



CONSEIL D'ÉTAT
section de législation

RAAD VAN STATE
afdeling Wetgeving

avis 58.449/4
du 7 décembre 2015

advies 58.449/4
van 7 december 2015

sur

over

un avant-projet de loi
'relative à la conservation
des données dans le secteur
des communications
électroniques'

een voorontwerp van wet
'betreffende de bewaring van
gegevens in de
elektronische-communicatiesector'

Le 6 novembre 2015, le Conseil d'État, section de législation, a été invité par le Ministre de la Justice à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'relative à la conservation des données dans le secteur des communications électroniques'.

L'avant-projet a été examiné par la quatrième chambre le 7 décembre 2015. La chambre était composée de Pierre LIÉNARDY, président de chambre, Martine BAGUET et Bernard BLERO, conseillers d'État, Sébastien VAN DROOGHENBROECK et Jacques ENGLEBERT, assesseurs, 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 et Martine BAGUET.

L'avis, dont le texte suit, a été donné le 7 décembre 2015.

*

Op 6 november 2015 is de Raad van State, afdeling Wetgeving, door de Minister van Justitie verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'betreffende de bewaring van gegevens in de elektronische-communicatiesector'.

Het voorontwerp is door de vierde kamer onderzocht op 7 december 2015. De kamer was samengesteld uit Pierre LIÉNARDY, kamervoorzitter, Martine BAGUET en Bernard BLERO, staatsraden, Sébastien VAN DROOGHENBROECK en Jacques ENGLEBERT, assessoren, 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 en Martine BAGUET.

Het advies, waarvan de tekst hierna volgt, is gegeven op 7 december 2015.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2^o, des lois coordonnées sur le Conseil d'État, 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.

OBSERVATIONS GÉNÉRALES

I. PORTÉE DE L'AVANT-PROJET, DROIT ET JURISPRUDENCE EUROPÉENS, JURISPRUDENCE INTERNE

1. Par un arrêt du 8 avril 2014, rendu en grande chambre en réponse aux questions préjudicielles de la Haute Cour d'Irlande et de la Cour constitutionnelle d'Autriche (C.J.U.E., C-293/12, Digital Rights Ireland Ltd et C-594/12, Kärntner Landesregierung e.a.), la Cour de justice de l'Union européenne a invalidé 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).

Cet arrêt est motivé et décide comme suit :

« Sur l'existence d'une ingérence dans les droits consacrés par les articles 7 et 8 de la Charte

[...]

34. [...] l'obligation imposée par les articles 3 et 6 de la directive 2006/24 aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte.

35. En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A n° 116, § 48 ; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte.

36. De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel.

37. Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En

outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.

Sur la justification de l'ingérence dans les droits garantis par les articles 7 et 8 de la Charte

38. Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

39. En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte, il convient de constater que, même si la conservation des données imposée par la directive 2006/24 constitue une ingérence particulièrement grave dans ces droits, elle n'est pas de nature à porter atteinte audit contenu étant donné que, ainsi qu'il découle de son article 1^{er}, paragraphe 2, cette directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

40. Cette conservation des données n'est pas non plus de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, en raison du fait que la directive 2006/24 prévoit, à son article 7, une règle relative à la protection et à la sécurité des données selon laquelle, sans préjudice des dispositions adoptées en application des directives 95/46 et 2002/58, certains principes de protection et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, principes selon lesquels les États membres veillent à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données.

41. Quant à la question de savoir si ladite ingérence répond à un objectif d'intérêt général, il convient de relever que, si la directive 2006/24 est destinée à harmoniser les dispositions des États membres relatives aux obligations desdits fournisseurs en matière de conservation de certaines données qui sont générées ou traitées par ces derniers, l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1^{er}, paragraphe 1, à 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. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique.

42. Il ressort de la jurisprudence de la Cour que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales (voir, en ce sens, arrêts Kadi et Al Barakaat International Foundation/Conseil et Commission, C-402/05 P et C-415/05 P, EU:C:2008:461, point 363, ainsi que Al-Aqsa/Conseil, C-539/10 P et C-550/10 P, EU:C:2012:711, point 130). Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (voir, en ce sens, arrêt Tsakouridis, C-145/09, EU:C:2010:708, points 46 et 47). Par ailleurs, il convient de relever, à cet égard, que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté.

43. À cet égard, il ressort du considérant 7 de la directive 2006/24 que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, le Conseil 'Justice et affaires intérieures' du 19 décembre 2002 a considéré que les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée.

44. Force est donc de constater que la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24, répond effectivement à un objectif d'intérêt général.

45. Dans ces conditions, il y a lieu de vérifier la proportionnalité de l'ingérence constatée.

46. À cet égard, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs (voir, en ce sens, arrêts *Afton Chemical*, C-343/09, EU:C:2010:419, point 45 ; *Volker und Markus Schecke et Eifert*, EU:C:2010:662, point 74 ; *Nelson e.a.*, C-581/10 et C-629/10, EU:C:2012:657, point 71 ; *Sky Österreich*, C-283/11, EU:C:2013:28, point 50, ainsi que *Schaible*, C-101/12, EU:C:2013:661, point 29).

47. En ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêt *Cour EDH, S et Marper c. Royaume-Uni* [GC], n^{os} 30562/04 et 30566/04, § 102, CEDH 2008-V).

48. En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

49. En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive.

50. Cette appréciation ne saurait être remise en cause par la circonstance, invoquée notamment par MM. Tschohl et Seitlinger ainsi que par le gouvernement portugais dans leurs observations écrites soumises à la Cour, qu'il existe plusieurs modalités de communications électroniques qui ne relèvent pas du champ d'application de la directive 2006/24 ou qui permettent une communication anonyme. Si, certes, cette circonstance est de nature à limiter l'aptitude de la mesure de conservation des données à atteindre l'objectif poursuivi, elle n'est toutefois pas de nature à rendre cette mesure inapte, ainsi que l'a relevé M. l'avocat général au point 137 de ses conclusions.

51. En ce qui concerne le caractère nécessaire de la conservation des données imposée par la directive 2006/24, il convient de constater que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte.

52. S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

53. À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci.

54. Ainsi, la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, *Liberty et autres c. Royaume-Uni*, n° 58243/00, § 62 et 63, du 1^{er} juillet 2008 ; *Rotaru c. Roumanie*, précité, § 57 à 59, ainsi que *S et Marper c. Royaume-Uni*, précité, § 99).

55. La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, *S et Marper c. Royaume-Uni*, précité, § 103, ainsi que *M. K. c. France*, n° 19522/09, § 35, du 18 avril 2013).

56. Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

57. À cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves.

58. En effet, d'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans

toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

59. D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.

60. En deuxième lieu, à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1^{er}, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

61. En outre, quant à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci, mais il se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité.

62. En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles limitations.

63. En troisième lieu, s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

64. Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit

être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

65. Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

66. De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles.

67. L'article 7 de la directive 2006/24, lu en combinaison avec les articles 4, paragraphe 1, de la directive 2002/58 et 17, paragraphe 1, second alinéa, de la directive 95/46, ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.

68. En second lieu, il convient d'ajouter que ladite directive n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir, en ce sens, arrêt Commission/Autriche, C-614/10, EU:C:2012:631, point 37).

69. Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte ».

2. À la suite de cet arrêt de la Cour de justice, l'arrêt 84/2015 du 11 juin 2015 de la Cour constitutionnelle a annulé 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', laquelle avait pour objet d'assurer la transposition partielle de la directive 2006/24/CE.

