, moeten bewaren.

La première catégorie de données (cf. supra et voir l'article 3, § 1er) vise entre autres les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. Les données d'identification de l'abonné ne dépendent pas de l'utilisation effective du service auquel il est abonné. Les autorités qui ont accès aux données conservées doivent pouvoir demander les données d'identification dès que l'abonnement est contracté, sans pour autant que l'abonné ait déjà effectivement utilisé ce service.

Les données visées à l'article 3, § 1er, 1° (le numéro attribué à l'utilisateur final) et 2° (les données personnelles de l'utilisateur final) correspondent à des données énumérées dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Les données visées à l'article 3, § 1er, 3° (la date de début de l'abonnement ou de l'enregistrement au service) et 5° (l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré) ne sont pas reprises dans la directive mais doivent être conservées pour les raisons suivantes.

Grâce à la libéralisation du marché des télécommunications, il est beaucoup plus facile pour les utilisateurs finals de téléphonie de changer d'opérateur tout en conservant leur numéro. Pour pouvoir s'informer auprès du bon opérateur, il importe que les services publics bénéficiaires de la conservation des données sachent précisément depuis quand l'utilisateur final est affilié à son opérateur actuel et quel était son opérateur d'origine en cas de transfert de numéro. Grâce à ces informations, les autorités (par exemple le juge d'instruction ou le procureur du Roi) peuvent 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.

Il n'est pas suffisant de savoir que le numéro a été porté d'un opérateur à un autre. Encore faut-il savoir quand cela a eu lieu. Cela est possible en connaissant la date de début de l'abonnement ou de l'enregistrement au service. De plus, la durée qui s'écoule entre la souscription à l'abonnement et son utilisation active peut donner une indication sur le profil de l'utilisateur final, qui peut constituer un indice utile pour les autorités.

En ce qui concerne la portabilité des numéros, le fournisseur auquel un numéro est transféré devra pouvoir fournir l'identité du fournisseur duquel il a reçu le numéro. Le fournisseur qui transfère le numéro doit également pouvoir identifier le fournisseur qui le reçoit. En d'autres termes, lorsqu'un numéro a été porté plusieurs fois, le dernier fournisseur à qui un numéro est transféré doit savoir de qui il reçoit ce numéro mais ne doit pas savoir qui est le premier fournisseur de la chaîne.

Les données visées à l'article 3, § 1er, 4° (le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit) vont un peu plus loin que ce que prévoit la directive qui vise « le service téléphonique utilisé » (article 5.1., *d)*, 1°), mais pas les services annexes.

Par « services annexes », on entend les services supplémentaires auxquels un client peut souscrire gratuitement, ou contre paiement. Par exemple : service de répondeur, fax, service SMS, déviation d'appel, formule particulière pour appeler à tarif avantageux certains numéros ou destinations, service de Calling Card, conversation à plusieurs, etc.

Ces services annexes fournissent aux autorités publics bénéficiaires de la conservation des données des indices utiles quant à l'utilité d'une demande d'information auprès d'un opérateur. Ainsi, à titre d'illustration, il est intéressant pour les autorités de savoir qu'un utilisateur final a souscrit à un service de déviation d'appel. Cela pourrait, par exemple, indiquer que les recherches des autorités doivent plutôt s'orienter vers le numéro vers lequel la déviation d'appel est effectuée.

Les données visées à l'article 3, § 1er, 6° (les données relatives au type de paiement ainsi qu'à l'identification et à la date de paiement de l'abonnement ou de l'utilisation du service) sortent du cadre des données visées par la directive mais représentent un réel intérêt dans le cadre d'une enquête, où ces quelques informations sont souvent la seule piste dont disposent les services de police afin de tenter

De eerste categorie van gegevens (cf. supra en zie artikel 3, § 1) betreft onder andere de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. De identificatiegegevens van de abonnee zijn niet afhankelijk van het daadwerkelijke gebruik van de dienst waarop hij geabonneerd is. De autoriteiten die toegang hebben tot de bewaarde gegevens, moeten de identificatiegegevens kunnen opvragen zodra het abonnement is afgesloten, ook zonder dat de abonnee daarvoor al werkelijk van deze dienst gebruik heeft gemaakt.

De gegevens bedoeld in artikel 3, § 1, 1° (het aan de eindgebruiker toegewezen nummer) en 2° (de persoonsgegevens van de eindgebruiker) stemmen overeen met gegevens die opgesomd zijn in de richtlijn (zie omzettingstabel). Bovendien wordt verwezen naar de opmerkingen in verband met artikel 1, 7° (definitie van "persoonsgegevens").

De gegevens bedoeld in artikel 3, § 1, 3° (de datum van aanvang van het abonnement of van de registratie voor de dienst) en 5° (de identiteit van de aanbieder die het nummer en de identiteit overdraagt van de aanbieder naar wie het nummer wordt overgedragen) zijn niet vermeld in de richtlijn, maar moeten worden bewaard om de volgende redenen.

Met de liberalisering van de telecommunicatiemarkt is het voor telefonie-eindgebruikers veel makkelijker om over te schakelen van één operator naar een andere met behoud van hun nummer. Om bij de juiste operator een bevraging te doen is het van belang voor de openbare diensten die baat hebben bij de bewaring van de gegevens om precies te weten sinds wanneer de eindgebruiker bij zijn huidige operator is aangesloten en van welke operator hij bij nummeroverdracht afkomstig was. Met deze informatie kunnen de autoriteiten (bijvoorbeeld de onderzoeksrechter of de procureur des Konings) 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 efficiëntere en gerichtere vraagstelling aan de operatoren. Ze zullen bijkomend voorkomen dat onnodige vraagstellingen de operatoren belasten en dat hierdoor hogere gerechtskosten worden gegenereerd.

Het volstaat niet om het nummer te kennen dat van de ene operator naar de andere is overgedragen. Bovendien moet bekend zijn wanneer dat is gebeurd. Dit is mogelijk als de datum van aanvang van het abonnement of de registratie voor de dienst bekend is. Bovendien kan de tijd die verloopt tussen het nemen van het abonnement en het actieve gebruik ervan een indicatie geven over het profiel van de eindgebruiker, die voor de autoriteiten een nuttige aanwijzing kan vormen.

Wat de nummeroverdraagbaarheid betreft, zal elke aanbieder naar wie een nummer is overgedragen de identiteit van de aanbieder van wie hij het nummer heeft ontvangen, moeten kunnen verstrekken. De aanbieder die het nummer overdraagt, moet ook de aanbieder die het ontvangt kunnen identificeren. Met andere woorden, wanneer een nummer meermaals overgedragen is, moet de laatste aanbieder naar wie een nummer is overgedragen, weten van wie hij dat nummer ontvangt, maar hoeft hij niet te weten wie de eerste aanbieder in de rij is.

De gegevens bedoeld in artikel 3, § 1, 4° (het soort van gebruikte vaste-telefoniedienst alsook de andere soorten van gebruikte diensten waarop de eindgebruiker ingeschreven heeft) gaan iets verder dan wat de richtlijn voorschrijft, die "de gebruikte telefoondienst" (artikel 5.1., *d)*, 1°) beoogt, maar niet de aanvullende diensten.

Onder "aanvullende diensten" wordt verstaan de aanvullende diensten waarop een klant gratis of tegen betaling kan intekenen. Bijvoorbeeld : antwoorddienst, fax, sms-dienst, doorschakeling van oproepen, bijzondere formule om tegen voordeeltarief bepaalde nummers of bestemmingen te bellen, Calling-Carddienst, groepsgesprek, enz.

Deze aanvullende diensten verstrekken de overheden die gebaat zijn bij de gegevensbewaring nuttige aanwijzingen over het nut van een verzoek om informatie bij een operator. Het is bijvoorbeeld interessant dat de autoriteiten weten dat een eindgebruiker geabonneerd is op een dienst voor oproepdoorschakeling. Dit zou bijvoorbeeld erop kunnen duiden dat het onderzoek van de autoriteiten eerder gericht moet zijn op het nummer waarnaar de oproep doorgeschakeld is.

De gegevens bedoeld in artikel 3, § 1, 6° (de gegevens betreffende type, identificatie en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst) vallen buiten het bestek van de gegevens die door de richtlijn worden beoogd, maar is werkelijk van belang in het kader van een onderzoek, waar dat kleine stukje informatie vaak de enige piste is waarover de politiediensten beschikken om een verdachte

d'identifier un suspect. Ces données de paiement sont parfois pour les autorités judiciaires et les services de renseignement et de sécurité la seule trace conduisant à l'utilisateur final d'un service de communications déterminé.

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.

Il est demandé aux opérateurs de conserver les données 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.

Il est demandé aux opérateurs de conserver les données de paiement des douze derniers mois afin de pouvoir également analyser l'unique trace éventuelle pouvant conduire à l'utilisateur final réel durant la période où les données de trafic sont conservées.

Les données demandées sont actuellement disponibles chez les opérateurs et sont régulièrement demandées par les autorités judiciaires. Ainsi, sur base des factures 2006 à 2011 contrôlées par le NTSU-CTIF et payées par la Justice aux opérateurs, on constate qu'il a été demandé aux opérateurs sur base des articles 46*bis* et 88*bis* du Code d'instruction criminelle en moyenne par an 309 fois une copie du contrat intitial (pour déterminer le moyen de paiement), 446 fois une copie des factures (pour les mêmes raisons) et près de 5 500 fois des informations sur la recharge d'une carte prépayée (en vue de déterminer le lieu et moyen de paiement).

Ces données de paiement constituent donc pour le magistrat une trace susceptible de le mener à l'utilisateur final pour lequel il pourra ensuite ouvrir une enquête auprès des organismes bancaires concernés.

Les explications ci-dessus valent également pour les articles 4, 5 et 6.

La deuxième catégorie de données vise les données qui auront été générées lors d'une communication (voir l'article 3, § 2 et supra). Toutes les données visées au paragraphe 2 de l'article 3 sont reprises dans la directive (voir tableau de transposition).

S'il y a eu déviation d'appel, il est nécessaire que le fournisseur de réseau ou service de communications électroniques puisse fournir le numéro vers lequel l'appel a été dévié. De même, si plusieurs appels ont lieu simultanément, les données de trafic et les données de localisation doivent être fournies pour chaque numéro appelé ou appelant.

Egalement pour cette deuxième catégorie, une description du type de service utilisé doit permettre de déterminer s'il s'agit d'un appel vocal ou alternativement de l'envoi ou de la réception d'un fax (un fax est transporté par un canal vocal et les opérateurs ne sont généralement pas en mesure de distinguer un fax d'un appel vocal, sans regarder le contenu des communications, ce qui est interdit), de l'envoi ou de la réception d'un sms, etc. Par exemple, en cas d'utilisation d'une *Calling Card*, l'utilisation de cette carte et des données qui s'y rapportent (comme le lieu d'appel) devront être conservés.

Conformément à l'article 126, § 3, alinéa 3, de la LCE, l'article 3, § 3, de l'arrêté royal précise le point de départ pour le calcul du délai de conservation des données précitées.

Il en est de même pour l'article 4, § 3, l'article 5, § 3, et l'article 6, § 3, ci-après.

Article 4.

L'article 4 concerne les données que les fournisseurs de réseaux ou services de téléphonie mobile accessibles au public, à l'exception de la téléphonie par l'internet, doivent conserver.

Les données visées à l'article 4, § 1er, 1° (le code IMSI), 2° (les données personnelles de l'utilisateur final) sont reprises dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Pour ce qui concerne les cartes prépayées, le présent arrêté royal n'a pas pour objet d'imposer aux fournisseurs ou aux points de vente d'obtenir les données personnelles visées à l'article 2, 7°, de l'utilisateur final lors de l'achat d'une carte prépayée. Une telle obligation n'a en effet pas sa place ici. Cependant, si le fournisseur dispose de ces données personnelles ou de certaines d'entre elles, il doit les conserver.

te proberen identificeren. Deze betalingsgegevens vormen voor de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten soms het enige spoor naar de eindgebruiker van een bepaalde communicatiedienst.

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.

Aan de operatoren wordt gevraagd de volgende gegevens te bewaren :

- type betaling (overschrijving, ATM, kredietkaartbetaling,...);

- identificatie van het betalingsmiddel (rekeningnummer, betaalkaartnummer,...);

- datum en tijdstip van de betaling.

Aan de operatoren wordt gevraagd de betalingsgegevens van de laatste twaalf maanden bij te houden om over de periode waarin de verkeersgegevens worden bijgehouden ook het mogelijk enige spoor naar de werkelijke eindgebruiker te kunnen onderzoeken.

De gegevens die worden gevraagd zijn vandaag beschikbaar bij de operatoren en worden regelmatig opgevraagd door de gerechtelijke overheden. Aldus stelt men op basis van de facturen 2006 tot 2011 die door NTSU-CTIF gecontroleerd zijn en betaald door Justitie aan de operatoren, vast dat aan de operatoren op grond van de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvorderingen gemiddeld 309 keer per jaar een kopie van het oorspronkelijke contract is gevraagd (om het betalingsmiddel te bepalen), 446 keer een kopie van de facturen (om dezelfde redenen) en bijna 5 500 keer informatie over de herlaadbeurt van een voorafbetaalde kaart (om de plaats en het betalingsmiddel te bepalen).

Deze betalingsgegevens vormen voor de magistraat dus het spoor naar de eindgebruiker waarvoor hij dan vervolgens een onderzoek kan instellen bij de betrokken bankinstellingen.

De bovenstaande toelichtingen gelden ook voor de artikelen 4, 5 en 6.

De tweede categorie van gegevens zijn de gegevens die tijdens een communicatie zullen zijn gegenereerd (zie artikel 3, § 2 en supra). Alle gegevens bedoeld in paragraaf 2 van artikel 3 zijn opgenomen in de richtlijn (zie omzettingstabel).

