



CONSEIL D'ÉTAT
section de législation

RAAD VAN STATE
afdeling Wetgeving

avis 53.272/4
du 27 mai 2013

advies 53.272/4
van 27 mei 2013

sur

over

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

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

Le 26 avril 2013, le Conseil d'État, section de législation, a été invité par le Vice-Premier Ministre et Ministre de l'Économie à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du code d'instruction criminelle'.

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

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

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

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

*

Op 26 april 2013 is de Raad van State, afdeling Wetgeving, door de Vice-Eerste Minister en Minister van Economie verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van Strafvordering'.

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

Het verslag is uitgebracht door Anne VAGMAN, eerste auditeur.

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

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

*

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

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

OBSERVATION LIMINAIRE

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

L'exposé des motifs doit être complété par la présentation d'un tableau de correspondance entre le texte de l'avant-projet et celui des normes européennes pertinentes afin que les Chambres législatives puissent se prononcer en connaissance de cause sur le choix des moyens mis en œuvre par l'auteur de l'avant-projet, et éviter que l'exercice du droit d'amendement inscrit dans l'article 76 de la Constitution ne dépasse les limites du pouvoir d'appréciation laissé aux États membres par le droit européen ¹.

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

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

¹ *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet « Technique législative », recommandations n^{os} 191 à 195.

À cette occasion, la section de législation rappelle que ces tableaux auraient dû lui être communiqués d'initiative.

OBSERVATIONS GÉNÉRALES

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

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

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

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

2. Lors de son adoption en 2005, cette disposition avait pour objet de mettre en œuvre la possibilité conférée aux États membres par l'article 15 de la directive 2002/58/CE².

Cet article 15 disposait comme suit :

« Article 15

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

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

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions

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

nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

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

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

« 1bis. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication aux fins visées à l'article 1^{er}, paragraphe 1, de ladite directive »³.

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

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

Elles ont trait aux services de téléphonie fixe en réseau, de téléphonie mobile, d'accès à l'internet, de courrier électronique par l'internet et de téléphonie par l'internet⁶.

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

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

³ Quant à la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, elle a inséré, dans le même article, un paragraphe 1^{er}ter, rédigé comme suit :

« 1^{er}ter. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse ».

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

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

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

- l'autre, issu de la directive 2006/24/CE, qui, dans un but d'harmonisation en vue d'éliminer des entraves au marché intérieur⁷, impose aux États membres, de mettre en place un système de conservation de données afin de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne (par exemple, la criminalité organisée et les actes de terrorisme⁸).

Comme la Commission européenne l'a relevé :

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

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

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

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

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

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

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

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

Concernant la circonstance que les dispositions en matière de conservation des données en vigueur dans les États membre postérieurement à l'adoption de la

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

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

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

directive 2006/24/CE imposent, dans de nombreux cas ¹⁰, la conservation de certaines données en vue de rencontrer des objectifs dépassant la recherche, la détection et la poursuite « d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne », la Commission européenne a relevé ce qui suit :

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

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

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

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

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

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

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

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

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

Les observations particulières qui suivent prennent en compte cette exigence.

OBSERVATIONS PARTICULIÈRES

ARRÊTÉ DE PRÉSENTATION

L'arrêté de présentation sera rédigé comme suit :

« ALBERT II, Roi des Belges,

À tous, présents et à venir, Salut.

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

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

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

DISPOSITIF

Article 1^{er} nouveau

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

« Art. 1^{er}. La présente loi règle une matière visée à l'article 78 de la Constitution » ¹⁵.

Les autres articles seront renumérotés en conséquence.

Article 3

(devenant article 4)

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

¹⁴ *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet « Technique législative », recommandations n^{os} 226 et 227, formule F 5.

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

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

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

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

Par ailleurs, tant le procureur du Roi que le juge d'instruction, chacun pour leurs compétences propres, doivent respecter les principes de proportionnalité, de subsidiarité et de nécessité lorsqu'ils requièrent la collaboration des fournisseurs de réseaux ou de services pour la communication des données conservées. À cet égard, il convient de souligner que le fait de pouvoir avoir accès à ces données conservées peut tout autant permettre aux autorités judiciaires d'inculper la personne que de l'innocenter ».

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

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

Le texte en projet sera complété en conséquence.

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

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

« § 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[...]

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

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

La disposition à l'examen sera modifiée en conséquence.

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

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

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

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

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

*

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

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

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

INLEIDENDE OPMERKING

Het voorliggende voorontwerp strekt tot de gedeeltelijke omzetting van richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 ‘betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG’ (hierna richtlijn 2006/24/EG genoemd).