L'arrêt de la Cour constitutionnelle repose sur la motivation suivante :

« B.10.1. Comme la Cour de justice l'a relevé aux points 56 et 57 de son arrêt, la directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet, couvrant de manière généralisée toute personne et tous les moyens de communication électronique sans distinction en fonction de l'objectif de lutte contre les infractions graves que le législateur de l'Union entendait poursuivre.

La loi attaquée ne se distingue nullement de la directive sur ce point. En effet, ainsi qu'il est dit en B.8, les catégories de données qui doivent être conservées sont identiques à celles énumérées par la directive tandis qu'aucune distinction n'est opérée quant aux personnes concernées ou aux règles particulières à prévoir en fonction de l'objectif de lutte contre les infractions décrites à l'article 126, § 2, de la loi du 13 juin 2005 remplacé par la loi attaquée. Tout comme la Cour de justice l'a constaté à propos de la directive (point 58), la loi s'applique donc également à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel.

B.10.2. Pas plus que ce n'est le cas pour la directive, l'article 5 attaqué ne requiert-il une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Il ne limite pas non plus la conservation des données afférentes à une période temporelle ou à une zone géographique déterminée ou encore à un cercle de personnes susceptibles d'être mêlées à une infraction visée par la loi, ou qui pourraient contribuer par la conservation des données, à prévenir, détecter ou poursuivre ces infractions.

B.10.3. Si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l'article 126, § 5, 3^o, de la loi du 13 juin 2005, remplacé par l'article 5 de la loi attaquée, aucune condition matérielle ou procédurale n'est définie par la loi quant à cet accès.

B.10.4. Enfin, en ce qui concerne la durée de conservation des données, la loi n'opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

B.11. Par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive 'conservation des données' invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52.1 de la Charte des droits fondamentaux de l'Union européenne.

Partant, l'article 5 précité viole les articles 10 et 11 de la Constitution lus en combinaison avec ces dispositions. Le moyen unique dans l'affaire n° 5856 et le premier moyen dans l'affaire n° 5859 sont fondés.

B.12. En raison de leur caractère indissociable avec l'article 5, il y a lieu d'annuler également les articles 1^{er} à 4, 6 et 7 de la loi du 30 juillet 2013 attaquée et donc l'intégralité de ladite loi ».

L'avant-projet à l'examen se donne pour objet de faire suite à cet arrêt 84/2015 de la Cour constitutionnelle du 11 juin 2015, lequel fait lui-même suite à l'arrêt de la Cour de justice du 8 avril 2014.

3. Au regard du droit européen, il y a lieu d'observer que l'arrêt de la Cour de justice de l'union européenne qui se prononce sur une question en appréciation en validité du droit dérivé de l'Union, et conclut à l'invalidité d'une norme européenne, n'a pas pour effet de faire disparaître de l'ordre juridique la norme invalidée, ni de faire revivre les normes éventuellement abrogées par le dispositif invalidé.

Il n'en reste pas moins que l'ensemble des juridictions nationales sont liées par le constat d'invalidité¹, que les autorités de l'Union ont, elles, l'obligation de modifier ou d'abroger l'acte invalidé et que les autorités nationales ont celle de modifier ou d'abroger les règles nationales qui ont été adoptées en suite de l'acte invalidé en respectant les procédures nationales².

Par conséquent, dès lors qu'est invalidée la directive 2006/24/CE, qui avait pour objet d'harmoniser les différentes législations des États membres relatives à la conservation des données en matière de communications électroniques et, même si cette directive n'a pas encore été abrogée ou modifiée par les autorités compétentes de l'Union européenne, il n'y a pas lieu d'y avoir égard mais seul le droit applicable avant son entrée en vigueur doit être pris en considération.

À ce propos, il faut tenir compte 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), tel qu'il était en vigueur avant sa modification par la directive 2006/24/CE³.

¹ À charge éventuellement pour celles-ci d'interroger à nouveau la Cour si des doutes subsistent sur la portée exacte de l'invalidité.

² Voir, sur ces questions, « *Contentieux de l'Union européenne. Renvoi préjudiciel, recours en manquement/3* », sous la direction de C. SOULARD, A. RIGAUX, D. SIMON et R. MUNOZ, Paris, éditions Lamy, Wolters-Kluwer France, 2011 pp. 108 et s.

³ Sur la question de savoir si le droit de l'Union européenne et plus spécialement la Charte des droits fondamentaux est d'application pour les mesures prises par les États membres en matière de conservation de métadonnées dans un but de sécurité publique, la défense et la sûreté de l'État, il faut avoir égard aux articles 72 et 73 du Traité sur le fonctionnement de l'Union européenne, dispositions figurant sous le Titre V de la troisième partie du Traité, relatif à l'espace de liberté, de sécurité et de justice; l'article 72 dispose que « [l]e présent titre ne porte pas atteinte à l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure », tandis que l'article 73 prévoit qu'« [i]l est loisible aux États membres d'organiser entre eux et sous leur responsabilité des formes de coopération et de coordination qu'ils jugent appropriées entre les services compétents de leurs administrations chargées d'assurer la sécurité nationale ». Toutefois, comme le relève le Conseil d'État de France, le droit dérivé de l'Union s'avère parfois plus complexe sur cette question. Ainsi, s'agissant de l'article 15 de la directive 2002/58/CE, le Conseil d'État de France, dans un document intitulé « Les rapports du Conseil d'État – Le numérique et les droits fondamentaux » a exposé ce qui suit : « [...] tant la directive n° 95/46/CE que la directive n° 2002/58/CE excluent de leur champ la matière pénale et les traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'État. Et l'existence de ces actes, mettant en œuvre le droit de l'Union, est une condition d'application de la Charte. La directive n° 2002/58/CE est cependant ambiguë à cet égard : si son article 1.3 restreint son champ d'application, son article 15.1 dispose que les États ne peuvent déroger aux droits garantis par la directive pour les finalités énumérées ci-dessus que s'il s'agit de mesures nécessaires et proportionnées, prises dans le respect des « principes généraux du droit communautaire ». Il traite en particulier de la conservation des données, en prévoyant que « les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié » par l'une des finalités énumérées ci-dessus. Il est donc possible de soutenir que la directive n° 2002/58/CE régit les législations des

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.

1^{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 réponse⁴.

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

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

4. Concernant le droit interne, comme le souligne l'exposé des motifs relatif à l'avant-projet à l'examen, dès lors que les dispositions de la loi du 30 juillet 2013 ont été

États relatives à la conservation des métadonnées. Les usages des métadonnées en matière de sécurité nationale échappent au champ d'application du droit de l'Union, mais la conservation porte atteinte par elle-même, indépendamment de l'usage, aux droits garantis par la directive, puisque l'article 5 impose en principe l'effacement des données. En outre, si la proposition de directive relative à la protection des données personnelles en matière pénale était adoptée, les traitements de données personnelles à des fins de police judiciaire entreraient pleinement dans le champ du droit de l'Union européenne. Dès lors, en raison de l'ambiguïté du champ d'application de la directive n° 2002/58/CE, la question de la conformité de la législation nationale à la Charte des droits fondamentaux de l'Union européenne, telle qu'elle a été interprétée par la C.J.U.E. dans l'arrêt *Digital Rights Ireland*, reste posée », <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>, pp. 199-200.

⁴ Paragraphe inséré par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 'modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs'.

annulées, elles sont censées ne jamais avoir existé et les dispositions abrogées par cette loi redeviennent applicables.