Als er een oproep is doorgeschakeld moet de aanbieder van een netwerk of dienst voor elektronische communicatie in staat zijn om het nummer te geven waarnaar de oproep is doorgeschakeld. Zo ook, indien er verschillende oproepen tegelijkertijd plaatshebben, moeten de verkeers- en locatiegegevens worden verstrekt voor elk oproepend of opgeroepen nummer.

Ook voor deze tweede categorie moet aan de hand van een beschrijving van het type van gebruikte dienst kunnen worden bepaald of het gaat om een gesprek of om de verzending of ontvangst van een fax (een fax wordt over een spraakkanaal verzonden en doorgaans zijn de operatoren niet in staat om een fax te onderscheiden van een gesprek, zonder de inhoud van de communicatie te bekijken, wat verboden is), de verzending of ontvangst van een sms, enz. Wanneer bijvoorbeeld een Calling Card wordt gebruikt, zal het gebruik van die kaart en de gegevens die er betrekking op hebben (zoals de plaats van de oproep) moeten worden bewaard.

Overeenkomstig artikel 126, § 3, derde lid, van de WEC, preciseert artikel 3, § 3, van het koninklijk besluit het startpunt voor de berekening van de bewaartermijn van bovenvermelde gegevens.

Hetzelfde geldt voor artikel 4, § 3, artikel 5, § 3, en artikel 6, § 3, hierna.

Artikel 4

Artikel 4 betreft de gegevens die de aanbieders van mobiele openbare telefonienetwerken of –diensten, met uitzondering van internettelefonie, moeten bewaren.

De gegevens bedoeld in artikel 4, § 1, 1° (de IMSI-code), 2° (de persoonsgegevens van de eindgebruiker) zijn opgenomen in de richtlijn (zie omzettingstabel). Bovendien wordt verwezen naar de opmerkingen in verband met artikel 1, 7° (definitie van "persoonsgegevens").

Wat voorafbetaalde kaarten betreft, heeft het onderhavige koninklijk besluit niet tot doel de aanbieders of de verkooppunten te verplichten om de persoonsgegevens bedoeld in artikel 2, 7°, van de eindgebruiker te verkrijgen bij aankoop van een voorafbetaalde kaart. Een dergelijke verplichting hoort hier immers niet thuis. Indien de aanbieder echter over die persoonsgegevens of enkele daarvan beschikt, dan moet hij die bewaren.

Pour ce qui concerne la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final (article 4, § 1er, 3°) et la portabilité des numéros (article 4, § 1er, 6°), les commentaires de l'article 3 s'appliquent *mutatis mutandis* à l'article 4. On ajoutera que le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final est une donnée utile pour les autorités.

Vu les canaux commerciaux, l'abonnement peut être souscrit ou l'enregistrement peut être effectué dans un magasin, un phoneshop ou un bureau local, où la copie originale du contrat signé est généralement également conservée. Toutes les données personnelles qui y sont indiquées ne sont pas nécessairement transmises à l'opérateur. C'est pourquoi il est intéressant de savoir où l'abonnement a été souscrit ou où l'enregistrement a eu lieu. Sur la base de l'écriture et de la signature, il est possible de vérifier si le contrat a réellement été conclu par la personne dont les coordonnées sont reprises dans le document ou si cette personne a été victime d'une usurpation d'identité.

Ce lieu est actuellement disponible chez les opérateurs et est régulièrement demandé par les autorités judiciaires. Ainsi, sur base des factures 2006 à 2011 contrôlées par le NTSU-CTIF et payées par la Justice aux opérateurs, on constate qu'il a été demandé aux opérateurs sur base des articles 46*bis* et 88*bis* du Code d'instruction criminelle en moyenne par an 60 fois le « point d'achat ».

Les données visées à l'article 4, § 1er, 4° (la date et l'heure de la première activation du service ainsi que l'identifiant cellulaire à partir duquel le service a été activé) correspondent au prescrit de la directive (voir article 5.1., *e)*, 2), vi), qui limite néanmoins cette donnée aux services anonymes à prépaiement.

Il est important de connaître avec exactitude le moment ainsi que l'endroit à partir desquels le service a été activé. Savoir quand la carte SIM a été achetée, et quand elle a été utilisée la première fois (3° et 4°) peut fournir des indices précieux aux enquêteurs. Cela vaut tant pour un abonnement régulier que pour un abonnement prépayé ou une carte prépayée. Par exemple, l'utilisation du service peut indiquer qu'un acte a été commis avec préméditation. L'absence d'utilisation du service peut indiquer un cas de fraude et une tentative de création d'une fausse identité.

Pour ce qui concerne les services annexes (article 4, § 1er, 5°), et les informations relatives au type de paiement (article 4, § 1er, 7°), données qui ne sont pas prévues dans la directive, les commentaires effectués à l'article 3 s'appliquent *mutatis mutandis* à l'article 4.

Par services annexes pour la téléphonie mobile, on entend les services supplémentaires auxquels un client peut souscrire gratuitement, ou contre paiement. Par exemple : service de répondeur, déviation d'appel, formule particulière pour appeler à tarif avantageux certains numéros ou destinations, conversation à plusieurs, etc. En ce qui concerne l'utilité de conserver ce type de données, il est renvoyé aux explications données pour l'article 3, § 1er, 4°.

Les données visées au paragraphe 2 de l'article 4 sont toutes reprises dans la directive, à l'exception de l'article 4, § 2, 6° et 7° de l'arrêté royal.

L'article 4, § 2, 6°, vise la localisation du point de terminaison du réseau au début et à la fin de chaque connexion. On rappelera que la téléphonie mobile diffère de la téléphonie fixe principalement au niveau de la localisation du point de terminaison de réseau qui sera différente pour chaque communication. La directive vise bien « l'identité de localisation (identifiant cellulaire) au début de la communication » (article 5, 1, *f)*, 1)) et prévoit donc la conservation du point de terminaison au début de la communication. Il est souhaitable de 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.

Il est exigé d'enregistrer la localisation du point de terminaison du réseau au début et à la fin de chaque connexion, mais non pas au cours de cette connexion. En d'autres termes, lorsque l'utilisateur final se déplace en téléphonant, la localisation des mâts intermédiaires utilisés au cours de la connexion ne doit pas être enregistrée.

Wat betreft de datum en de plaats van inschrijving op het abonnement of de registratie van de eindgebruiker (artikel 4, § 1, 3°) en de nummeroverdracht (artikel 4, § 1, 6°), gelden de opmerkingen van artikel 3 *mutatis mutandis* ook voor artikel 4. Hieraan wordt toegevoegd dat de plaats van inschrijving op het abonnement of de registratie van de eindgebruiker een nuttig gegeven is voor de autoriteiten.

Gelet op de commerciële kanalen, kan het abonnement of de registratie worden aangegaan in een winkel, phoneshop of lokaal kantoor, waar gewoonlijk ook het originele getekende contract wordt bewaard. Alle persoonlijke gegevens die erin zijn vermeld worden niet noodzakelijk aan de operator bezorgd. Daarom is het interessant om te weten waar het abonnement of de registratie werd aangegaan. Er kan aan de hand van handschrift en handtekening nagegaan worden of het contract werkelijk werd aangegaan door de persoon met de persoonsgegevens opgegeven in het document of dat deze persoon het slachtoffer werd van identiteitsdiefstal.

Die plaats is momenteel beschikbaar bij de operatoren en wordt geregeld gevraagd door de gerechtelijke autoriteiten. Zo stelt men op basis van de facturen 2006 tot 2011 die door NTSU-CTIF gecontroleerd zijn en betaald door Justitie aan de operatoren, vast dat aan de operatoren op grond van de artikelen 46*bis* en 88*bis* van het Wetboek van strafvorderingen gemiddeld 60 keer per jaar "het verkooppunt" is gevraagd.

De gegevens bedoeld in artikel 4, § 1, 4° (de datum en het tijdstip van de eerste activering van de dienst, alsook de celidentiteit van waaruit de dienst is geactiveerd) stemmen overeen met wat de richtlijn voorschrijft (zie artikel 5.1., *e)*, 2), vi), die dat gegeven echter beperkt tot de anonieme diensten met voorafbetaling.

Het is belangrijk exact het ogenblik en ook de plaats van activering van de dienst te kennen. Weten wanneer de simkaart is gekocht en wanneer deze voor de eerste keer is gebruikt (3° en 4°) kan kostbare aanwijzingen opleveren voor de rechercheurs. Dat geldt zowel voor een gewoon abonnement als voor een voorafbetaald abonnement of een voorafbetaalde kaart. Het gebruik van de dienst kan bijvoorbeeld erop wijzen dat een daad is gepleegd met voorbedachten rade. Het niet gebruiken van de dienst kan wijzen op een geval van fraude en een poging om een valse identiteit te creëren.

Wat betreft de aanvullende diensten (artikel 4, § 1, 5°), en de gegevens met betrekking tot de soort van betaling (artikel 4, § 1, 7°), gegevens waarin de richtlijn niet voorziet, geldt de commentaar bij artikel 3 *mutatis mutandis* ook voor artikel 4.

Onder aanvullende diensten voor mobiele telefonie wordt verstaan de aanvullende diensten waarop een klant gratis of tegen betaling kan intekenen. Bijvoorbeeld : antwoorddienst, doorschakeling van oproepen, bijzondere formule om bepaalde nummers of bestemmingen tegen voordeeltarief te bellen, groepsgesprek, enz. Wat het nut betreft om dergelijke gegevens te bewaren, wordt verwezen naar de uitleg die wordt gegeven bij artikel 3, § 1, 4°.

De gegevens bedoeld in paragraaf 2 van artikel 4 zijn allemaal opgenomen in de richtlijn, met uitzondering van artikel 4, § 2, 6° en 7° van het koninklijk besluit.

Artikel 4, § 2, 6°, doelt op de lokalisatie van het netwerkaansluitpunt aan het begin en op het einde van elke verbinding. Zoals bekend, verschilt mobiele telefonie van vaste telefonie, voornamelijk op het vlak van de locatie van het netwerkaansluitpunt, dat voor elke communicatie verschillend zal zijn. De richtlijn doelt wel degelijk op "de locatieaanduiding (Cell ID) bij het begin van de verbinding" (artikel 5, 1, *f)*, 1)) en schrijft dus voor dat het netwerkaansluitpunt bij het begin van de verbinding wordt bijgehouden. Het is wenselijk om 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 weten waar dit is gelegen.

Sommige Belgische operatoren hebben in het verleden hun systemen aangepast om dit gegeven te kunnen aanleveren en verstrekken deze gegevens nu op verzoek van de gerechtelijke overheden.

Er wordt geëist dat de plaats van het netwerkaansluitpunt wordt geregistreerd aan het begin en op het einde van elke verbinding, maar niet tijdens deze verbinding. Wanneer de eindgebruiker zich dus al telefonerend verplaatst, hoeft de plaats van de tussenliggende masten die tijdens de verbinding zijn gebruikt, niet te worden geregistreerd.

L'article 4, § 2, 7°, vise « les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée », alors que l'article 5.1, *f)*, 2) de la directive vise « les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées. » (c'est nous qui soulignons).

Il vaut mieux dire que les données de localisation des cellules doivent être conservées en prenant en compte cette localisation au moment où la communication a eu lieu. Cela permettra aux autorités de recevoir ces données de localisation telles qu'elles existaient au moment de la communication, mêmes si des modifications ont été faites dans l'architecture du réseau après la fin de la communication et ont modifié la localisation de ces cellules.

On rappelera à cet égard que la configuration d'un réseau mobile est assez dynamique. Fréquemment des antennes et des cellules sont reconfigurées ou déplacées. Un identifiant d'une cellule qui désigne une localisation à un moment donné peut être tout à fait différent 6 mois plus tard. D'où l'importance de connaître la configuration du réseau au moment de la communication.

Par exemple si, au jour J, la cellule X du fournisseur concerné couvrait un périmètre déterminé, il se peut qu'au moment où les autorités compétentes demanderont l'accès aux données de localisation, la configuration du réseau ait été profondément modifiée. Il est donc nécessaire de pouvoir dire, à la date de la demande d'accès aux données, quel était le périmètre couvert au jour J, ce dernier ayant pu changer depuis.

Les données visées à l'article 4, § 1er, 8° (le numéro IMEI) sont reprises dans la directive (voir tableau de transposition).

Article 5

L'article 5 vise les fournisseurs de réseaux ou services offrant un accès à l'internet accessible au public, à l'exception du courrier électronique par l'internet accessible au public et de la téléphonie par l'internet accessible au public.

Les données visées à l'article 5, § 1er, 1° (l'identifiant de l'utilisateur final) et 2° (les données personnelles de l'utilisateur final) sont également reprises dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Les données visées à l'article 5, § 1er, 3° (la date et l'heure de la souscription à l'abonnement ou l'enregistrement de l'utilisateur final) et 4° (l'adresse IP et le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final) ne sont pas reprises dans la directive mais doivent être conservées pour les raisons suivantes.

Différents services d'accès à Internet permettent de s'enregistrer en ligne en tant que nouvel utilisateur final.

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 final encoder de fausses données d'identité. Pour permettre l'identification réelle de l'utilisateur final, il faut en pareils cas conserver les traces laissées sur Internet (adresse IP, port source et point de terminaison du réseau lors de la création du compte).

En plus de l'adresse IP, il est nécessaire de conserver le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final pour les raisons suivantes.

Jusqu'en 2011, une adresse IP utilisée à un certain moment permettait l'identification d'une seule personne.

Pour des raisons techniques et commerciales, un grand nombre de fournisseurs d'accès à internet ont récemment migré vers le partage d'une adresse IP entre plusieurs utilisateurs finals.

Afin de rendre cela possible, les 65 536 ports (TCP / UDP) disponibles pour une adresse IP sont divisés entre les différents utilisateurs finals de cette adresse IP.

La conservation des données a pour but d'identifier de manière précise et univoque l'utilisateur final internet impliqué dans un dossier judiciaire, et d'exclure les autres.