Aan de memorie van toelichting moet een tabel worden toegevoegd waarin voor elke bepaling van het voorontwerp de overeenkomstige bepalingen van de relevante Europese richtlijnen wordt aangegeven, opdat de Wetgevende Kamers zich met kennis van zaken kunnen uitspreken over de middelen die de steller van het voorontwerp heeft gekozen en opdat het amenderingsrecht vervat in artikel 76 van de Grondwet niet verder reikt dan de beoordelingsbevoegdheid die de lidstaten krachtens het Europees recht kunnen uitoefenen.¹

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

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

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

ALGEMENE OPMERKINGEN

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

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

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

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

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

Dat artikel 15 luidde als volgt:

“Artikel 15

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

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

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

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

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

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

“*1bis*. Lid 1 is niet van toepassing op de uit hoofde van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden”.³

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

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

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

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

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

³ Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 heeft in hetzelfde artikel een lid *1ter* ingevoegd, luidende als volgt:

“*1ter*. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord”.

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

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

⁶ Artikel 5 van richtlijn 2006/24/EG.

- de andere regeling komt voort uit richtlijn 2006/24/EG en streeft ernaar de verschillende nationale wetgevingen op elkaar af te stemmen teneinde te voorkomen dat de werking van de interne markt wordt belemmerd⁷; ze verplicht de lidstaten een regeling voor gegevensbewaring in te voeren om te garanderen dat deze gegevens beschikbaar zijn om ernstige strafbare feiten zoals gedefinieerd in de nationale wetgevingen van de lidstaten, (bijvoorbeeld georganiseerde misdaad en terroristische daden)⁸ te onderzoeken, op te sporen en te vervolgen.

De Commissie heeft het volgende gesteld:

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

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

Aldus luidt paragraaf 4 van de ontworpen bepaling als volgt:

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

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

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

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

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

Betreffende de omstandigheid dat de bepalingen inzake gegevensbewaring die na de aanneming van richtlijn 2006/24/EG in de Europese lidstaten van kracht zijn geworden, in tal van gevallen¹⁰ voorschrijven bepaalde gegevens te bewaren teneinde doelstellingen te

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

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

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

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

verwezenlijken die verder reiken dan het onderzoeken, opsporen en vervolgen van “ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten”, heeft de Europese Commissie het volgende opgemerkt:

“De meeste lidstaten die de richtlijn hebben omgezet, gaan, in overeenstemming met hun nationale wetgeving, verder in het toestaan van toegang tot en gebruik van bewaarde gegevens dan de richtlijn zelf, bijvoorbeeld voor het voorkomen en bestrijden van criminaliteit in het algemeen en van gevaar voor lijf en leden. Hoewel dit is toegestaan uit hoofde van de e-privacyrichtlijn, blijft de mate van harmonisatie die met EU-wetgeving tot stand is gekomen op dit gebied beperkt. Verschillen in het doel van de gegevensbewaring hebben gevolgen voor het aantal en de frequentie van de verzoeken en dus ook voor de kosten die moeten worden gemaakt voor het nakomen van de verplichtingen die voortvloeien uit de richtlijn. Bovendien biedt deze situatie wellicht in onvoldoende mate de voorspelbaarheid die vereist is bij elke wetgevende maatregel die het recht op privacy beperkt¹¹. De Commissie zal nagaan of en hoe verdere harmonisatie op dit vlak moet worden verwezenlijkt^{12,13}.”

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

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

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

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

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

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

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

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

BIJZONDERE OPMERKINGEN

INDIENINGSBESLUIT

Het indieningsbesluit moet worden gesteld als volgt:

“ALBERT II, Koning der Belgen,

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

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

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

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

DISPOSITIEF

Nieuw artikel 1

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

“Art. 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet”.¹⁵

De andere artikelen moeten dienovereenkomstig worden hernoemd.

¹⁴ *Beginnelsen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbevelingen 226 en 227, formule F 5

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

Artikel 3

(dat artikel 4 wordt)

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

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

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

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

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

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

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

De ontworpen tekst moet dienovereenkomstig worden aangevuld.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[...]

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

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

De voorliggende bepaling moet dienovereenkomstig worden gewijzigd.

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

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

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

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

De ontworpen tekst moet dienovereenkomstig worden aangevuld, inclusief de toevoeging van het begrip “oproepeling zonder resultaat”¹⁶ aan de definities in artikel 2 van het voorontwerp van wet.

LE GREFFIER – DE GRIFFIER

LE PRÉSIDENT – DE VOORZITTER

Colette GIGOT

Pierre LIÉNARDY

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