Plus spécialement, à la suite de l'annulation de la loi du 30 juillet 2013, l'article 126 de la loi du 13 juin 2005 'relative aux communications électroniques'⁵, est d'application tel qu'il était en vigueur avant l'entrée en vigueur de la loi du 30 juillet 2013, qui 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 ».

L'exposé des motifs relatif au texte en projet mentionne à ce propos que l'article 126 reproduit ci-avant n'est pas « satisfaisant ».

5. Dans ce contexte, l'auteur de l'avant-projet entend dès lors adopter un dispositif qui n'a plus pour objet de transposer la directive invalidée par la Cour de Justice, mais bien plutôt de mettre en place un système de conservation des données qui permettraient d'atteindre les objectifs dont la Cour de justice et la Cour constitutionnelle ont reconnu le caractère légitime, tout en se conformant aux décisions de ces hautes juridictions, dans leur dispositif et leur motivation.

Il convient en outre de relever que comme l'article 126 en vigueur, ainsi que l'article 126 annulé par l'arrêt 84/2015 de la Cour constitutionnelle, le dispositif en projet impose la conservation de données dans des buts qui dépassent 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, les données dont la conservation est imposée seront communiquées aux autorités habilitées, à des fins déterminées, fins parmi lesquelles figurent notamment l'identification des personnes ayant fait appel à un service d'urgence, en vue de permettre l'intervention du service concerné dans un délai utile, la recherche de personnes dont la disparition est inquiétante et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité

⁵ Ci-après « la loi du 13 juin 2005 ».

physique de la personne disparue se trouve en danger imminent, ou encore, l'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques⁶.

Ainsi en va-t-il aussi des finalités reprises au texte en projet, qui concernent la prévention et la répression de la criminalité en général, les risques pour la vie humaine ou l'intégrité physique des personnes et des biens, ou encore les utilisations non autorisées du système de communications électroniques, qui s'inscrivent dans les finalités énumérées à l'article 15 de la directive 2002/58/CE.

II. MISE EN ŒUVRE, PAR LE TEXTE EN PROJET, DES EXIGENCES DÉCOULANT DES ARRÊTS DE LA COUR DE JUSTICE ET DE LA COUR CONSTITUTIONNELLE

1. À la lecture de l'arrêt de la Cour de justice, dans le prolongement duquel est intervenu l'arrêt de la Cour constitutionnelle, il y a lieu de retenir essentiellement ce qui suit :

1° La conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24/CE, constitue une ingérence dans le droit fondamental au respect de la vie privée et les autres droits consacrés à l'article 7 et à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, aggravée par la circonstance que les autorités pourront prendre connaissance de ces données.

2° Cette ingérence n'est toutefois pas de nature à porter atteinte au contenu essentiel de ces droits, étant donné que, ainsi qu'il découle de son article 1^{er}, paragraphe 2, cette directive 2006/24/CE ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

3° Cette ingérence répond par ailleurs à un objectif d'intérêt général, étant la lutte contre le terrorisme international, la lutte contre la criminalité grave afin de garantir la sécurité publique et le droit de toute personne à la sûreté, et la conservation des données concernées peut être considérée comme apte à réaliser l'objectif poursuivi par cette directive 2006/24/CE.

4° La question se pose dès lors de savoir si l'ingérence prévue est proportionnée au but poursuivi, à savoir si elle comprend les mesures strictement nécessaires pour atteindre ce but ; à ce propos, la réglementation en cause « doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données ».

Sur ce point, il faut avoir égard aux éléments suivants.

1° Au fait que la réglementation couvre de manière généralisée toute personne et tous les moyens de communications électroniques ainsi que l'ensemble des données relatives au

⁶ Article 126, § 2, en projet.

trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves ; ainsi,

a) d'une part, la réglementation n'impose pas que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales et elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel ;

b) d'autre part, la réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.

2° Au fait que, à cette absence générale de limites, s'ajoute la circonstance que la réglementation « ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence » ; à cet égard, la réglementation « ne contient pas les conditions matérielles et procédurales y afférentes » et « ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci » ; spécialement, il n'est prévu « aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi » et « l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales ».

3° Au fait que s'agissant de la durée de conservation des données, la conservation des données pendant une période d'au moins six mois est prévue « sans que soit opérée une quelconque distinction entre les catégories de données [...] en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées » ; « [c]ette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire ».

Il en résulte que, selon la Cour de justice, l'on ne peut considérer que l'« ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire ».

En outre,

4° Il n'est pas prévu de « règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité » ; plus spécialement, il n'est pas imposé aux fournisseurs « un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles » : en particulier, rien ne garantit la « destruction irrémédiable des données au terme de la durée de conservation de celles-ci ».

5° Rien n'impose que les données en cause soient conservées sur le territoire de l'Union, de sorte « qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents ».

2. Comme exposé ci-avant, si l'avant-projet à l'examen, dans les finalités qu'il poursuit, est plus large que la directive 2006/24/UE invalidée par la Cour de Justice, il n'apparaît pas que les buts poursuivis par le texte en projet ne seraient pas tous et chacun légitimes, et notamment qu'ils ne pourraient pas être poursuivis conformément à l'article 15, paragraphe 1^{er}, de la directive 2002/58/CE.

L'avant-projet de loi doit donc être examiné en tenant compte de la circonstance que les exigences qui résultent de l'arrêt de la Cour de justice concernant la conservation et l'accès subséquent à des données, telles que visées par la directive 2006/24/UE, à savoir la conservation et l'accès à des données « en vue de garantir la disponibilité [de celles-ci] à des fins de recherche, de détection et de poursuite d'infractions graves » : la portée de l'arrêt de la Cour et des conséquences à en tirer, aussi rigoureuses soient-elles, sont donc limitées à une conservation de données dont la finalité est, en sa phase ultime, la sanction pénale, par hypothèse, nécessairement non anodine, de comportements et d'actes constitutifs d'infractions graves.

Rien ne permet, *a priori*, d'étendre la portée de cet arrêt à une conservation ou à un accès à des données conservées qui auraient d'autres finalités comme la recherche, par un service de médiation, de l'auteur d'appels malveillants, l'identification de l'appelant ou du lieu d'un appel aux services d'urgence, en vue de permettre à ceux-ci d'intervenir afin de pouvoir garantir la sauvegarde des biens et des personnes, ou la recherche, indépendante de tout contexte infractionnel, d'une personne dont la disparition est inquiétante et dont il apparaît que la vie pourrait être en danger imminent, ni même aux activités des services de renseignements.

Ces dernières hypothèses ne seront donc examinées qu'au regard du droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par l'article 22 de la Constitution ⁷.

⁷ Voir e.a., L. TASSONE, « La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme » in « Enjeux européens et mondiaux de la protection des données personnelles », ouvrage collectif sous la direction d'A. GROSJEAN, Larcier, coll. Création Information Communication, p. 53 et s., et les références citées ; concernant les services de renseignement et de sécurité, voir e.a. l'avis 42.178/2 donné le 19 février 2007 sur un

3. Compte tenu du contexte ainsi rappelé, le texte en projet appelle les observations générales suivantes.

3.1. Quant au fait que le texte en projet couvre de manière généralisée toute personne, sans distinction entre personnes, période temporelle et zone géographique, et sans qu'une relation soit requise entre les données dont la conservation est prévue et une menace pour la sécurité publique

3.1.1. À cet égard, l'exposé des motifs mentionne ce qui suit :

« Le besoin d'identifier le titulaire d'un numéro de gsm ou d'une adresse IP est devenu un aspect routinier des enquêtes et une étape indispensable de celles-ci. L'accès à l'historique des communications ou la localisation *a posteriori* du suspect ou de la victime sont des mesures plus attentatoires à la vie privée et moins utilisées que l'identification mais sont néanmoins très souvent indispensables dans certains types d'affaires.