Pour différencier les différents utilisateurs finals d'Internet partageant une même adresse IP, et identifier de manière non ambigüe un certain utilisateur final (le suspect), il est nécessaire que le fournisseur

Artikel 4, § 2, 7°, doelt op "de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt", terwijl er in artikel 5.1, *f)*, 2) van de richtlijn sprake is van "gegevens voor het identificeren van de geografische locatie van cells middels referentie aan hun locatieaanduidingen (Cell ID's) gedurende de periode dat communicatiegegevens worden bewaard." (door ons onderstreept).

Voor een beter begrip komt het erop neer de locatiegegevens van de cellen te bewaren op het ogenblik dat de communicatie plaatsvond. Dit maakt het mogelijk voor de autoriteiten om deze locatiegegevens te ontvangen zoals ze bestonden op het ogenblik van de communicatie, zelfs wanneer in de netwerkarchitectuur wijzigingen zijn aangebracht na het einde van de communicatie die de locatie van deze cellen veranderd hebben.

Daarbij wordt opgemerkt dat de configuratie van een mobiel netwerk nogal dynamisch is. Vaak worden antennes en cellen geherconfigureerd of verplaatst. Een celidentiteit die op een gegeven moment een plaats aanduidt, kan 6 maanden later helemaal anders zijn. Vandaar het belang om de netwerkconfiguratie te kennen op het ogenblik van de communicatie.

Indien bijvoorbeeld, op dag D, cel X van de betrokken aanbieder een bepaald gebied zou bestrijken, is het mogelijk dat op het ogenblik dat de bevoegde autoriteiten de toegang tot de locatiegegevens zullen vragen, de configuratie van het netwerk grondig is gewijzigd. Het is dus noodzakelijk om op de datum van het verzoek om inzage in de gegevens te kunnen zeggen welk gebied op dag D werd bestreken, omdat dat dekkingsgebied sindsdien veranderd kan zijn.

De gegevens bedoeld in artikel 4, § 1, 8° (het IMEI-nummer) zijn opgenomen in de richtlijn (zie omzettingstabel).

Artikel 5

Artikel 5 heeft betrekking op de aanbieders van netwerken of diensten die een openbare internettoegangsdienst aanbieden, met uitzondering van openbare e-mail via internet en openbare internettelefonie.

De gegevens bedoeld in artikel 5, § 1, 1° (de toegewezen eindgebruikersidentificatie) en 2° (de persoonsgegevens van de eindgebruiker) stemmen eveneens overeen met de richtlijn (zie omzettingstabel). Bovendien wordt verwezen naar de opmerkingen in verband met artikel 1, 7° (definitie van "persoonsgegevens").

De gegevens bedoeld in artikel 5, § 1, 3° (de datum en het tijdstip van het nemen van het abonnement of de registratie van de eindgebruiker) en 4° (het IP-adres en de bronpoort van de verbinding die gediend hebben voor het nemen van het abonnement of voor de registratie van de eindgebruiker) worden niet vermeld in de richtlijn maar moeten worden bewaard om de volgende redenen.

Verschillende diensten voor internettoegang maken het mogelijk om zich online te registreren als nieuwe eindgebruiker.

Bij gebrek aan reëel contact tussen de operator of dienstenverstrekker en de klant, is het steeds vaker zo dat de eindgebruiker valse identiteitsgegevens invoert. Om tot een reële identificatie van de eindgebruiker te kunnen komen, is het in deze gevallen dan noodzakelijk om de internetsporen (IP-adres, bronpoort en netwerkaansluitingspunt bij creatie van het account) te bewaren.

Behalve het IP-adres moet de bronpoort van de verbinding die gediend heeft voor het nemen van het abonnement of voor de registratie van de eindgebruiker worden bewaard om de volgende redenen.

Tot omstreeks 2011 was het zo dat een IP-adres dat op een bepaald ogenblik werd gebruikt, juist één internetgebruiker (abonnee) identificeerde.

Om technische en commerciële redenen zijn een groot aantal internetproviders recent overgestapt naar het delen van een IP-adres onder verschillende eindgebruikers.

Om dit mogelijk te maken, worden de 65 536 poorten (TCP / UDP) die per IP-adres beschikbaar zijn, verdeeld over de verschillende eindgebruikers van dat IP-adres.

De gegevensbewaring is erop gericht om interneteindgebruikers die betrokken zijn in een gerechtelijk dossier op een éénduidige manier te identificeren en anderen dus uit te sluiten.

Om de verschillende interneteindgebruikers van eenzelfde IP-adres van elkaar te onderscheiden en één bepaalde eindgebruiker (een verdachte) op éénduidige manier te kunnen identificeren, is het

d'accès à internet qui partage les adresses IP entre plusieurs utilisateurs finals conserve également pour chaque utilisateur final, à côté de l'adresse IP, les ports qui lui ont été attribués et la période de cette attribution.

Il faut rappeler à cet égard que la directive a été adopté le 15 mars 2006 et qu'à cette époque, les fournisseurs d'accès à Internet ne partageaient pas une adresse IP entre plusieurs utilisateurs finals. Il est donc logique que la directive n'ait pas pu prévoir la conservation des ports. Le présent arrêté prend en compte cette évolution technologique et économique en visant également les ports.

Les données visées à l'article 5, § 1er, 5° (l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu'utilisateur final) ne sont pas reprises telles quelles dans la directive. On notera cependant que la directive vise « la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication » (article 5.1, *e)*, 3), ii), de la directive), ce qui revient à demander l'identification du point de terminaison du réseau pour chaque communication. Les données à conserver en vertu de l'article 5, § 1er, 5°, ne constituent donc pas une charge supplémentaire importante pour les opérateurs.

Le point de terminaison du réseau correspond à l'identification de l'appareil utilisé pour la connexion. Il s'agit, entre autres, de l'adresse MAC du modem ou du routeur connecté au point de terminaison chez l'utilisateur final (numéro d'identification qui se compose d'une série de 12 chiffres et / ou lettres). Par contre, le présent arrêté royal n'oblige pas les opérateurs à identifier l'adresse MAC des équipements qui sont connectés chez l'utilisateur final à ce modem ou routeur, ce qui ne serait d'ailleurs pas possible dans bien des cas. L'identification du point de terminaison du réseau permet au fournisseur d'accès d'identifier son client et donc de lui attribuer une adresse IP grâce à laquelle il pourra établir sa connexion. En conservant uniquement l'adresse IP et les ports source sans conserver le point de terminaison du réseau, il ne serait pas possible de localiser l'utilisateur final.

Les données visées à l'article 5, 6° (les services annexes auxquels l'utilisateur final a souscrit auprès du fournisseur d'accès public à l'internet) ne sont pas reprises telles quelles dans la directive. Néanmoins, l'article 5.1, *e)*, 3, ii) de la directive prévoit la conservation de « la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication ». Dans sa communication au fournisseur, l'utilisateur final est donc amené à lui demander à s'abonner aux services annexes.

Il faut entendre par « services annexes auxquels l'utilisateur final a souscrit » les différentes possibilités ou formules offertes par l'opérateur à son client : telles qu'une bande passante plus importante, par exemple. Il est ainsi par exemple intéressant pour les autorités de savoir que l'utilisateur final a souscrit à un service similaire à Skype, mais offert par le fournisseur de l'accès à Internet, ce qui pourrait indiquer que les recherches doivent s'orienter vers les communications sur ce type de service.

Les données visées à l'article 5, § 1er, 7° (les données relatives au type de paiement ainsi qu'à l'identification et à la date du paiement de l'abonnement ou de l'utilisation du service) ne sont pas prévues par la directive. Il est renvoyé aux explications données à l'article 3 à ce égard.

Les données visées à l'article 5, § 2, 1° (l'identifiant de l'utilisateur final) sont prévues par la directive (voir tableau de transposition).

Les données visées à l'article 5, § 2, 2°, (a) l'adresse IP et *b)* en cas d'utilisation partagée d'une adresse IP, les ports attribués de l'adresse IP ainsi que la date et l'heure de l'attribution) vont un peu plus loin que ce que prévoit la directive qui vise notamment « l'adresse IP (protocole internet), qu'elle soit dyamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet » (article 5, 1, *c)*, 2, *i)*).

Comme il a été ci-dessus (voir commentaires relatifs à l'article 5, § 1er, 4°), vu que plusieurs fournisseurs partagent une adresse IP entre plusieurs utilisateurs finals, il n'est plus suffisant de conserver cette adresse IP mais également les ports sources.

Les données visées à l'article 5, § 2, 3° (l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion) vont un peu plus loin que la directive qui ne prévoit la conservation de ces données que pour le début d'une connexion (voir l'article 5, 1, *f)*, 1) de la directive).

noodzakelijk dat de aanbieder van internettoegang die IP-adressen deelt over verschillende eindgebruikers, dus ook voor elke eindgebruiker naast het IP-adres de toegekende poorten en de periode van deze toekenning bewaart.

Daarbij moet worden opgemerkt dat de richtlijn aangenomen is op 15 maart 2006 en dat de internetproviders destijds geen IP-adres verdeelden over verschillende eindgebruikers. Het is dus logisch dat de richtlijn het bewaren van de poorten niet kon voorzien. Het onderhavige besluit houdt rekening met deze technologische en economische ontwikkeling, door ook de poorten mee te rekenen.

De gegevens bedoeld in artikel 5, § 1, 5° (de identificatie van het netwerkaansluitpunt dat gediend heeft voor het nemen van het abonnement of voor de inschrijving als eindgebruiker) zijn niet als zodanig vermeld in de richtlijn. Er moet echter worden opgemerkt dat de richtlijn het heeft over "de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie" (artikel 5.1, *e)*, 3), ii), van de richtlijn), wat erop neerkomt dat de identificatie van het netwerkaansluitpunt voor elke communicatie wordt gevraagd. De gegevens die krachtens artikel 5, § 1, 5°, moeten worden bewaard, vormen dus geen grote extra last voor de operatoren.

Het netwerkaansluitpunt stemt overeen met de identificatie van het toestel dat voor de verbinding wordt gebruikt. Het gaat onder andere om het MAC-adres van de modem of van de router die aangesloten is op het aansluitpunt bij de eindgebruiker (identificatienummer dat uit een reeks van 12 cijfers en / of letters bestaat). Het onderhavige besluit verplicht de operatoren echter niet om het MAC-adres te identificeren van de apparatuur die bij de eindgebruiker op deze modem of router aangesloten is, hetgeen trouwens in heel wat gevallen onmogelijk zou zijn. Dankzij de identificatie van het netwerkaansluitpunt kan de aanbieder van toegang zijn klant identificeren en hem dus een IP-adres toewijzen waarmee hij zijn verbinding tot stand kan brengen. Door enkel het IP-adres en de bronpoorten te bewaren zonder het netwerkaansluitpunt te bewaren, zou het niet mogelijk zijn om de plaats van de eindgebruiker te bepalen.

De gegevens bedoeld in artikel 5, 6° (de aanvullende diensten waarop de eindgebruiker ingeschreven heeft bij de betrokken aanbieder van openbare internettoegang) zijn niet als zodanig opgenomen in de richtlijn. Artikel 5.1, *e)*, 3, ii) van de richtlijn voorziet echter in de bewaring van "de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie". In zijn mededeling aan de aanbieder moet de eindgebruiker dus hem vragen om zich te abonneren op de aanvullende diensten.

Onder "de aanvullende diensten waarop de eindgebruiker ingeschreven heeft" moeten de verschillende mogelijkheden of formules worden verstaan die de operator aan zijn klant verstrekt, zoals een grotere bandbreedte. Zo is het bijvoorbeeld voor de autoriteiten interessant te weten of de eindgebruiker zich heeft ingeschreven voor een dienst zoals Skype, maar die wordt aangeboden door de internetprovider, wat erop zou kunnen wijzen dat het onderzoek zich moet toespitsen op de communicatie via dit soort van dienst.

De gegevens bedoeld in artikel 5, § 1, 7° (de gegevens betreffende type, identificatie en tijdstip van de betaling voor het abonnement of voor het gebruik van de dienst) staan niet in de richtlijn. Er wordt verwezen naar de desbetreffende uitleg die wordt gegeven bij artikel 3.

De gegevens bedoeld in artikel 5, § 2, 1° (de eindgebruikersidentificatie) worden voorgeschreven door de richtlijn (zie omzettingstabel).

De gegevens bedoeld in artikel 5, § 2, 2°, (a) het IP-adres en *b)* in geval van het gedeelde gebruik van een IP-adres de toegewezen poorten van het IP-adres evenals de datum en uur van de toewijzing) gaan iets verder dan wat de richtlijn voorschrijft; daar is met name sprake van "het IP-adres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen" (artikel 5, 1, *c)*, 2, *i)*).

Zoals hierboven is uitgelegd (zie commentaar bij artikel 5, § 1, 4°), is het niet langer voldoende om dit IP-adres te bewaren, maar zijn ook de bronpoorten nodig, aangezien verschillende aanbieders een IP-adres delen over verscheidene eindgebruikers.

De gegevens bedoeld in artikel 5, § 2, 3° (de identificatie en de locatie van het netwerkaansluitpunt dat door de eindgebruiker wordt gebruikt bij aanvang en bij het einde van een sessie) gaan wat verder dan de richtlijn, die enkel de bewaring van die gegevens aan het begin van een communicatie voorschrijft (zie artikel 5, 1, *f)*, 1) van de richtlijn).

Grâce aux nouvelles technologies il est possible de se connecter sans fil à l'internet (p.ex en « Wifi » ou Internet mobile) depuis n'importe quelle localisation couverte par un réseau sans fil. Il existe également des standards wi-fi qui permettent à l'utilisateur final de se déplacer lors de sa connexion au réseau et qui permettent à cette connexion d'être continue car passant d'une antenne à une autre. Il est donc utile de préciser ici que si l'utilisateur final se déplace durant la connexion et que celle-ci passe d'une station de base ou d'une antenne à une autre, le fournisseur de réseau ou service de communications électroniques offrant un accès à l'internet accessible au public devra être capable de communiquer la localisation de l'utilisateur final au début et à la fin de la connexion, comme c'est le cas dans le cadre de la téléphonie mobile. La localisation de l'utilisateur final pendant la connexion ne doit par contre pas être conservée, ce qui signifie que lorsque l'utilisateur final se déplace pendant la communication, la localisation des mats ou stations de base intermédiaires ayant servi à la connexion ne doit pas être conservée.

L'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion permettra de déterminer d'où à où cet utilisateur final s'est déplacé, ce qui peut constituer des informations utiles pour les autorités.

Les données visées à l'article 5, § 2, 4° (la date et l'heure d'ouverture et de la fermeture d'une session du service d'accès à l'internet) sont prévues par la directive (voir tableau de transposition).

A l'article 5, § 2, 5°, il est demandé aux fournisseurs de conserver le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée.

En d'autres termes, il est demandé aux fournisseurs de conserver, par durée de connexion (ou autre unité de temps, qui pourrait être la durée pendant laquelle une adresse IP précise a été attribuée), le volume de données téléchargées ou uploadées.

Ces données ne sont pas reprises dans la directive mais la conservation de ces dernières est justifiée comme suit.

Tout d'abord, depuis l'apparition des connexions à large bande avec tarif mensuel fixe et des réseaux wifi pour utilisateurs finals à domicile, les utilisateurs finals restent de plus en plus souvent connectés à Internet 24 heures sur 24. Pour pouvoir fournir les données de connexion et procéder à une évaluation de la faisabilité technique d'une interception internet, il est important pour les enquêteurs de pouvoir se faire une idée de l'activité effective de la connexion internet concernée.

Ensuite, connaître l'activité d'une personne peut également permettre aux enquêteurs et au juge de décider s'il est opportun de faire une interception de la ligne utilisée. En effet, s'il n'y a aucune activité, il ne sera pas productif d'effectuer une interception et dès lors, des frais de justice inutiles seront évités.

Par ailleurs, ces données sont actuellement conservées systématiquement par les fournisseurs dans leurs données clients.

Finalement, l'activité d'une personne peut, en partie, être déduite des volumes de données uploadés et downloadés.

Si, par exemple, une adresse IP apparaît lors de l'identification des connexions sur un site pédopornographique, il sera utile de savoir si cette personne est plutôt active (upload de fichiers – quelle taille), ou si elle télécharge de gros volume de fichiers mis à disposition (plutôt consommatrice).

Connaître son activité up / download au moment où son adresse IP a été utilisée pourra être utile.

En d'autres termes, un des buts de la conservation des données relatives au volume de données téléchargées ou uploadées est de pouvoir analyser le comportement de la personne si celle-ci est soupçonnée de comportement illicite.

A contrario, voir que cette personne n'a pas utilisé sa capacité de téléchargement ou d'upload pourrait également la disculper.

Les données visées à l'article 5, § 2, 6° (les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée) correspondent à l'article 5.1, *f)*, 2), de la directive. Cette dernière se réfère cependant à l'identifiant cellulaire des cellules *« pendant la période au cours de laquelle les données de communications sont conservées »* alors que le présent arrêté se réfère à l'identifiant cellulaire des cellules au moment où la communication a été effectuée. Il est renvoyé à cet égard à l'explication donnée ci-dessus par rapport à l'article 4, § 2, 7°.

Le paragraphe 3 de l'article 5 fixe le point de départ du délai de conservation conformément à l'article 126, § 3, de la LCE. Ce dernier article stipule en son alinéa 1er que « Les données visant à identifier les

Dankzij de nieuwe technologieën is het mogelijk zich draadloos op het internet aan te sluiten (zoals via "wifi" of mobiel internet) van op bijna elke plek die gedekt wordt door een draadloos netwerk. Er zijn ook wifi-normen die de eindgebruiker in staat stellen om zich tijdens zijn verbinding te verplaatsen en die het mogelijk maken dat deze verbinding continu is, omdat er van de ene naar de andere antenne wordt overgegaan. Het is dus nuttig om hier te verduidelijken dat wanneer de eindgebruiker zich verplaatst tijdens de verbinding en deze van het ene basisstation of de ene antenne naar een ander basisstation of andere antenne overgaat, de aanbieder van een netwerk of dienst voor elektronische communicatie die een openbare internettoegang aanbiedt, in staat zal moeten zijn om de locatie van de eindgebruiker mee te delen aan het begin of op het einde van de verbinding, zoals dat het geval is bij mobiele telefonie. De plaats van de eindgebruiker tijdens de aansluiting moet echter niet worden bewaard, wat inhoudt dat wanneer de eindgebruiker zich tijdens de communicatie verplaatst, de locatie van de tussenliggende masten of basisstations die voor de aansluiting hebben gediend, niet moet worden bewaard.

De identificatie en lokalisatie van het netwerkaansluitpunt dat gebruikt wordt door de eindgebruiker aan het begin of op het einde van een verbinding zal het mogelijk maken te bepalen van waar tot waar deze eindgebruiker zich verplaatst heeft, hetgeen nuttige informatie kan opleveren voor de autoriteiten.

De gegevens bedoeld in artikel 5, § 2, 4° (de datum en het tijdstip van de log-in en log-off van een sessie van de internettoegangsdienst) zijn vermeld in de richtlijn (zie omzettingstabel).

In artikel 5, § 2, 5°, worden de aanbieders gevraagd om het tijdens de sessie of een ander gevraagde tijdseenheid geüploade en gedownloade volume van gegevens te bewaren.

De aanbieders worden met andere woorden gevraagd om, per verbindingssessie (of andere tijdseenheid, bijvoorbeeld de periode waarin een bepaald IP-adres werd toegewezen), het volume van geüploade of gedownloade gegevens te bewaren.

Deze gegevens worden niet vermeld in de richtlijn maar de bewaring ervan wordt gerechtvaardigd door wat volgt.

In de eerste plaats gebeurt het, sinds de komst van breedbandverbindingen met een vast maandelijks tarief en van wifinetwerken voor thuis-eindgebruikers, steeds vaker dat de eindgebruikers hun internetverbinding 24 u. per dag laten opstaan. Om de verbindingsgegevens te kunnen verstrekken en om een inschatting te kunnen maken van de technische haalbaarheid van een internetinterceptie, is het van belang dat de onderzoekers zich een beeld kunnen vormen van de werkelijke activiteit van de betreffende internetverbinding.

Vervolgens kan het de onderzoekers en de rechter ook in staat stellen om te beslissen of een interceptie van de gebruikte lijn gepast is indien zij de activiteit van een persoon kennen. Indien er immers geen activiteit is, zal het niet productief zijn om een interceptie uit te voeren en worden dus zinloze gerechtskosten vermeden.

Deze gegevens worden overigens door de operatoren thans ook steeds bijgehouden in hun klantengegevens.

Ten slotte kan de activiteit van een persoon voor een deel worden afgeleid uit de volumes van geüploade en gedownloade gegevens.

Indien een IP-adres bijvoorbeeld verschijnt bij de identificatie van de verbindingen op een site met kinderporno, zal het nuttig zijn om te weten of deze persoon eerder actief is (upload van bestanden – welke grootte), of indien hij grote volumes bestanden downloadt die ter beschikking worden gesteld (en dus eerder consument is).

Zijn up- / downloadactiviteit kennen op het ogenblik waarop zijn IP-adres werd gebruikt kan nuttig blijken.

Met andere woorden : de bewaring van gegevens betreffende het volume van gedownloade en geüploade gegevens beoogt onder meer het gedrag van een persoon te analyseren wanneer deze wordt verdacht van onwettige handelingen.

Zien dat deze persoon zijn download- of uploadcapaciteit niet heeft gebruikt, kan deze persoon daarentegen ook vrijpleiten.

De gegevens bedoeld in artikel 5, § 2, 6° (de gegevens die het mogelijk maken de geografische locatie van de cellen vast te stellen door zich te baseren op hun celidentiteit op het ogenblik waarop de verbinding is gelegd) stemmen overeen met artikel 5.1, *f)*, 2), van de richtlijn. Daar wordt echter gesproken van de celidentiteit "*gedurende de periode dat communicatiegegevens worden bewaard*" terwijl het onderhavige besluit verwijst naar de celidentiteit op het moment dat de communicatie wordt verricht. Er wordt hierbij verwezen naar de desbetreffende uitleg die wordt gegeven bij artikel 4, § 2, 7°.

Paragraaf 3, van artikel 5, bepaalt het startpunt voor de bewaartermijn conform artikel 126, § 3, van de WEC. Dat laatste artikel bepaalt in zijn eerste lid dat "De gegevens ter identificatie van de eindgebruikers,

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

Lorsqu'un service d'accès à l'internet est utilisé, une communication se crée toujours entre l'utilisateur final et le serveur du fournisseur de service d'accès à internet. Dans le contexte du service d'accès à l'internet, la communication entrante ou sortante mentionnée dans l'article 126, § 3, de la LCE, est donc la communication avec le serveur et donc en pratique l'utilisation du service d'accès à l'internet.

Article 6

L'article 6 vise les données à conserver par les fournisseurs de services de courrier électronique par internet accessibles au public et par les fournisseurs de services de téléphonie par internet accessibles au public, à l'exception de l'accès à l'internet accessible au public.

En ce qui concerne les services de courriers électroniques, on vise tant les courriers SMTP que les webmails, pour autant qu'ils soient offerts en Belgique.

Il existe différentes formes de téléphonie qui utilisent le protocole Internet; on parle souvent de « Voice over IP » (« VoIP »). La téléphonie par internet suppose qu'un ou les deux participants à la communication utilisent un logiciel spécial afin qu'un ordinateur puisse entrer en contact avec un autre. Lorsque seul l'appelant utilise un logiciel spécifique permettant à un ordinateur d'entrer en contact avec un correspondant en utilisant un numéro de téléphone, l'appelant doit établir une connexion via son fournisseur de service avec le réseau téléphonique classique. Dans ce même exemple, l'article 6 s'applique pour ce qui concerne la partie téléphonie par internet.

Les données visées à l'article 6, § 1er, 1° (l'identifiant de l'utilisateur final) et 2° (les données personnelles de l'utilisateur final) sont également prévues dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Les données visées à l'article 6, § 1er, 3° (la date et l'heure de la création du compte de courrier électronique ou de téléphonie par Internet) ne sont pas reprises dans la directive.

En ce qui concerne les comptes mails activés par défaut lors de la souscription d'un abonnement chez un fournisseur d'accès, certaines des données mentionnées au paragraphe 1er (telles que les date et heure de création du compte) sont déjà conservées par les opérateurs en pratique dans le cadre de la souscription à un abonnement ou à un enregistrement à un service et ne doivent pas être conservées séparément. Ainsi, par exemple, les date et heure de création du compte coïncideront avec les date et heure de souscription de l'abonnement. Il ne s'agit donc pas d'une charge lourde supplémentaire pour les opérateurs.

En revanche, si l'utilisateur final demande l'ouverture d'une seconde adresse e-mail, ou crée un second alias, ces données devront être conservées au même titre que la création d'un nouveau compte.

La conservation de la date et de l'heure de la création du compte de courrier électronique ou de téléphonie par internet est utile pour les raisons suivantes. La durée qui s'écoule entre la souscription au compte et son utilisation active peut donner une indication sur le profil de l'utilisateur final, qui peut constituer un indice utile pour les autorités. Un compte qui n'est pas utilisé ou de manière très sporadique peut être un indice de fraude ou de création d'une fausse identité électronique.

Les données visées à l'article 6, § 1er, 4° (l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet) ne sont pas reprises dans la directive.

Comme expliqué ci-dessus pour ce qui concerne l'article 5, § 1er, 4°, 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 final encoder de fausses données d'identité. Pour permettre l'identification réelle de l'utilisateur final, il faut en pareils cas conserver les traces laissées sur Internet (adresse IP, port source et point de terminaison du réseau lors de la création du compte).

Par exemple, si un utilisateur final d'Internet crée une boîte à messages internet sur mail.be au nom d'une personnage de fiction habitant dans un lieu imaginaire, les « données personnelles » enregistrées ne sont d'aucune utilité. L'adresse IP de cet utilisateur

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

Wanneer een internettoegangsdienst wordt gebruikt, komt er steeds een communicatie tot stand tussen de eindgebruiker en de server van de aanbieder van de internettoegangsdienst. In het kader van de internettoegangsdienst is de binnenkomende of uitgaande communicatie vermeld in artikel 126, § 3, van de WEC, dus de communicatie met de server en in de praktijk dus het gebruik van de internettoegangsdienst.

Artikel 6

Artikel 6 heeft betrekking op de gegevens die moeten worden bewaard door de aanbieders van openbare e-maildiensten via internet en door de aanbieders van openbare internettelefoniediensten, met uitzondering van openbare internettoegang.

Wat de e-maildiensten betreft, worden zowel SMTP-mail bedoeld als webmail voor zover zij worden aangeboden in België.

Er bestaan verschillende vormen van telefonie die gebruik maken van het internetprotocol; vaak wordt gesproken over "Voice over IP" ("VoIP"). Bij internettelefonie maken één of beide deelnemers aan de spraakcommunicatie gebruik van specifieke programmatuur om vanop een computer met elkaar in contact te komen. Wanneer alleen de oproeper gebruik maakt van specifieke programmatuur om van op een computer in contact te komen met zijn gesprekspartner via diens telefoonnummer, dan zal de oproeper via zijn dienstenverlener een verbinding maken met het klassieke telefoonnet. In hetzelfde voorbeeld is artikel 6 van toepassing wat het deel internettelefonie betreft.

De gegevens bedoeld in artikel 6, § 1, 1° (de eindgebruikersidentificatie) en 2° (de persoonsgegevens van de eindgebruiker) zijn eveneens vastgelegd in de richtlijn (zie omzettingstabel). Bovendien wordt verwezen naar de opmerkingen in verband met artikel 1, 7° (definitie van "persoonsgegevens").

De gegevens bedoeld in artikel 6, § 1, 3° (de datum en het tijdstip waarop de e-mail- of internettelefonieaccount is gecreëerd) komen niet ter sprake in de richtlijn.