Le contenu des communications n'est pas visé par le projet de loi.

Le secteur du terrorisme est évidemment particulièrement d'actualité. L'accès aux données de communication est une étape incontournable pour identifier les personnes et les liens entre celles-ci. Lorsqu'une perquisition mène à la découverte d'un sac entier de cartes SIM ou la saisie d'un ordinateur portable, il s'ensuit un grand nombre d'actes d'enquêtes pour retracer les communications passées à partir de ces éléments puis à partir d'autres éléments ainsi identifiés, etc. Ce type de mesures sera aussi indispensable lorsqu'une personne qui n'était pas encore connue des services de police ou de renseignement s'avère avoir rejoint les rangs d'une organisation terroriste en Syrie par exemple. Enfin, l'enquête après un attentat impose évidemment de revenir en arrière dans les communications du suspect pour notamment vérifier s'il a agi seul ou identifier des complices.

L'autre secteur très souvent mentionné pour illustrer l'importance de ces données est celui de la pédopornographie. Ici aussi, il faut pouvoir remonter dans le temps à partir de la détection d'un élément sur Internet pour pouvoir mettre à jour l'ensemble du réseau criminel.

Mais ces exemples particulièrement parlants ne doivent pas laisser penser que les données sont nécessaires uniquement pour lutter contre des phénomènes de criminalité certes choquants mais relativement limités en nombre. La réalité est que les données de communications sont nécessaires dans une grande variété de situations mais où on imagine aisément que ces données sont souvent la fois le point de départ et une étape de l'enquête, par exemple :

- la réaction à une disparition inquiétante ;
- le trafic de stupéfiants ;
- la vente par Internet de médicaments contrefaits ;
- les incitations à la haine ou à la violence ;
- le harcèlement, y compris chez les jeunes ;
- l'espionnage qui peut s'étaler sur plusieurs années de même que le recrutement et où le hacking à des fins d'espionnage peut être découvert plusieurs mois après qu'il ait eu lieu ;

- le piratage de comptes bancaires ;
- le vol d'identité ;
- le hacking associé par exemple au chantage de la divulgation des données personnelles ou commerciales collectées ;
- etc.

Il faut ajouter à cela un facteur majeur qui influence l'élément temporel et le besoin de revenir dans le passé. Ce facteur est celui de la localisation des fournisseurs de service par Internet et le fait que certains de ces services basés à l'étranger exigent le passage par la coopération judiciaire formelle pour transmettre des données. Or le passage par la coopération judiciaire, notamment avec les États-Unis est un processus très lourd et très lent. La Belgique tente d'améliorer la situation mais n'a évidemment pas toutes les cartes en main. Cet élément doit donc être pris en compte.

Cette situation fait qu'il faudra souvent plusieurs mois pour obtenir d'un fournisseur de services par Internet l'adresse IP à partir de laquelle un message par exemple a été posté. Ce n'est qu'à partir de ce moment que les enquêteurs belges peuvent demander l'accès aux données d'identification sur base de l'adresse IP en question.

L'accès aux données de communication est donc indispensable tout comme la possibilité de pouvoir remonter dans le passé pour une certaine période. Cela dépend forcément de la durée de conservation des données.

[...]

L'argumentaire de la Cour constitutionnelle est très bref et renvoie surtout à la décision de la Cour de justice UE concernant la directive 2006/24/CE.

La Cour conclut que l'article 126 LCE attaqué, comme la directive, constitue une limitation disproportionnée du droit au respect de la vie privée. Cette violation du principe de proportionnalité découle de la combinaison de quatre éléments :

- le fait que la conservation des données concerne toutes les personnes ;
- l'absence de différenciation en fonction des catégories de données conservées et leur utilité ;
- l'absence ou l'insuffisance de règles quant à l'accès des autorités aux données concernées ;
- et enfin, bien que cet élément soit soulevé seulement par la Cour de justice et pas par la Cour constitutionnelle, l'absence ou la faiblesse des règles sur la sécurisation des données chez les fournisseurs ou les opérateurs.

Ces éléments, et les réponses que le projet de loi y apporte, sont passés en revue ci-dessous.

[...] La distinction en fonction des personnes, périodes temporelles et zones géographiques

Le premier des trois éléments dont la combinaison viole le principe de proportionnalité concerne le principe même de l'obligation de conservation des données. C'est le fait de conserver les données de toutes les personnes de manière indifférenciée. Après analyse approfondie, il ressort qu'il n'est pas possible d'opérer une différenciation a priori de cet élément.

Dans l'avis 33-2015 [relatif au texte en projet], la Commission [de la protection de la vie privée] va dans le même sens puisqu'elle indique que 'certains aspects des arrêts [de la Cour de justice et de la Cour constitutionnelle] lui paraissent difficilement applicables,

en particulier la distinction en fonction des personnes, périodes temporelles et/ou zones géographiques’.

a) Toutes les personnes même si elles ne sont pas encore impliquées dans une enquête.

Limiter la conservation des données à celles concernant des personnes qui font déjà l’objet d’une enquête pénale ou de renseignement n’a pas de sens car cette possibilité existe déjà par ailleurs. Les autorités judiciaires comme les services de renseignement peuvent déjà imposer le ‘repérage’ des communications dans le cadre d’une enquête précise et donc obliger les opérateurs et fournisseurs d’accès à conserver les données pour le futur une fois qu’on a identifié la personne ou un service de communication dans une enquête pénale. L’objectif de l’article 126 LCE est de s’assurer qu’un certain nombre de données existeront aussi pour une période limitée du passé. L’article 126 n’a donc de sens que s’il porte sur les personnes qui ne font pas encore nécessairement l’objet d’une enquête pénale ou de renseignement.

Cette dimension est indispensable comme le montrent les exemples repris au point 2.

Il faut par ailleurs rappeler que la mesure peut tout aussi bien bénéficier à la victime pour ses propres données (dans des affaires de harcèlement par exemple, il s’agira de retourner dans le passé des données de la victime pour identifier l’origine d’un appel, un email ou un sms) que l’accusé (les données de localisation peuvent montrer que l’accusé n’était pas sur le lieu de l’infraction au moment où elle a été commise). Il peut aussi s’agir d’identifier des témoins ce qui peut jouer à charge comme à décharge.

b) Pas de différenciation en fonction de la période temporelle, la zone géographique ou un cercle de personnes

La Cour constitutionnelle, renvoyant à l’arrêt de la Cour de justice, note que l’article 126 attaqué ‘ne limite pas non plus la conservation des données afférentes à une période temporelle ou à une zone géographique déterminée ou encore à un cercle de personnes susceptibles d’être mêlées à une infraction visée par la loi, ou qui pourraient contribuer par la conservation des données, à prévenir, détecter ou poursuivre ces infractions’.

Cette partie de l’arrêt de la Cour de justice a suscité beaucoup d’interrogations quant à sa portée. Le groupe de travail qui a préparé le présent projet de loi s’est lui aussi interrogé sur la possibilité de limiter l’impact de l’article 126 en travaillant sur les critères soulevés par la Cour de justice, c’est-à-dire une ‘période temporelle’, ‘une zone géographique déterminée’ ou encore ‘un cercle de personnes’.

La conclusion est que cette partie de l’arrêt de la Cour de justice doit être lue comme une explication de la sensibilité du principe de conservation généralisée des données. Mais il n’est pas possible d’y puiser une solution pour appliquer une différenciation.