Wat betreft de mailaccounts die automatisch worden geactiveerd bij het nemen van een abonnement bij een toegangsprovider, worden sommige gegevens vermeld in paragraaf 1 (zoals de datum en het tijdstip waarop de account wordt gemaakt) in de praktijk al door de operatoren bewaard in het kader van het nemen van een abonnement of een registratie op een dienst en moeten ze niet apart worden bewaard. Zo zullen bijvoorbeeld de datum en het tijdstip waarop de account wordt gemaakt, samenvallen met de datum en het tijdstip waarop het abonnement wordt genomen. Het gaat dus niet om een zware bijkomende last voor de operatoren.

Indien de eindgebruiker daarentegen vraagt om een tweede mailadres te openen, of een tweede alias creëert, zullen die gegevens op dezelfde manier moeten worden bewaard als bij de creatie van een nieuwe account.

De bewaring van de datum en het tijdstip waarop de e-mail- of internettelefonieaccount is gecreëerd, heeft nut om de volgende redenen. De tijd die verloopt tussen het inschrijven op de account en het actieve gebruik ervan kan een indicatie geven over het profiel van de eindgebruiker, die voor de autoriteiten een nuttige aanwijzing kan vormen. Een account die niet of maar zeer sporadisch wordt gebruikt, kan op fraude wijzen of op de creatie van een valse elektronische identiteit.

De gegevens bedoeld in artikel 6, § 1, 4° (het IP-adres en de bronpoort die gediend hebben voor de creatie van de e-mail- of internettelefonieaccount) worden niet vermeld in de richtlijn.

Zoals hierboven uitgelegd wat betreft artikel 5, § 1er, 4°, bij gebrek aan reëel contact tussen de operator of dienstenverstrekker en de klant, is het steeds vaker zo dat de eindgebruiker valse identiteitsgegevens invoert. Om tot een reële identificatie van de eindgebruiker te kunnen komen, is het in deze gevallen dan noodzakelijk om de internetsporen (IP-adres, bronpoort en netwerkaansluitingspunt bij creatie van het account) te bewaren.

Bijvoorbeeld, indien een interneteindgebruiker een webmailbox aanmaakt bij mail.be onder de naam van een fictieve persoon wonende op een ingebeelde plek, dan zijn de geregistreerde "persoonsgegevens" helemaal van geen nut. Het IP-adres van deze interneteindgebruiker, de

final, le port source, ainsi que la date et l'heure de la création de son « abonnement » sont les seules données fiables pouvant conduire les autorités au véritable utilisateur final.

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 du personnage de fiction 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.

Les données visées à l'article 6, § 1er, 5° (les données relatives au paiement ainsi qu'à l'identification et à la date du paiement de l'abonnement ou de l'utilisation du service) ne sont pas reprises dans la directive. Il est renvoyé aux explications pour l'article 3, § 1er, 6°.

Les données visées à l'article 6, § 2 sont reprises dans la directive. Néanmoins, l'article 6, § 2, 3° de l'arrêté royal ne correspond pas exactement au prescrit de la directive.

En effet, cet article prévoit la conservation de « *a)* l'adresse IP et le port source utilisés par l'utilisateur final et *b)* l'adresse IP et le port source utilisé par le destinaire ».

La directive ne vise quant à elle que la conservation de l'adresse IP (voir article 5, 1, *c)*, 2, *i)*.

Pour ce qui concerne la conservation des ports, il est renvoyé aux explications ci-dessus données par rapport à l'article 5, § 1er, 4° et § 2, 2°.

Le paragraphe 3 de l'article 6 prévoit que les données d'identification doivent être conservées aussi longtemps qu'une communication entrante ou sortante est possible. Une communication sera possible aussi longtemps qu'un compte existe.

Article 7

Le premier alinéa vise les fournisseurs de différents services de communications électroniques de façon combinée, tel que par exemple l'envoi d' e-mails via un téléphone mobile intelligent (« *Smart Phone* ») qui permet également d'offrir des services de téléphonie mobile classique.

Dans ce même exemple le fournisseur devra conserver les données correspondant tant au paragraphe 2 de l'article 4 (téléphonie mobile) qu'à celles du paragraphe 2 de l'article 6 (courrier électronique).

Dans l'exemple visé à l'article 6, il y a clairement l'utilisation d'un service de téléphonie par l'internet qui est combiné avec un service de téléphonie fixe ou mobile. Pour ce qui concerne le service de téléphonie par l'internet, l'article 6 est d'application alors que pour la téléphonie fixe ou mobile, c'est respectivement l'article 3 ou 4 qui s'applique.

En vue de l'administration de la preuve, il est nécessaire que tous les fournisseurs de communications électroniques visés utilisent la même indication de l'heure. Actuellement, de nombreuses horloges des systèmes utilisés par les fournisseurs n'indiquent pas une heure conforme à l'heure officielle. Cela peut entraîner des problèmes pour l'administration de la preuve si les données des différents fournisseurs doivent être comparées entre elles. C'est pourquoi le présent article prévoit que les horloges utilisées dans les systèmes des fournisseurs doivent être synchronisées avec le signal horaire GPS.

Article 8

L'article 8 institue, au sein de chaque Cellule Coordination Justice, un préposé à la protection des données, comme le permet l'article 17*bis*, alinéas 2 et 3, 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. Par ailleurs, cette mesure spécifique vise à protéger et sécuriser les données comme l'exige l'article 7 de la directive.

L'article 8, alinéa 3, vise à garantir l'indépendance du préposé dans ses fonctions.

Dans son premier avis (avis n° 24/2008 du 2 juillet 2008), la commission de la vie privée avait demandé que lui soient communiqués de manière systématique les avis et rapports des préposés à la protection des données, la nature du lien juridique entre ces préposés et le service dans lequel ils exerceront leur fonction de préposé, tous les éléments concernant les qualifications professionnelles relatives à la fonction de préposé et les mesures prises par le responsable du traitement en fonction des missions que doit exercer le préposé à la protection des données.

Ces recommandations de la commission de la vie privée n'ont cependant pas été suivies dans le présent arrêté, dès lors que la communication des données susmentionnées risque de créer une charge administrative conséquente tant pour les fournisseurs que pour la commission de la vie privée.

bronpoort en de datum en het tijdstip van de creatie van zijn "abonnement" zijn de enige betrouwbare gegevens die de autoriteiten kunnen leiden naar de echte eindgebruiker.

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 de fictieve persoon maar op naam van een onwetende, bestaande persoon, is de detectie van het valse karakter van deze persoonsgegevens niet voor de hand liggend.

De gegevens bedoeld in artikel 6, § 1, 5° (de gegevens betreffende type, identificatie en tijdstip van de betaling voor het abonnement of het gebruik van de dienst) staan niet in de richtlijn. Er wordt verwezen naar de uitleg bij artikel 3, § 1, 6°.

De gegevens bedoeld in artikel 6, § 2 staan in de richtlijn. Artikel 6, § 2, 3° van het koninklijk besluit stemt echter niet precies overeen met wat in de richtlijn wordt bepaald.

Dit artikel voorziet immers in de bewaring van "*a)* het IP-adres en de bronpoort die worden gebruikt door de eindgebruiker en *b)* het IP-adres en de bronpoort die worden gebruikt door de bestemmeling".

De richtlijn beoogt echter enkel de bewaring van het IP-adres (zie artikel 5, 1, *c)*, 2, *i)*.

Wat de bewaring van de poorten betreft, wordt verwezen naar de bovenstaande uitleg die wordt gegeven bij artikel 5, § 1, 4° en § 2, 2°.

Paragraaf 3 van artikel 6 bepaalt dat de identificatiegegevens moeten worden bewaard zolang binnenkomende of uitgaande communicatie mogelijk is. Communicatie zal mogelijk zijn zolang een account bestaat.

Artikel 7

Het eerste lid slaat op de aanbieders van een combinatie van verschillende diensten voor elektronische communicatie, zoals het verzenden van e-mails via een intelligente mobiele telefoon ("smartphone") die het ook mogelijk maakt om diensten voor klassieke mobiele telefonie te verstrekken.

In datzelfde voorbeeld zal de aanbieder de gegevens moeten bewaren die overeenstemmen met zowel paragraaf 2 van artikel 4 (mobiele telefonie) als met die van paragraaf 2 van artikel 6 (e-mail).

In het voorbeeld van artikel 6 is er duidelijk sprake van het gebruik van een internettelefoniedienst die wordt gecombineerd met een dienst voor vaste of mobiele telefonie. Wat de internettelefoniedienst betreft, geldt artikel 6 terwijl voor vaste of mobiele telefonie, respectievelijk artikel 3 of 4 geldt.

Met het oog op het leveren van het bewijs is het nodig dat alle beoogde aanbieders van elektronische communicatie dezelfde tijdsaanduiding gebruiken. Momenteel wijzen heel wat klokken van de systemen die door de aanbieders worden gebruikt niet een uur aan dat overeenstemt met het officiële uur. Dit kan tot problemen leiden bij het leveren van het bewijs, als de gegevens van de verschillende aanbieders onderling moeten worden vergeleken. Daarom schrijft dit artikel voor dat de klokken die worden gebruikt in de systemen van de aanbieders, moeten worden gesynchroniseerd met het gps-tijdssignaal.

Artikel 8

Artikel 8 wijst binnen elke Coördinatiecel Justitie een aangestelde voor de gegevensbescherming aan, zoals dat wordt toegestaan door artikel 17*bis*, tweede en derde lid, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Bovendien wil deze specifieke maatregel de gegevens beschermen en beveiligen, zoals geëist wordt door artikel 7 van de richtlijn.

Artikel 8, derde lid, is erop gericht de onafhankelijkheid van de aangestelde in zijn functie te garanderen.

In haar eerste advies (advies nr. 24/2008 van 2 juli 2008) had de Privacycommissie gevraagd om de adviezen en rapporten van de aangestelden voor de gegevensbescherming systematisch aan haar over te zenden, alsook de aard van de juridische band tussen deze aangestelden en de dienst waarin ze hun functie als aangestelde zullen uitvoeren, alle elementen in verband met de beroepsbekwaamheid voor de functie van aangestelde en de maatregelen genomen door de verantwoordelijke voor de verwerking volgens de opdrachten, die de aangestelde voor de gegevensbescherming moet uitvoeren.

Deze aanbevelingen van de Privacycommissie zijn echter niet gevolgd in het onderhavige besluit, omdat de mededeling van de bovenstaande gegevens nu éénmaal een aanzienlijke administratieve last dreigt te scheppen, niet alleen voor de aanbieders maar ook voor de Privacycommissie.

La commission disposera de la possibilité de prendre contact avec les préposés pour leur demander les informations qu'elle souhaite lorsque cela est nécessaire.

Article 9

L'article 9 donne obligation aux fournisseurs concernés de communiquer annuellement à l'Institut un certain nombre d'informations statistiques qui seront destinées au ministre qui a les communications électroniques dans ses attributions et au ministre de la Justice. Les ministres compétents font en sorte que ces données, conformément à l'article 10 de la directive, soient transmises à la Commission européenne.

Articles 10 et 11

Aucune règle particulière n'est prévue pour l'entrée en vigueur du présent arrêté. Cependant, une disposition transitoire donne un délai de douze mois aux fournisseurs pour mettre en place les systèmes nécessaires pour conserver les données. De la sorte, les fournisseurs qui parviennent à mettre en place l'infrastructure nécessaire pour conserver les données visées aux articles 3 à 6 du présent arrêté avant le délai de douze mois peuvent conserver légalement ces données.

Nous avons l'honneur d'être,

Sire,
de Votre Majesté,
les très respectueux
et très fidèles serviteurs,

Le Ministre de l'Economie,
J. VANDE LANOTTE

La Ministre de la Justice,
Mme A. TURTELBOOM

Conseil d'Etat
section de législation
avis 53.841/2/V du 26 août 2013
sur

un projet d'arrêté royal 'portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques'

Le 23 juillet 2013 , le Conseil d'Etat, section de législation, a été invité par le Vice-Premier Ministre et Ministre de l'Economie, des Consommateurs et de la Mer du Nord à communiquer un avis, dans un délai de trente jours prorogé jusqu'au 29 août 2013 (*) , sur un projet d'arrêté royal 'portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques'.

Le projet a été examiné par la deuxième chambre des vacations le 26 août 2013. La chambre était composée de Robert Andersen, premier président du Conseil d'Etat, Pierre Vandernoot et Michel Pâques, conseillers d'Etat, Yves De Cordt, assesseur et Anne-Catherine Van Geersdaele, greffier.

Le rapport a été présenté par Laurence Vancrayebeck, auditrice.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre Liénardy, président de chambre.

L'avis, dont le texte suit, a été donné le 26 août 2013.

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

Sur ces trois points, le projet appelle les observations suivantes.

Formalités préalables

Il ne ressort d'aucune des pièces communiquées au Conseil d'Etat que l'examen préalable de la nécessité de procéder à une évaluation d'incidence au sens de l'article 19/1 de la loi du 5 mai 1997 'relative à la coordination de la politique fédérale de développement durable' a bien été réalisé.

Si ce n'est chose faite, cet examen préalable devra donc encore être accompli, ainsi que, s'il y a lieu, l'évaluation d'incidence subséquente.

De Commissie zal de mogelijkheid hebben om contact op te nemen met de aangestelden om ze, wanneer dat nodig is, de informatie te vragen die ze wenst.

Artikel 9

Artikel 9 legt de betrokken aanbieders de verplichting op om het Instituut jaarlijks een aantal statistische inlichtingen mee te delen die bestemd zijn voor de minister bevoegd voor de elektronische communicatie en de minister van Justitie. De bevoegde ministers zorgen ervoor, in overeenstemming met artikel 10 van de richtlijn, dat deze gegevens meegedeeld worden aan de Europese Commissie.