La référence à la ‘période temporelle’ pourrait par exemple viser une situation spécifique et temporaire de menace pour l’ordre ou la sécurité publique. Mais, d’une part, ce type de critère n’est pas cohérent avec un grand nombre de situations et de types de criminalité pour lesquels la conservation des données s’avère décisive (par exemple en matière de pédopornographie) et, d’autre part, la où il pourrait trouver à s’appliquer, ce type de critère négligerait le fait que la situation en question ne peut pas forcément être anticipée (par exemple en cas de menace terroriste matérialisée par un attentat). Quant à la référence à une ‘zone géographique’ ou un ‘cercle de personnes’, une activation de

l'article 126 LCE sur base de ce type de critère s'apparenterait à du profilage avec les risques de discrimination qui en découlent.

c) Pas d'exclusion de certaines professions

La Cour constitutionnelle note enfin, toujours concernant cette absence de différenciation entre les personnes dont les données sont conservées, que 'la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel'.

Ici aussi, on s'est interrogé sur la possibilité de créer une différenciation pour faire suite à cette partie de l'arrêt. Il s'agirait d'exclure a priori certaines personnes, en fonction de leur profession, de la conservation des données.

Cette différenciation n'est pas possible. D'une part, s'il est vrai que certaines professions sont protégées en matière de collecte de la preuve ou de renseignement, cette protection n'est jamais absolue. D'autre part, il faut ici encore noter que la conservation des données ne peut pas être vue comme une mesure visant un accès a posteriori aux données nécessairement 'contre' la personne. La donnée en question peut servir à disculper celle-ci ou encore être utile lorsque la personne en question est victime d'une infraction. Rappelons à nouveau que la conservation des données ne concerne pas le contenu des communications.

On verra toutefois plus loin que la protection de certaines professions est bien renforcée dans le présent projet de loi mais au niveau de la réglementation de l'accès aux données conservées.

On peut conclure qu'il n'est pas possible de modaliser l'article 126 LCE sur base du premier élément (l'absence de différenciation en fonction des personnes) repris par la Cour constitutionnelle et la Cour de justice. Tous les pays européens contactés sont arrivés à la même conclusion.

Ni l'arrêt de la Cour constitutionnelle ni celui de la Cour de justice UE ne concluent toutefois qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant l'élément essentiel de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle auraient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments.

Dans son avis précité sur le présent projet de loi, la Commission vie privée soutient cette interprétation et indique : « comme indiqué dans l'Exposé des Motifs, aucun des deux arrêts ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects ».

Il faut donc combiner les différents éléments soulevés par la Cour de justice UE et la Cour constitutionnelle. Puisque le principe de la conservation généralisée (c'est-à-dire sans différenciation entre les personnes) des données de communication constitue en soi une limitation très importante du droit au respect de la vie privée, il faut 'compenser' cet élément par un régime plus strict sur les autres aspects ».

3.1.2. Concernant l'impossibilité – constatée également par la Commission pour la protection de la vie privée dans son avis sur le texte en projet – de limiter la conservation des données à certaines personnes, ou à certains groupes de personnes, notamment celles qui feraient déjà l'objet d'une enquête, la section de législation n'aperçoit pas les raisons qui seraient susceptibles de remettre en question les justifications données dans l'exposé des motifs. Ainsi, si

aucune obligation de conservation n'était imposée de manière générale aux opérateurs et fournisseurs, le système qui en résulterait impliquerait que seuls une conservation et un accès aux données *a posteriori* seraient possibles, sans que l'autorité puisse avoir accès aux données passées (ou *a priori*), qui sont pourtant nécessaires, voire indispensables, à la réalisation des objectifs légitimes prévus par le texte en projet.

De même, concernant une éventuelle limitation de l'obligation de conservation à une zone géographique ou à une période temporelle déterminée, la section de législation n'aperçoit pas les raisons qui seraient susceptibles de remettre en question le raisonnement figurant dans l'exposé des motifs. Quant à ces deux dernières limitations, la question se pose toutefois de savoir s'il ne serait pas envisageable, sans nuire aux objectifs légitimes poursuivis, de définir un délai général de conservation plus restreint, tout en mettant en place un système dans lequel moyennant certaines garanties procédurales⁸, le Roi pourrait être habilité, dans des circonstances objectives de menace potentielle spécifique à définir avec précision, à étendre le délai de conservation des données (le législateur fixant toutefois une limite à cette extension de délai), tout en définissant, le cas échéant, compte tenu de la nature ou de l'étendue de la menace, une zone géographique déterminée.

Enfin, s'agissant de la limitation à certaines professions dont l'exercice fait l'objet d'un secret professionnel, outre les éléments mentionnés dans l'exposé des motifs, l'on ne peut exclure que les titulaires de ces professions utilisent le même service de communications électroniques pour des communications tant privées ou, de manière générale, non couvertes par le secret professionnel, que pour des communications couvertes par le secret professionnel. Compte tenu de cette possibilité, l'essentiel est donc non pas de limiter la conservation des données mais d'éviter qu'elles soient divulguées dans des conditions qui, pour celles couvertes par le secret professionnel, ne seraient pas conformes aux principes en la matière.

3.1.3. Si l'on comprend la logique des raisons pour lesquelles l'auteur de l'avant-projet se déclare dans l'impossibilité de donner suite à la lecture la plus stricte des exigences ici visées, il reste que, par hypothèse, le texte en projet envisage de ne pas répondre à ces exigences, ce qui en fragilise le dispositif.

Cette fragilité est toutefois fonction de la portée qu'il convient de conférer aux arrêts concernés, et surtout, à celui de la Cour de justice.

⁸ Par exemple, un arrêté délibéré en Conseil des ministres, soumis préalablement à l'avis de la Commission pour la protection de la vie privée et à celui de l'Institut.

Concernant ce dernier, le Conseil d'État de France a relevé ce qui suit :

« L'arrêt *Digital Rights Ireland*, dont la Cour n'a pas différé les effets, soulève deux questions : celle de la possibilité de continuer à appliquer les législations nationales sur la conservation des données et celle du cadre qui devrait être défini pour se substituer à la directive n° 2006/24/CE. Les deux questions procèdent en réalité d'une même interrogation sur l'interprétation de l'arrêt. De manière schématique, deux lectures peuvent en être faites : celle d'une condamnation de l'insuffisance des garanties prévues par la directive ; celle d'une condamnation de tout système de conservation générale des métadonnées, quel qu'il soit.

[...]

La première interprétation de cet arrêt peut se fonder sur le fait que la Cour a fait masse de trois éléments pour juger que le principe de proportionnalité était méconnu, et que le second avait trait à l'absence de toute précision sur les conditions d'accès des États aux métadonnées conservées par les opérateurs.

Selon cette interprétation, si la directive avait fixé des garanties concernant l'accès, l'appréciation de la Cour aurait peut-être été différente. Elle aurait également pu être influencée par l'existence de restrictions concernant la conservation, par exemple une durée maximale plus courte que celle de deux ans fixée par la directive. Les conclusions de l'avocat général peuvent conforter une telle interprétation. L'avocat général déplore le fait que la directive n'ait défini ni la nature des infractions pouvant justifier l'accès aux métadonnées, ni les autorités pouvant obtenir cet accès, ni les garanties relatives à l'effacement des données par les autorités après leur utilisation et à l'information des personnes concernées (§ 125 à 129 des conclusions). Il relevait aussi qu'il y avait une différence entre une durée de conservation se mesurant en mois et une durée se mesurant en années (§ 148). Cependant, si la Cour est parvenue à la même solution que l'avocat général, la construction de son raisonnement est assez différente, et il n'est donc pas évident que les conclusions permettent d'éclairer la portée de l'arrêt sur la condamnation du système de conservation en tant que tel.

La seconde interprétation se fonde en premier lieu sur ce que deux des trois éléments pris en compte par la Cour pour juger que le principe de proportionnalité est méconnu tiennent au caractère général et indiscriminé de la conservation : dans le premier élément, la Cour critique le fait que les métadonnées de tous les utilisateurs des communications soient collectées, indépendamment de l'existence d'un soupçon quant à la participation à une infraction grave; dans le troisième élément, c'est le fait que la durée de conservation soit fixée de manière indiscriminée qui est contesté. C'est donc le caractère systématique et uniformément durable de la conservation des métadonnées qui est en cause. En second lieu, l'arrêt qualifie sévèrement la conservation systématique des métadonnées, en y voyant une 'ingérence particulièrement grave' dans les droits garantis par les articles 7 et 8 de la Charte, l'absence d'information des intéressés étant en outre 'susceptible de générer dans l'esprit des personnes concernées (...) le sentiment que leur vie privée fait l'objet d'une surveillance constante'. Si la Cour admet que la conservation préventive des données poursuit un but d'intérêt général, elle juge que l'ingérence ne peut être admise que si elle est proportionnée.

À l'issue de son contrôle de proportionnalité, elle conclut que la directive 'comporte une ingérence dans des droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire' (§ 65). On peut donc en déduire que l'ingérence résultant d'un

système de conservation systématique peut difficilement être considérée comme limitée au strict nécessaire »⁹.

Cette difficulté de conférer une portée certaine à l'arrêt de la Cour de justice et la circonstance qu'une des interprétations possibles de cet arrêt amène à mettre à mal le principe même de l'obligation de conservation des données *a priori*, ont été par ailleurs mises en exergue par la doctrine, en ces termes :

« [...] il est difficile de voir quelle garantie pourrait être prévue pour répondre à ce défaut de l'instrument sans changer fondamentalement le principe même de la conservation *a priori* contenu dans la directive. Cette partie du raisonnement de la Cour laisse donc perplexe : d'un côté, la Cour semble insister sur le fait que l'important est d'apporter des garanties compensatoires mais en même temps une des 'garanties' à apporter remet en cause le principe même contenu dans la directive.

La Cour ne facilite donc pas l'intervention du législateur européen¹⁰ pour 'réparer' la directive 2006/24/CE : faut-il changer complètement d'approche voire abroger purement et simplement la directive (mais alors pourquoi la Cour ne l'a-t-elle pas clairement exprimé) ou cette critique adressée à la directive rend-elle seulement les autres garanties évoquées par la Cour d'autant plus importantes ?

Ces questions rendent le sort du dossier très incertain »¹¹.

3.1.4. L'auteur de l'avant-projet a retenu la première des deux interprétations mentionnées ci-avant, tout en s'efforçant, dans ce cadre, de renforcer par rapport à la loi annulée¹² les exigences et conditions attachées au système mis en place en termes de garantie de la confidentialité et de la sécurisation de la conservation des données, de procédure et de délai d'accès aux données, de finalité d'accès et d'autorités habilitées à accéder aux données ainsi qu'en termes de destruction des données une fois le délai de conservation expiré, et ce tout en envisageant des mesures de protection particulières pour les données en relation avec l'exercice de certaines professions soumises au secret professionnel¹³.

⁹ « *Les rapports du Conseil d'État – Le numérique et les droits fondamentaux* », source : <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>, pp. 198 à 201.

¹⁰ À ce jour, la Commission européenne n'a pris d'initiative officielle relative à l'abrogation ou la modification de la directive 2006/24/CE.

¹¹ S. DE BIOLLEY et A. WEYEMBERGH, « Chronique de jurisprudence consacrée à l'espace de liberté, de sécurité et de justice II – Jurisprudence de la Cour de justice relative à la coopération policière et judiciaire en matière pénale (2009-2014) » in *Cahiers de droit européen*, 50^e année (2014), n° 2, pp. 430 à 434. Voir également, P.-Y. DETHY, note sous C.J.U.E, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd* et C-594/12, *Kärntner Landesregierung e.a.*, « *Quelques réflexions sur l'arrêt C-293/12 et C-594/12* », in *Revue du droit des industries de réseau*, 2014/3, pp. 338 à 349.

¹² L'auteur de l'avant-projet se situe ainsi dans la ligne des recommandations du Conseil d'État de France, qui expose : « L'arrêt de la C.J.U.E. soulève la question de la conformité au droit de l'Union européenne des législations nationales, telles que la législation française, qui prévoient une telle obligation de conservation générale des données de connexion. Compte tenu des enjeux de la surveillance des communications pour la protection de la sécurité nationale, l'étude du Conseil d'État ne propose pas de supprimer cette obligation mais préconise de renforcer les garanties concernant l'accès et l'utilisation de ces données. » (« *Les rapports du Conseil d'État – Le numérique et les droits fondamentaux* », source : <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>, p. 20).

¹³ Les observations qui suivent examinent chacune des mesures envisagées pour assurer ce renforcement des garanties ; elles indiquent les aspects pour lesquels ces mesures pourraient ne pas être qualifiées de suffisantes au regard de la jurisprudence de la Cour de justice et de la Cour constitutionnelle et proposent des améliorations, là où

À l'appui de cette interprétation plus souple, l'on peut essentiellement retenir que dans son arrêt, la Cour de justice n'a pas condamné expressément le principe de la conservation *a priori* des données constatant que celui-ci ne portait pas atteinte au contenu essentiel des libertés fondamentales en cause et qu'il répond à un objectif d'intérêt général, à savoir la protection de la sécurité publique ¹⁴.

La condamnation de la conservation *a priori* des données elle-même, fut-elle opérée de manière indifférenciée quant aux modes de communication visés et aux circonstances et personnes concernées, ne ressort pas davantage de la jurisprudence ultérieure de la Cour de Justice. L'arrêt *Schrems* du 6 octobre 2015 ¹⁵ laisse en ce sens apparaître que la contrariété au droit de l'Union ne survient que lorsque cette conservation généralisée est couplée à l'absence de critère objectif encadrant l'accès des autorités aux données ainsi conservées et leur utilisation :

« Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données [voir en ce sens, en ce qui concerne 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 (JO L 105, p. 54), arrêt *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU:C:2014:238, points 57 à 61] ».

Enfin, la section de législation estime que, entre deux interprétations possibles des arrêts de la Cour de Justice et de la Cour constitutionnelle ainsi que des normes appliquées par l'une et l'autre, il y a lieu de retenir celle qui permet de concilier au mieux les impératifs contradictoires du droit au respect de la vie privée des personnes faisant usage des moyens de communications électroniques, d'un côté, et de la protection due aux droits des personnes menacées par les agissements criminels d'autrui, d'un autre côté. La section de législation rappelle en ce sens que l'article 2 de la Convention européenne des droits de l'Homme met à charge des autorités l'obligation de protéger la vie des personnes contre de tels agissements ¹⁶, notamment lorsqu'ils prennent la forme du terrorisme ¹⁷. Quant à l'article 8 du même instrument, il impose entre autres que l'intégrité sexuelle des enfants soit adéquatement protégée dans les rapports en particulier et que les atteintes portées à cette intégrité donnent lieu à une répression pénale effective, sans que l'anonymat garanti aux utilisateurs de l'internet ne puisse y faire obstacle. Statuant à propos de la protection due à un enfant victime d'une annonce à caractère

cela s'avère possible et, bien évidemment, dans les limites du contrôle de légalité effectué en vertu de la loi par la section de législation.