Artikelen 10 en 11

Er zijn geen specifieke regels vastgesteld voor de inwerkingtreding van het onderhavige besluit. Een overgangsbepaling geeft de aanbieders evenwel een termijn van twaalf maanden om de nodige systemen in te voeren voor de bewaring van de gegevens. Op die manier kunnen de aanbieders die erin slagen om voor de termijn van twaalf maanden de nodige infrastructuur in te stellen voor de bewaring van de gegevens bedoeld in de artikelen 3 tot 6 van het onderhavige besluit, deze gegevens wettelijk bewaren.

We hebben de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaars,

De Minister van Economie,
J. VANDE LANOTTE

De Minister van Justitie,
Mevr. A. TURTELBOOM

Raad van State
afdeling Wetgeving
advies 53.841/2/V van 26 augustus 2013
over

een ontwerp van koninklijk besluit 'tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie'

Op 23 juli 2013 is de Raad van State, afdeling Wetgeving, door de Vice-Eerste Minister en Minister van Economie, Consumenten en Noordzee verzocht binnen een termijn van dertig dagen verlengd tot 29 augustus 2013 (*) een advies te verstrekken over een ontwerp van koninklijk besluit 'tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie'.

Het ontwerp is door de tweede vakantiekamer onderzocht op 26 augustus 2013 . De kamer was samengesteld uit Robert Andersen, eerste voorzitter van de Raad van State, Pierre Vandernoot en Michel Pâques, staatsraden, Yves De Cordt, assessor, en Anne-Catherine Van Geersdaele, griffier.

Het verslag is uitgebracht door Laurence Vancrayebeck, auditeur.

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

Het advies, waarvan de tekst hierna volgt, is gegeven op 26 augustus 2013.

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

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

Voorafgaande vormvereisten

Uit geen van de stukken die aan de Raad van State bezorgd zijn, blijkt dat het voorafgaand onderzoek met betrekking tot de noodzaak om een effectbeoordeling uit te voeren in de zin van artikel 19/1 van de wet van 5 mei 1997 'betreffende de coördinatie van het federale beleid inzake duurzame ontwikkeling', heeft plaatsgevonden.

Mocht dit nog niet gebeurd zijn, dan moeten dat voorafgaand onderzoek, en, zo nodig, de daaropvolgende effectbeoordeling dus nog uitgevoerd worden.

Observations générales

1. L'arrêté en projet vise à exécuter l'article 126 de la loi du 13 juin 2005 'relative aux communications électroniques', tel que remplacé par l'article 5 de la loi 'portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle' (1), afin de transposer partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 'sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, et modifiant la Directive 2002/58/CE' (ci-après, la Directive 2006/24/CE).

Plusieurs dispositions de l'arrêté en projet prévoient la conservation de données qui ne figurent pas dans la liste des données à conserver prévue par l'article 5 de la Directive 2006/24/CE. Il convient à cet égard de renvoyer à l'avis 53.272/4 donné le 27 mai 2013 sur l'avant-projet devenu la loi précitée, dans lequel le Conseil d'État s'est interrogé sur la question de savoir si le législateur pouvait prévoir la conservation de certaines données dans des buts qui dépassent les finalités prévues par la Directive 2006/24/CE. A ce propos, la section de législation a notamment observé ce qui suit :

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

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

Il reste que, vu la complexité du droit européen et, pour reprendre les termes de la Commission européenne, vu 'la relation juridique compliquée' entre la Directive 2006/24/CE et la Directive 2002/58/CE, il est permis de se demander si la solution qui serait la plus de nature à garantir le respect du droit européen ne consisterait pas à mettre en place deux systèmes parallèles, l'un transposant la Directive 2006/24/CE, l'autre s'appuyant sur la Directive 2002/58/CE. A cet égard, la section de législation observe par ailleurs que les considérants 15 et 16 du préambule de la Directive 2006/24/CE mentionnent que 'la Directive 95/46/CE et la Directive 2002/58/CE sont pleinement applicables aux données conservées conformément à la [Directive 2006/24/CE]'.

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

Selon l'article 15 de la Directive 2002/58/CE, les Etats membres peuvent prévoir la conservation de données pendant une durée limitée pour autant qu'il s'agisse d'une mesure « nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'Etat – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ».

A cet égard, le rapport au Roi contient de nombreux développements qui semblent pouvoir justifier que certaines données, bien que non mentionnées à l'article 5 de la Directive 2006/24/CE, soient conservées dans l'un des buts énumérés à l'article 126, § 2, de la loi précitée du 13 juin 2005.

2. A plusieurs reprises, l'arrêté en projet reproduit ou paraphrase des dispositions de l'article 126 de la loi précitée du 13 juin 2005.

Tel est notamment le cas de l'article 3 du projet – qui reproduit l'article 126, § 1er, alinéa 6, de la loi – et des articles 4, § 3, 5, § 3, 6, § 3 et 7, § 3, du projet – qui paraphrasent l'article 126, § 3, alinéas 1er et 2, de la loi. Ces dispositions seront dès lors omises.

Il n'appartient en effet pas au Roi de reproduire, dans un arrêté réglementaire, une règle déjà inscrite dans une disposition législative. Pareil procédé peut induire en erreur sur la nature de la règle en question. Il laisse par ailleurs à penser qu'il est au pouvoir du Roi de modifier cette règle alors que ce pouvoir appartient au seul législateur.

Algemene opmerkingen

1. Het ontworpen besluit strekt ertoe artikel 126 van de wet van 13 juni 2005 'betreffende de elektronische communicatie', zoals vervangen bij artikel 5 van de wet 'houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering'(1), uit te voeren om Richtlijn 2006/24/EG van 15 maart 2006 van het Europees Parlement en de Raad 'betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG' (hierna "Richtlijn 2006/24/EG" genoemd) gedeeltelijk om te zetten.

Diverse bepalingen van het ontworpen besluit voorzien in de bewaring van gegevens die niet voorkomen in de lijst van de te bewaren gegevens bedoeld in artikel 5 van Richtlijn 2006/24/EG. Wat dat betreft, dient verwezen te worden naar advies 53.272/4 van 27 mei 2013 over het voorontwerp van wet dat de voormelde wet geworden is, waarin de Raad van State zich heeft afgevraagd of de wetgever mocht voorzien in de bewaring van bepaalde gegevens met oogmerken die verder reiken dan de oogmerken bepaald door Richtlijn 2006/24/EG. De afdeling Wetgeving heeft hieromtrent onder meer het volgende opgemerkt :

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

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

Desalniettemin, gelet op de complexiteit van het Europees recht en, om de bewoordingen van de Europese Commissie aan te halen, gelet op 'dit ingewikkelde juridische verband' tussen Richtlijn 2006/24/EG en Richtlijn 2002/58/EG, kan men zich afvragen of de beste oplossing om te garanderen dat het Europees recht wordt nageleefd er niet in bestaat twee naast elkaar bestaande regelingen op te zetten : een regeling die Richtlijn 2006/24/EG omzet en een andere regeling die op Richtlijn 2002/58/EG steunt. In dit verband merkt de afdeling Wetgeving voorts op dat in overwegingen 15 en 16 van de aanhef van Richtlijn 2006/24/EG wordt vermeld dat 'de Richtlijnen 95/46/EG en 2002/58/EG integraal van toepassing zijn op de overeenkomstig (...) Richtlijn [2006/24/EG] bewaarde gegevens'.

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

Volgens artikel 15 van Richtlijn 2002/58/EG mogen de lidstaten bepalen dat gegevens gedurende een beperkte periode bewaard worden, voor zover het gaat om een maatregel die "in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem".

Het verslag aan de Koning bevat in dat verband talloze toelichtingen die lijken te kunnen rechtvaardigen dat bepaalde gegevens, hoewel niet opgenomen in artikel 5 van Richtlijn 2006/24/EG, bewaard worden met een van de oogmerken opgesomd in artikel 126, § 2, van de voormelde wet van 13 juni 2005.

2. In het ontworpen besluit worden meermaals bepalingen van artikel 126 van de voormelde wet van 13 juni 2005 overgenomen of geparafraseerd.

Dat is met name het geval in artikel 3 van het ontwerp – dat artikel 126, § 1, zesde lid, van de wet overneemt – en in de artikelen 4, § 3, 5, § 3, 6, § 3 en 7, § 3, van het ontwerp – die artikel 126, § 3, eerste en tweede lid, van de wet parafraseren. Deze bepalingen moeten dus vervallen.

Het komt de Koning immers niet toe in een verordeningsbesluit een regel over te nemen die reeds besloten ligt in een bepaling van wetgevende aard. Een dergelijke werkwijze kan verwarring doen ontstaan over de aard van de betreffende regel. Ze wekt bovendien de indruk dat de Koning bevoegd is om deze regel te wijzigen terwijl deze bevoegdheid alleen aan de wetgever toekomt.

3. L'article 126, § 1er, alinéa 1er, de la loi précitée du 13 juin 2005 impose aux fournisseurs de services ou de réseaux de communications électroniques qui y sont cités de conserver, notamment, des données « d'identification d'utilisateurs finals ». L'alinéa 4 de la même disposition habilite en outre le Roi à déterminer plus précisément les données qui entrent dans cette catégorie.

L'arrêté en projet ne se réfère pas à l'identification « d'utilisateurs finals », mais bien à l'identification « de l'abonné ou de l'utilisateur » (2). Ces trois notions – utilisateur, utilisateur final et abonné – sont respectivement définies par l'article 2, 12°, 13° et 15°, de la loi précitée du 13 juin 2005. Il ressort de ces définitions que la notion d'utilisateur est plus large que celle d'utilisateur final. Il n'est pas admissible qu'en ce qui concerne la conservation de données d'identification, l'arrêté en projet ait un champ d'application plus large que celui prévu par l'article 126 de la loi précitée du 13 juin 2005.

Il n'est pas certain que telle soit l'intention de l'auteur du projet. En effet, à plusieurs reprises, s'agissant d'énumérer les données qui permettent d'identifier « l'abonné ou l'utilisateur », l'arrêté en projet fait référence à l'utilisateur « enregistré », c'est-à-dire l'utilisateur qui s'est enregistré auprès d'un opérateur, par opposition à l'utilisateur qui lui aurait souscrit un abonnement. Si l'intention est donc uniquement de distinguer, parmi les utilisateurs finals, ceux qui sont abonnés et ceux qui sont enregistrés, l'arrêté en projet devrait être rédigé en ce sens.

Observations particulières

Préambule

A l'alinéa 1er, même si la directive mentionnée contribue à déterminer le cadre juridique du projet, elle n'en constitue pas le fondement légal.

L'alinéa 1er sera omis.

Dispositif

Article 2

L'article 2, 5°, de l'arrêté en projet, définit l'« identifiant d'un utilisateur » comme étant « l'identifiant exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'Internet ou à un service de communication par l'Internet ».

Or, dans les articles 6 et 7 de l'arrêté en projet, qui ont trait aux services d'accès à l'internet et aux services de communication par internet, il n'est pas fait référence à l'identifiant d'un utilisateur, mais bien à l'identifiant « de l'abonné ou de l'utilisateur ».

Selon le rapport au Roi, la définition de l'identifiant d'un utilisateur est une transposition d'un concept défini à l'article 2 de la Directive 2006/24/CE. Or, dans cet article, la notion utilisée est celle de « numéro d'identifiant », défini comme étant « le numéro d'identification exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'internet ou à un service de communication par l'internet ».

Mieux vaut dès lors utiliser cette notion de numéro d'identifiant tant à l'article 2, 5°, qu'aux articles 6 et 7 du projet.

Notes

(*) Par courriel du 25 juillet 2013.

(1) Cette loi a été adoptée par le Parlement en date du 18 juillet 2013 (*Doc. parl.*, Sénat., 2012-2013, n° 2222/4 et *Doc. parl.*, Chambre, 2012-2013, n° 2921/6). Selon les informations transmises par le délégué du ministre, elle devrait bientôt être transmise au Roi pour sanction et promulgation.

(2) Voir les articles 4, § 1er, 5, § 1er, 6, § 1er, et 7, § 1er, du projet.

Le greffier, Le premier président,

Anne-Catherine Van Geersdaele Robert Andersen

3. Artikel 126, § 1, eerste lid, van de voormelde wet van 13 juni 2005 legt de erin genoemde aanbieders van openbare elektronische communicatiediensten of –netwerken op om onder meer gegevens voor de "identificatie van de eindgebruikers" te bewaren. Bovendien verleent het vierde lid van dezelfde bepaling de Koning de bevoegdheid om de onder deze categorie vallende gegevens nader te bepalen.

Het ontworpen besluit verwijst niet naar de identificatie "van eindgebruikers", maar naar de identificatie "van de abonnee of de gebruiker".(2) Deze drie begrippen – gebruiker, eindgebruiker en abonnee – zijn respectievelijk gedefinieerd in artikel 2, 12°, 13° en 15° van de voormelde wet van 13 juni 2005. Uit deze definities volgt dat het begrip 'gebruiker' ruimer is dan dat van 'eindgebruiker'. Het is onaanvaardbaar dat, met betrekking tot de bewaring van identificatiegegevens, het ontworpen besluit een ruimer toepassingsgebied heeft dan dat waarin artikel 126 van de voormelde wet van 13 juni 2005 voorziet.

Het is niet zeker dat dat de bedoeling van de steller van het ontwerp is. Bij het opnoemen van de gegevens die het mogelijk maken "de abonnee of de gebruiker" te identificeren, verwijst het ontworpen besluit immers meermaals naar de "geregistreerde" gebruiker, met andere woorden de gebruiker die zich bij een operator geregistreerd heeft, in tegenstelling tot de gebruiker die een abonnement heeft genomen. Als het dus alleen de bedoeling is om de eindgebruikers onder te verdelen in geabonneerde en geregistreerde gebruikers, dan zou het ontworpen besluit in die zin moeten worden geredigeerd.

Bijzondere opmerkingen

Aanhef

De in het eerste lid aangehaalde Richtlijn vormt geen rechtsgrond van het ontwerp, ook al draagt ze bij tot het bepalen van het juridische kader ervan.

Het eerste lid moet bijgevolg vervallen.