¹⁴ Voir les paragraphes 39, 42 et 44 de l'arrêt C.J.U.E., n° C-293/12, 8 avril 2014 (*Digital Rights Ireland Ltd*).

¹⁵ Voir C.J.U.E., n° C-362/14, 6 octobre 2015 (*Maximillian Schrems c. Data Protection commissioner*), pt. 93.

¹⁶ Voir Cour eur. D.H., arrêt *Van Colle c. Royaume-Uni*, 13 novembre 2012.

¹⁷ Voir Cour eur. D.H., déc. *Finogenov and Others v. Russia*, 18 mars 2010, req. n° 18299/03.

sexuel publiée à son nom sur un site de rencontre, un arrêt *K.U. c. Finlande* du 2 décembre 2008 énonce ce qui suit (§ 49) :

« Une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier et poursuivre l'auteur, c'est-à-dire la personne qui avait passé l'annonce. Or pareilles mesures n'ont pas été prises. La prépondérance ayant été accordée à l'exigence de confidentialité, il n'a jamais été possible de procéder à une enquête efficace. Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Sans préjudice de la question de savoir si, compte tenu de sa nature répréhensible, la conduite de la personne ayant passé l'annonce illégale sur Internet relève ou non de la protection des articles 8 et 10, le législateur aurait dû en tout cas prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte ».

Il reste que la question de la portée effective de l'arrêt C-293/12, *Digital Rights Ireland Ltd* ne pourra trouver une réponse que dans la jurisprudence future de la Cour de justice, lorsqu'elle sera appelée, comme c'est déjà le cas¹⁸, à se prononcer sur les législations des différents États membres en la matière, spécialement au regard de l'article 15, paragraphe 1^{er}, de la directive 2002/58/CE, et des articles 7, 8 et 52, de la Charte des droits fondamentaux de l'Union européenne.

3.2. Quant à la question de savoir si le texte en projet fixe des critères objectifs pour délimiter l'accès des autorités compétentes aux données et leur utilisation conformes aux objectifs poursuivis, en termes notamment de procédure

3.2.1. Dans un premier temps, il convient de rappeler que la directive 2006/24/CE ne comportait aucune disposition régissant directement l'accès aux données par les autorités des États membres. Ainsi, en son article 4, elle se bornait à prévoir que

« Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées

¹⁸ Voir à ce propos la demande de décision préjudicielle présentée par la Kamarrätten i Stockholm (Suède) le 4 mai 2015 — *Tele2 Sverige AB/Post- och telestyrelsen* (Affaire C-203/15) (*Journal officiel* 2015/C 221/06), dans laquelle la juridiction suédoise pose les questions préjudicielles suivantes :

« 1) Une obligation générale de conservation de données, relative à toute personne et à tous les moyens de communication électronique et portant sur l'ensemble des données relatives au trafic, sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre la criminalité [telle que décrite dans la décision de renvoi], est-elle compatible avec l'article 15, paragraphe 1, de la directive 2002/58 (1) compte tenu des articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne ?

2) S'il est répondu par la négative à la première question, une telle obligation de conservation peut-elle néanmoins être admise :

a) si l'accès par les autorités nationales aux données conservées est encadré de la manière précisée [dans la décision de renvoi], et

b) si les exigences de protection et de sécurité des données sont régies de la manière précisée [dans la décision de renvoi], et que

c) toutes les données en question doivent être conservées pendant six mois à compter du jour de l'achèvement de la communication avant d'être effacées, comme il l'est exposé [dans la décision de renvoi] ? ».

dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme ».

Quant à la loi du 30 juillet 2013 annulée par la Cour constitutionnelle, elle énumérait seulement les finalités de la conservation, sans déterminer précisément les autorités habilitées à demander l'accès aux données conservées, ni la procédure à suivre. L'article 126, § 2, de la loi du 13 juin 2005, tel qu'inséré par la loi du 30 juillet 2013 prévoyait en effet que :

« § 2. Les données visées au paragraphe 1^{er}, alinéa 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.

Les fournisseurs de services et de réseaux visés au paragraphe 1^{er}, alinéa 1^{er}, font en sorte que les données reprises au paragraphe 1^{er}, alinéa 1^{er}, soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières »¹⁹.

3.2.2. Le texte en projet entend déterminer les autorités ou instances habilitées à demander l'accès aux données conservées, ainsi que les finalités de cet accès et, selon la finalité et le demandeur d'accès, la période temporelle du passé pour laquelle ces autorités ou instances peuvent demander l'accès. Dans certains cas, comme les hypothèses de l'appel à un service d'urgence ou l'identification de l'auteur d'un appel malveillant, le texte en projet fixe également des délais dans lesquels les demandes doivent être adressées à l'opérateur ou au fournisseur à dater d'un fait déterminé.

3.2.2.1. En ce qui concerne les finalités qui consistent à intervenir en vue de faire suite à un appel aux services d'urgence ou à rechercher une personne disparue dont l'intégrité physique

¹⁹ La loi annulée prévoyait également en l'article 126, § 5, 3^o, qu'elle insérerait dans la loi du 13 juin 2005 que les fournisseurs concernés devaient « garanti[r] que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et par les agents et préposés de ces fournisseurs spécifiquement autorisés par ladite Cellule ». Contrairement à ce que pourrait laisser penser l'arrêt de la Cour constitutionnelle (B.10.3), étaient ainsi visées non pas les « autorités » compétentes habilitées à accéder aux données conservées, mais les membres du personnel de l'opérateur ou du fournisseur concerné, autorisés à avoir accès aux données en vue de les transmettre à l'autorité, cette disposition étant destinée à assurer la transposition non pas de l'article 4 de la directive 2006/24/CE, mais de l'article 7, c) de celle-ci.

est en danger imminent, l'ingérence dans l'exercice de libertés fondamentales apparaît moins importante que dans le cadre d'une intervention du pouvoir judiciaire ou des services de renseignements et de sécurité, en vue, selon le cas, de la prévention et de la répression d'infractions ou de la collecte secrète d'informations. Il en va de même lorsque l'accès est demandé par un officier de police judiciaire de l'Institut en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et 126 en projet, de la loi du 13 juin 2005, dès lors que la finalité est alors précisément de garantir le respect des dispositions considérées par les opérateurs et fournisseurs et par conséquent, de garantir le respect des droits fondamentaux des utilisateurs.

Concernant les procédures régissant les demandes d'accès précités, et auxquels l'enseignement de l'arrêt de la Cour de justice n'a pas vocation, *a priori*, à s'appliquer pour les raisons évoquées plus haut, il n'apparaît pas disproportionné de ne pas prévoir l'intervention préalable d'une juridiction ou d'une autorité administrative présentant des garanties d'autonomie et d'indépendance par rapport au demandeur d'accès.

Il reste toutefois que les garanties procédurales prévues par le texte en projet ne s'avèrent pas suffisantes. Il est, sur ce point, renvoyé aux observations particulières ci-après, relatives à l'article 3 de l'avant-projet (article 126 en projet).

3.2.2.2. En ce qui concerne la demande émanant du Service de médiation pour les télécommunications, même si, selon le texte en projet, une telle demande ne peut porter que sur les données d'identification, elle peut être considérée comme entraînant une atteinte plus importante aux droits et libertés de l'appelant dont l'identification est demandée dès lors que l'article 43bis, § 3, alinéa 1^{er}, 7^o, de la loi du 21 mars 1991 'portant réforme de certaines entreprises publiques économiques' confie au service de médiation la mission d'examiner la demande de « toute personne se prétendant victime d'une utilisation malveillante d'un réseau ou d'un service de communications électroniques visant à obtenir communication de l'identité et l'adresse des utilisateurs de réseaux ou de services de communications électroniques l'ayant importunée, pour autant que ces données sont disponibles »²⁰.