Dispositief

Artikel 2

Artikel 2, 5°, van het ontworpen besluit definieert "gebruikersidentificatie" als "een unieke identificatie die aan een persoon wordt toegewezen wanneer deze zich abonneert op of registreert bij een internettoegangsdienst of een internetcommunicatiedienst".

In de artikelen 6 en 7 van het ontworpen besluit, die betrekking hebben op de internettoegangsdiensten en de internetcommunicatiediensten, wordt evenwel niet naar de "gebruikersidentificatie", maar naar de "abonnee- of gebruikersidentificatie" verwezen.

Volgens de Franse versie van het verslag aan de Koning vormt de definitie van de "identifiant d'un utilisateur" een omzetting van een begrip dat gedefinieerd is in artikel 2 van Richtlijn 2006/24/EG. In dit artikel is het gebruikte begrip echter "numéro d'identifiant", gedefinieerd als "le numéro d'identification exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'internet ou à un service de communication par l'internet".

Het zou dan ook beter zijn om, zowel in artikel 2, 5°, als in de artikelen 6 en 7 van het ontwerp, in de Nederlandse tekst het begrip "gebruikersidentificatie" en in de Franse tekst het begrip "numéro d'identifiant" te gebruiken.

Nota's

(*) Bij e-mail van 25 juli 2013.

(1) Deze wet is op 18 juli 2013 door het Parlement goedgekeurd (*Parl.St.* Senaat 2012-13, nr. 2222/4 en *Parl.St.* Kamer 2012-13, nr. 2921/6). Volgens de door de gemachtigde van de Minister verstrekte informatie zou ze binnenkort naar de Koning overgezonden worden voor bekrachtiging en afkondiging.

(2) Zie de artikelen 4, § 1, 5, § 1, 6, § 1, en 7, § 1, van het ontwerp.

De griffier, De eerste voorzitter,

Anne-Catherine Van Geersdaele Robert Andersen

19 SEPTEMBRE 2013. — Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 13 juin 2005 relative aux communications électroniques, l'article 126, tel que modifié par la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité et par la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle;

Vu les avis de l'Institut belge des services postaux et des télécommunications, donnés les 18 juin 2008, 7 juillet 2008 et 12 mars 2013;

Vu les avis de la Commission de la protection de la vie privée, n° 24/2008, donné le 2 juillet 2008 et n° 20/2009, donné le 1er juillet 2009;

Vu l'avis de l'Inspecteur des Finances du SPF Economie, donné le 14 mars 2013;

Vu l'avis de l'Inspecteur des Finances du SPF Justice, donné le 18 mars 2013;

Vu l'accord du Ministre du Budget, donné le 25 mars 2013;

Vu la consultation du 29 mars 2013 au 9 avril 2013 du Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision;

Vu l'accord du Comité de concertation du 24 avril 2013;

Vu l'avis n° 53.841/2/V du Conseil d' Etat, donné le 26 août 2013, en application de l'article 84, § 1er, alinéa 1er, 1°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973;

Sur la proposition du Ministre de l'Economie et de la Ministre de la Justice et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. Le présent arrêté transpose partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive « conservation de données ») (*J.O. C.E.* 13 avril 2006, L 105/54) et l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») (*J.O.C.E.* 31 juillet 2002, L 201/37).

Art. 2. Pour l'application de présent arrêté, il y a lieu d'entendre par :

1° « Loi » : la loi du 13 juin 2005 relative aux communications électroniques;

2° « Institut » : l'Institut belge des services postaux et des télécommunications, tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;

3° « Ministre » : le ministre ou le secrétaire d'Etat qui a les télécommunications dans ses attributions;

4° « Arrêté royal du 9 janvier 2003 » : l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques;

5° « Identifiant d'un utilisateur final » : l'identifiant exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'Internet ou à un service de communication par l'Internet;

6° « Identifiant cellulaire » : le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin;

7° « Données personnelles » : les nom et prénom ainsi que les adresses de facturation et de livraison de l'utilisateur final.

Art. 3. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final;

2° les données personnelles de l'utilisateur final;

19 SEPTEMBER 2013. — Koninklijk besluit tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie

FILIP, Koning der Belgen,

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

Gelet op de wet van 13 juni 2005 betreffende de elektronische communicatie, artikel 126, zoals gewijzigd bij de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten en door de wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering;

Gelet op de adviezen van het Belgisch Instituut voor postdiensten en telecommunicatie, gegeven op 18 juni 2008, 7 juli 2008 en 12 maart 2013;

Gelet op de adviezen van de Commissie voor de bescherming van de persoonlijke levenssfeer, nr. 24/2008, gegeven op 2 juli 2008 en nr. 20/2009, gegeven op 1 juli 2009;

Gelet op het advies van de Inspecteur van Financiën, van de FOD Economie, gegeven op 14 maart 2013;

Gelet op het advies van de Inspecteur van Fnanciën van de FOD Justitie, gegeven op 18 maart 2013;

Gelet op de akkoordbevinding van de Minister van Begroting, gegeven op 25 maart 2013;

Gelet op de raadpleging van 29 maart 2013 tot 9 april 2013 van het Interministerieel Comité voor Telecommunicatie en Radio-omroep en Televisie;

Gelet op het akkoord van het Overlegcomité van 24 april 2013;

Gelet op het advies nr. 53.841/2/V van de Raad van State, gegeven op 26 augustus 2013, met toepassing van artikel 84, § 1, eerste lid, 1°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Minister van Economie en van de Minister van Justitie en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Dit besluit voorziet in een gedeeltelijke omzetting van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische-communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG ("dataretentierichtlijn") (*PbEG* 13 april 2006, L 105/54) en van artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ("richtlijn betreffende privacy en elektronische communicatie") (*PbEG* 31 juli 2002, L 201/37).

Art. 2. Voor de toepassing van dit besluit wordt verstaan onder :

1° "Wet" : de wet van 13 juni 2005 betreffende de elektronische communicatie;

2° "Instituut" : het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

3° "Minister" : de minister of staatssecretaris die de Telecommunicatie onder zijn bevoegdheid heeft;

4° "Koninklijk besluit van 9 januari 2003" : het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie;

5° "Eindgebruikersidentificatie" : een unieke identificatie die aan een persoon wordt toegewezen wanneer deze zich abonneert op of registreert bij een internettoegangsdienst of een internetcommunicatiedienst;

6° "Celidentiteit" : de unieke code van een cel van waaruit een mobiele-telefonieoproep werd begonnen of beëindigd;

7° "Persoonsgegevens" : de naam en voornaam, en het facturatie- en het leveringsadres van de eindgebruiker.

Art. 3. § 1. Wat betreft de gegevens voor de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van openbare diensten voor vaste telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° het aan de eindgebruiker toegewezen nummer;

2° de persoonsgegevens van de eindgebruiker;

3° la date de début de l'abonnement ou de l'enregistrement au service;

4° le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit;

5° en cas de transfert du numéro de l'utilisateur final auprès d'un autre fournisseur, l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré;

6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identification du numéro de téléphone de l'appelant et de l'appelé;

2° la localisation du point de terminaison du réseau de l'appelant et de l'appelé;

3° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

4° la date et l'heure exacte du début et de la fin de l'appel;

5° la description du service de téléphonie utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 4. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° le numéro attribué à l'utilisateur final ainsi que l'identité internationale d'abonné mobile (« International Mobile Subscriber Identity », « IMSI »);

2° les données personnelles de l'utilisateur final;

3° la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final;

4° la date et l'heure de la première activation du service, ainsi que l'identifiant cellulaire à partir duquel le service a été activé;

5° les services annexes auxquels l'utilisateur final a souscrit;

6° en cas de transfert de numéro auprès d'un autre opérateur, l'identité de l'opérateur d'origine de l'utilisateur final;

7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service;

8° le numéro d'identification du terminal mobile de l'utilisateur final (« International Mobile Equipment Identity », « IMEI »).

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identification du numéro de téléphone de l'appelant et de l'appelé;

2° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré;

3° l'identité internationale d'abonné mobile (« International Mobile Subscriber Identity », « IMSI ») de l'appelant et de l'appelé;

4° l'identité internationale d'équipement mobile (« International Mobile Equipment Identity », « IMEI ») du terminal mobile de l'appelant et de l'appelé;

5° la date et l'heure exacte du début et de la fin de l'appel;

6° la localisation du point de terminaison du réseau au début et à la fin de chaque connexion;

3° de datum van aanvang van het abonnement of van de registratie voor de dienst;

4° het soort van gebruikte vaste-telefoniedienst alsook de andere soorten van gebruikte diensten waarop de eindgebruiker ingeschreven heeft;

5° in geval van overdracht van het nummer van de eindgebruiker naar een andere operator, de identiteit van de aanbieder die het nummer en de identiteit overdraagt van de aanbieder naar wie het nummer wordt overgedragen;

6° de gegevens betreffende betalingswijze, identificatie van het betalingsmiddel en tijdstip van betaling voor het abonnement of voor het gebruik van de dienst.

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van openbare diensten voor vaste telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie de volgende gegevens :

1° de identificatie van het telefoonnummer van de oproeper en van de opgeroepene;

2° de plaats van het netwerkaansluitpunt van de oproeper en van de opgeroepene;

3° in geval van een groepsgesprek, oproepdoorschakeling of –doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

4° de datum en het juiste tijdstip van aanvang en einde van de oproep;

5° de beschrijving van de gebruikte telefoniedienst.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 4. § 1. Wat betreft de gegevens voor de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van een openbare dienst voor mobiele telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° het aan de eindgebruiker toegewezen nummer alsook de internationale identiteit van de mobiele abonnee ("International Mobile Subscriber Identity", "IMSI");

2° de persoonsgegevens van de eindgebruiker;

3° de datum en de plaats van inschrijving op het abonnement of de registratie van de eindgebruiker;

4° de datum en het tijdstip van de eerste activering van de dienst, alsook de celidentiteit van waaruit de dienst is geactiveerd;

5° de aanvullende diensten waarop de eindgebruiker heeft ingetekend;

6° in geval van nummeroverdracht naar een andere operator, de identiteit van de operator vanwaar de eindgebruiker komt;

7° de gegevens betreffende betalingswijze, identificatie van het betaalmiddel en tijdstip van de betaling voor het abonnement of voor het gebruik van de dienst;

8° het identificatienummer van het mobiele eindtoestel van de eindgebruiker ("International Mobile Equipment Identity", "IMEI").

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van een openbare dienst voor mobiele telefonie en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de identificatie van het telefoonnummer van de oproeper en van de opgeroepene;

2° in geval van een groepsgesprek, oproepdoorschakeling of –doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

3° de "International Mobile Subscriber Identity" ("IMSI") van de oproepende en opgeroepen deelnemer;

4° de "International Mobile Equipment Identity" ("IMEI") van het mobiele eindapparaat van de oproepende en opgeroepen deelnemer;

5° de datum en het juiste tijdstip van aanvang en einde van de oproep;

6° de locatie van het netwerkaansluitpunt bij aanvang en bij het einde van elke verbinding;

7° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée;

8° les caractéristiques techniques du service de téléphonie utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 5. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de service d'accès à l'internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final;

4° l'adresse IP et le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final;

5° l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu' utilisateur final;

6° les services annexes auxquels l'utilisateur final a souscrit auprès du prestataire d'accès Internet public concerné;

7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de service d'accès à l'internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° *a)* l'adresse IP;

b) en cas d'utilisation partagée d'une adresse IP, les ports attribués de l'adresse IP ainsi que la date et l'heure de l'attribution;

3° l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service d'accès à l'internet;

5° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée;

6° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi .

Art. 6. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de courrier électronique par internet accessible au public, les fournisseurs d'un service de téléphonie par internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final;

2° les données personnelles de l'utilisateur final;

3° la date et l'heure de la création du compte de courrier électronique ou de téléphonie par internet;

4° l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet;

5° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service.

7° de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt;

8° de technische karakteristieken van de gebruikte telefoondienst.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 5. § 1. Wat betreft de gegevens in verband met de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van openbare internettoegangsdiensten en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de toegewezen eindgebruikersidentificatie;

2° de persoonsgegevens van de eindgebruiker;

3° de datum en het tijdstip van het nemen van het abonnement of de registratie van de eindgebruiker;

4° het IP-adres en de bronpoort van de verbinding die gediend hebben voor het nemen van het abonnement of voor de registratie van de eindgebruiker;

5° de identificatie van het netwerkaansluitpunt dat gediend heeft voor het nemen van het abonnement of voor de inschrijving als eindgebruiker;

6° de aanvullende diensten waarop de eindgebruiker ingeschreven heeft bij de betrokken aanbieder van openbare internettoegang;

7° de gegevens betreffende betalingswijze, identificatie van het betaalmiddel en tijdstip van de betaling voor het abonnement of voor het gebruik van de dienst.

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van openbare internettoegangsdiensten en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de eindgebruikersidentificatie;

2° *a)* het IP-adres;

b) in geval van het gedeelde gebruik van een IP-adres, de toegewezen poorten van het IP-adres evenals de datum en het uur van de toewijzing;

3° de identificatie en de locatie van het netwerkaansluitpunt dat door de eindgebruiker wordt gebruikt bij aanvang en bij het einde van een verbinding;

4° de datum en het tijdstip van de log-in en log-off van een sessie van de internettoegangsdienst;

5° het tijdens de sessie of een ander opgevraagde tijdseenheid geüploade en gedownloade volume van gegevens;

6° de gegevens voor het identificeren van de geografische locatie van cellen middels referentie aan hun celidentiteit op het ogenblik dat de verbinding is gemaakt.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 6. § 1. Wat betreft de gegevens voor de identificatie van de eindgebruiker, van de eindapparatuur die vermoed wordt te zijn gebruikt en van de gebruikte elektronische-communicatiedienst, bewaren de aanbieders van een openbare e-maildienst via internet, de aanbieders van een openbare internettelefoniedienst en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de eindgebruikersidentificatie;

2° de persoonsgegevens van de eindgebruiker;

3° de datum en het tijdstip waarop de e-mail- of internettelefonieaccount is gecreëerd;

4° het IP-adres en de bronpoort die gediend hebben voor de creatie van de e-mail- of internettelefonieaccount;

5° de gegevens betreffende betalingswijze, identificatie van het betaalmiddel en tijdstip van de betaling voor het abonnement of het gebruik van de dienst.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d'un service de courrier électronique par internet accessible au public, les fournisseurs d'un service de téléphonie par internet accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1° l'identifiant de l'utilisateur final du compte de courrier électronique ou de téléphonie par internet, ainsi que le numéro ou l'identifiant du destinataire prévu de la communication;

2° le numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public dans le cadre d'un service téléphonique par internet;

3° *a)* l'adresse IP et le port source utilisés par l'utilisateur final;

b) l'adresse IP et le port source utilisés par le destinataire;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service de courrier électronique ou de téléphonie par internet;

5° la date et l'heure de la connexion établie à l'aide du compte de téléphonie par Internet;

6° les caractéristiques techniques du service utilisé.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi .

Art. 7. § 1er. Les fournisseurs de réseaux ou de services qui utilisent conjointement différents services conservent toutes les données relatives aux différents services utilisés, conformément aux articles 3 à 6.

La combinaison des données enregistrées doit permettre d'établir la relation entre l'origine de la communication et sa destination.

§ 2. Les heures qui doivent être enregistrées conformément aux articles 3 à 6 du présent arrêté doivent, en se référant au système de la division du jour en 24 heures, être précises à la seconde près. L'indication de l'heure doit toujours se faire par référence au fuseau horaire auquel la Belgique appartient et en tenant compte des périodes de l'heure d'été et de l'heure d'hiver.

Les fournisseurs précités doivent synchroniser l'horloge de leurs systèmes utilisés pour l'enregistrement de toutes les heures mentionnées dans le présent arrêté avec le signal horaire GPS.

Art. 8. § 1er. Chaque fournisseur désigne parmi les membres de la Cellule de Coordination de Justice, visée à l'article 2 de l'arrêté royal du 9 janvier 2003, un préposé à la protection des données à caractère personnel.

Dans l'exercice de ses missions, le préposé à la protection des données à caractère personnel agit en toute indépendance, et a accès à toutes les données visées par le présent arrêté qui sont traitées par le fournisseur ainsi qu'à tous les locaux pertinents du fournisseur.

L'exercice de ses missions ne peut entraîner pour le préposé des désavantages. Il ne peut, en particulier, être licencié ou remplacé comme préposé à cause de l'exécution des tâches qui lui sont confiées, sans motivation approfondie.

Le préposé à la protection des données veille à ce que les traitements effectués par la cellule Coordination Justice soient exécutés conformément à la loi.

Le préposé doit être placé à un niveau de la hiérarchie tel qu'il ait la possibilité de communiquer directement avec le management ou le comité de direction et d'exercer sa mission directement auprès du responsable du traitement.

§ 2. En particulier, il veille à ce que :

1° les traitements poursuivent les finalités décrites à l'article 126 de la loi;

2° pour l'application du présent arrêté, seules les données décrites ci-dessus soient conservées pour les finalités prévues;

3° seules les catégories de personnes autorisées en vertu de l'article 126 de la loi et du présent arrêté aient accès aux données;

4° les mesures de protection des données décrites dans l'article 126 de la loi soient respectées.

§ 2. Wat de verkeers- en locatiegegevens betreft, bewaren de aanbieders van een openbare e-maildienst via internet, de aanbieders van een openbare internettelefoniedienst en de aanbieders van de onderliggende openbare netwerken voor elektronische communicatie, de volgende gegevens :

1° de eindgebruikersidentificatie met betrekking tot de e-mail- of internettelefonieaccount, alsook het nummer of de identificatiecode van de beoogde ontvanger van de communicatie;

2° het telefoonnummer toegewezen aan elke communicatie die het openbare telefoonnetwerk binnenkomt in het kader van een internettelefoniedienst;

3° *a)* het IP-adres en de bronpoort die worden gebruikt door de eindgebruiker;

b) het IP-adres en de bronpoort die worden gebruikt door de bestemmeling;

4° de datum en het tijdstip van de log-in en log-off van een sessie van een e-maildienst via internet of internettelefoniedienst;

5° de datum en het tijdstip van een verbinding die tot stand wordt gebracht met behulp van de internettelefonieaccount;

6° de technische karakteristieken van de gebruikte dienst.

§ 3. De in paragraaf 1 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, eerste lid, van de wet.

De in paragraaf 2 bedoelde gegevens zijn onderworpen aan artikel 126, § 3, tweede lid, van de wet.

Art. 7. § 1. De aanbieders van netwerken of diensten die samen verschillende diensten gebruiken, bewaren alle gegevens in verband met de verschillende gebruikte diensten, zoals die worden opgelegd in de artikelen 3 tot 6.

De combinatie van de geregistreerde gegevens moet het mogelijk maken om de relatie te leggen tussen de bron en de bestemming van de communicatie.

§ 2. De tijdstippen die op basis van de artikelen 3 tot 6 van dit besluit moeten worden geregistreerd of meegedeeld, dienen gebruikmakend van het 24-urenstelsel precies te zijn tot op de seconde. De tijdsaanduiding moet steeds gebeuren in de Belgische tijdszone, rekening houdend met de periodes van zomer- en wintertijd.

De voormelde aanbieders moeten de klok op hun systemen die gebruikt wordt voor de registratie van alle tijdstippen die in dit besluit worden vermeld, synchroniseren met het GPS-tijdssignaal.

Art. 8. § 1. Elke aanbieder wijst onder de leden van de Coördinatiecel Justitie, bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003, een aangestelde voor de bescherming van de persoonsgegevens aan.

Bij de uitvoering van zijn opdrachten handelt de aangestelde voor de bescherming van de persoonsgegevens in volledige onafhankelijkheid, en heeft hij toegang tot alle in dit besluit bedoelde gegevens die door de aanbieder worden verwerkt, alsook tot alle relevante lokalen van de aanbieder.

De uitoefening van zijn opdrachten mag voor de aangestelde geen nadelen met zich brengen. Hij mag in het bijzonder als aangestelde niet worden ontslagen of vervangen wegens de uitvoering van de taken die hem zijn toevertrouwd, zonder uitvoerige motivatie.

De aangestelde voor de gegevensbescherming zorgt ervoor dat de verwerkingen door de Coördinatiecel Justitie worden uitgevoerd overeenkomstig de wet.

De aangestelde dient op een dusdanig niveau in de hiërarchie geplaatst te worden zodat hij over de mogelijkheid beschikt om rechtstreeks met het management of het directiecomité te communiceren en zijn opdracht rechtstreeks uit te oefenen bij de verantwoordelijke voor de verwerking.

§ 2. In het bijzonder zorgt hij ervoor dat :

1° de verwerkingen de in artikel 126 van de wet beschreven doeleinden nastreven;

2° ter uitvoering van dit besluit worden enkel de hierboven beschreven gegevens voor de vastgestelde doeleinden bewaard;

3° enkel de categorieën van krachtens artikel 126 van de wet en dit besluit gemachtigde personen toegang hebben tot de gegevens;

4° de maatregelen ter bescherming van de in artikel 126 van de wet beschreven gegevens in acht worden genomen.

Art. 9. Au plus tard le 1er mars de chaque année, les fournisseurs de services et de réseaux communiquent à l'Institut les informations statistiques anonymes suivantes :

a) le nombre de cas dans lesquels des données ont été, au cours de la dernière année civile écoulée, transmises aux autorités compétentes;

b) pour chaque donnée transmise, le délai 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;

c) les cas dans lesquels des demandes de données n'ont pu être satisfaites.

L'Institut transmet ces informations annuellement au ministre et au Ministre de la Justice.

Art. 10. Les fournisseurs de services et de réseaux doivent être en mesure de conserver les données visées aux articles 3 à 6 au plus tard le premier jour qui suit l'expiration d'un délai d'un an prenant cours le jour de la publication du présent arrêté au *Moniteur belge*.

Art. 11. Le ministre qui a les Télécommunications dans ses attributions est chargé de l'exécution du présent arrêté.

Donné à Bruxelles, le 19 septembre 2013.

PHILIPPE

Par le Roi :

Le Ministre de l'Economie,
J. VANDE LANOTTE

La Ministre de la Justice,
Mme A. TURTELBOOM

Art. 9. Uiterlijk op 1 maart van elk jaar deelt elke aanbieder van een dienst of netwerk de volgende anonieme statistische inlichtingen mee aan het Instituut :

a) het aantal gevallen waarin in de loop van het jongste afgelopen kalenderjaar gegevens zijn verstrekt aan de bevoegde autoriteiten;

b) voor elk overgezonden gegeven 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;

c) de gevallen waarin verzoeken om gegevens niet konden worden ingewilligd.

Het Instituut bezorgt die inlichtingen jaarlijks aan de minister en aan de Minister van Justitie.

Art. 10. De aanbieders van diensten en netwerken moeten uiterlijk de eerste dag die volgt op de afloop van een termijn van een jaar die ingaat de dag waarop dit besluit wordt bekendgemaakt in het *Belgisch Staatsblad* in staat zijn om de in de artikelen 3 tot 6 bedoelde gegevens te bewaren.

Art. 11. De minister bevoegd voor Telecommunicatie is belast met de uitvoering van dit besluit.

Gegeven te Brussel, 19 september 2013.

FILIP

Van Koningswege :

De Minister van Economie,
J. VANDE LANOTTE

De Minister van Justitie,
Mevr. A. TURTELBOOM

SERVICE PUBLIC FEDERAL ECONOMIE, P.M.E., CLASSES MOYENNES ET ENERGIE ET SERVICE PUBLIC FEDERAL FINANCES

[C − 2013/03330]

1er OCTOBRE 2013. — Arrêté royal relatif aux modalités d'application en ce qui concerne la certification d'un système de caisse enregistreuse dans le secteur horeca

RAPPORT AU ROI

Sire,

La loi du 30 juillet 2013 relative à la certification d'un système de caisse enregistreuse dans le secteur horeca a pour objet d'instaurer une procédure de certification des systèmes de caisse enregistreuse destinée à garantir le bon fonctionnement des mesures mises en place dans le cadre de l'arrêté royal du 30 décembre 2009 fixant la définition et les conditions auxquelles doit répondre un système de caisse enregistreuse dans le secteur horeca. Ces mesures visent à encadrer la réduction du taux de T.V.A. à 12 p.c. pour les prestations de restaurant et de restauration.

Afin de garantir que le système de caisse enregistreuse utilisé par l'exploitant d'un établissement où sont consommés régulièrement des repas ainsi que par le traiteur qui effectue régulièrement des prestations de restauration, corresponde aux exigences techniques minimales imposées par le service compétent du SPF Finances, le fabricant ou l'importateur est tenu de soumettre pour certification chaque système de caisse ou chaque fiscal data module mis sur le marché en Belgique.

Les articles 3, 4 et 5 de la loi relative à la certification d'un système de caisse enregistreuse dans le secteur horeca, confèrent au Roi le pouvoir de régler certaines modalités d'application relatives à la procédure de certification.

Ces modalités d'applications font l'objet du présent projet d'arrêté royal.

L'article 1er du projet précise que le système de caisse enregistreuse faisant l'objet du présent arrêté ne concerne que le secteur horeca.

La délégation au Ministre des Finances de la détermination des exigences techniques de ce système s'avère nécessaire compte tenu du nombre et de la complexité des éléments techniques auxquels doit répondre le système de caisse ou le fiscal data module. Ces exigences techniques feront ainsi l'objet d'une circulaire appropriée.

FEDERALE OVERHEIDSDIENST ECONOMIE, K.M.O., MIDDENSTAND EN ENERGIE EN FEDERALE OVERHEIDSDIENST FINANCIEN

[C − 2013/03330]

1 OKTOBER 2013. — Koninklijk besluit met betrekking tot de toepassingsmodaliteiten ten aanzien van de certificatie van een geregistreerd kassasysteem in de horecasector

VERSLAG AAN DE KONING

Sire,

De wet van 30 juli 2013 met betrekking tot de certificatie van een geregistreerd kassasysteem in de horecasector voorziet in de invoering van een certificatieprocedure van de geregistreerde kassasystemen bestemd om de goede werking te verzekeren van de maatregelen ingesteld in het kader van het koninklijk besluit van 30 december 2009 tot het bepalen van de definitie en de voorwaarden waaraan een geregistreerd kassasysteem in de horecasector moet voldoen. Deze maatregelen ondersteunen de verlaging van het btw-tarief tot 12 pct. voor de restaurant- en cateringdiensten.

Om te verzekeren dat het geregistreerd kassasysteem, gebruikt door de exploitant van een inrichting waar regelmatig maaltijden worden verbruikt alsmede door de traiteur die regelmatig cateringdiensten verricht, beantwoordt aan de minimale technische vereisten opgelegd door de bevoegde dienst van de FOD Financiën, is de producent of de invoerder ertoe gehouden elk kassasysteem of elke fiscale data module die op de Belgische markt wordt gebracht ter certificatie aan te bieden.

De artikelen 3, 4 en 5 van de wet met betrekking tot de certificatie van een geregistreerd kassasysteem in de horecasector, verlenen aan de Koning de macht om bepaalde toepassingsmodaliteiten met betrekking tot de certificatieprocedure te regelen.

Deze toepassingsmodaliteiten maken het voorwerp uit van onderhavig ontwerp van koninklijk besluit.

Artikel 1 van het ontwerp preciseert dat het geregistreerd kassasysteem waarover onderhavig besluit handelt, de horecasector aanbelangt.

De delegatie aan de Minister van Financiën om de technische vereisten van dit systeem vast te leggen, is noodzakelijk rekening houdend met het aantal en de complexiteit van deze bestanddelen waaraan het kassasysteem of de fiscale data module dient te beantwoorden. Deze technische vereisten zullen aldus het voorwerp uitmaken van een circulaire ter zake.