L'accès aux données qui serait ainsi octroyé au service de médiation doit, dans ce contexte, être entouré de garanties spécifiques. Il est également renvoyé aux observations particulières relatives à l'article 3 de l'avant-projet (article 126 en projet).

²⁰ Il convient de souligner que le fait que la demande émanant du service de médiation puisse avoir pour effet d'aboutir à la communication de l'identité et de l'adresse de l'appelant à un particulier, et non à une autorité, découle de l'article 43bis précité, disposition dont la modification n'est pas envisagée par l'auteur de l'avant-projet, et qui participe, avec d'autres dispositions législatives contenues dans la loi du 13 juin 2005 à la transposition de l'article 10 de la directive 2002/58/CE, lequel prévoit notamment que :

« Les États membres veillent à ce que des procédures transparentes régissent les modalités grâce auxquelles le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessible au public peut passer outre [...] à la suppression de la présentation de l'identification de la ligne appelante, à titre temporaire, lorsqu'un abonné demande l'identification d'appels malveillants ou dérangeants; dans ce cas, conformément au droit interne, les données permettant d'identifier l'abonné appelant seront conservées et mises à disposition par le fournisseur d'un réseau public de communications et/ou d'un service de communications électroniques accessible au public ; ».

3.2.2.3. S'agissant de l'hypothèse où la demande émane des autorités judiciaires en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle, ces articles organisent une procédure précise concernant les demandes d'accès, en termes de données auxquelles il peut être accédé, de motivation de la décision, de proportionnalité de l'accès au regard du respect de la vie privée et de subsidiarité par rapport à d'autres devoirs d'enquête, de conditions d'accès et de secret professionnel, garanties qu'en ses articles 8 et 9, l'avant-projet envisage de renforcer, notamment en limitant le délai d'accès aux données conservées.

Au regard de l'enseignement des arrêts de la Cour de justice et de la Cour constitutionnelle, l'auteur de l'avant-projet doit veiller à mieux justifier le caractère de gravité des infractions pour lesquelles l'accès est demandé. Sur ce point, il convient que l'auteur de l'avant-projet vérifie s'il ne conviendrait pas, compte tenu bien évidemment des finalités à respecter, d'établir une liste plus restreinte des infractions pour lesquelles l'accès est autorisé, en énumérant plus précisément celles-ci, à l'instar de l'article 90*ter* du Code d'instruction criminelle ²¹.

Pour le surplus, il est renvoyé aux observations particulières sous les articles 8 et 9 de l'avant-projet.

3.3. Quant au fait que le texte en projet porte généralement sur tous les moyens de communications électroniques ainsi que l'ensemble des données relatives au trafic et quant au fait que le texte en projet ne fixe pas une durée de conservation en opérant une distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées

3.3.1. Se pose ici la question de la proportionnalité tout d'abord, d'une obligation générale de conserver toutes les données relatives au trafic pour tous les moyens de communications électroniques, et d'autre part, de l'absence de fixation de délais de conservation différents selon les catégories de données en fonction de leur utilité.

Tant l'arrêt de la Cour de Justice que celui de la Cour constitutionnelle ont, avant tout autre élément, relevé que la directive 2006/24/CE ou la loi belge concernait, de manière très générale, toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet.

Interrogé sur la situation en matière de conservation de données dans d'autres États membres de l'Union européenne, situation dont l'exposé des motifs fait état et sur laquelle il entend s'appuyer, le délégué du ministre a communiqué à la section de législation des informations dont il ressort que certains États membres, certes minoritaires, ont prévu ou envisagent d'adopter des traitements différenciés, en termes d'obligation et de durée de conservation, selon la nature des données : ainsi, en Allemagne, le délai de conservation en projet

²¹ Si une telle liste peut être établie, elle pourra s'avérer plus large que celle qui figure à l'article 90*ter*, dès lors que ce dernier concerne une ingérence plus importante dans la vie privée et la protection des données puisqu'il permet au juge d'instruction d'accéder au contenu des communications et télécommunications privées, d'en prendre connaissance et de les enregistrer : cette disposition autorise donc un accès au contenu, ce qui n'est pas le cas des articles 46*bis* et 88*bis* du Code d'instruction criminelle ni des articles 126 et 126/1 en projet de la loi du 13 juin 2005.

varierait selon qu'il s'agit de données de trafic ou de données de localisation, un délai plus bref étant prévu pour ces dernières, étant entendu que les données relatives aux e-mails seraient exclues de l'obligation de conservation ; quant aux Pays-Bas, la législation en projet prévoirait un délai de conservation de douze mois pour les données relatives à la téléphonie, et de six mois, pour les données relatives à l'Internet.

Sur ces questions, l'exposé des motifs mentionne ce qui suit :

« Le présent projet de loi introduit une distinction sur base de 3 catégories de données.

La première catégorie concerne les données d'identification (qui est titulaire de tel numéro de gsm, quel est le numéro de gsm de telle personne, qui se trouve derrière telle adresse IP, ...). Ces données sont les plus demandées et sont modérément attentatoires à la vie privée, par rapport notamment aux deuxième et troisième catégories.

La deuxième catégorie concerne les données de connexion et localisation (quel est notamment le lieu et la durée d'une communication).

La troisième catégorie concerne les données personnelles de communications (qui a appelé ou correspondu avec qui).

Les deuxième et troisième catégories sont plus attentatoires à la vie privée que la première. Les accès à ces données sont moins nombreux que ceux aux données d'identification mais restent fréquents.

Après de nombreuses discussions au sein du gouvernement et avec les services et autorités concernées, et après avoir envisagé une différenciation entre les délais de conservation en fonction des catégories de données, la conclusion est que, vu les nécessités liées à la lutte contre les infractions terroristes, une période de 12 mois de conservation est nécessaire pour chacune des 3 catégories ».

3.3.2. Restreindre la généralité des données à conserver, ou adapter le délai de conservation des données, selon les catégories de données, participerait sans doute d'un système de garanties plus importantes, en vue d'assurer la proportionnalité des mesures envisagées dans l'ingérence qu'elles constituent dans le droit au respect de la vie privée.

Aussi, si tant est que l'on retienne une lecture stricte des exigences rappelées ci-avant, le choix opéré par l'auteur de l'avant-projet pourrait apparaître comme fragilisant le système en projet.

Toutefois, il convient de constater qu'au regard des différentes finalités poursuivies, notamment la lutte contre le terrorisme et la pédopornographie, l'intervention faisant suite à un appel urgent, ou la recherche de personnes disparues dont la vie est estimée en danger imminent, la section de législation n'aperçoit pas, effectivement, comment ces finalités, toutes légitimes, pourraient être efficacement atteintes en imposant, par exemple, de conserver les seules données de téléphonie, et non les données internet, ou en prévoyant des délais de conservation différents pour certaines catégories de données. Par ailleurs, la mise en place d'un système dans lequel une différence de traitement est opérée en termes d'obligation même de conservation et de durée de celle-ci, selon la finalité ou les personnes concernées, se heurte au demeurant aux mêmes obstacles que ceux évoqués à l'observation 3.1. ci-avant.

En outre, en vue d'assurer la proportionnalité des mesures envisagées, le texte en projet prévoit des accès différenciés en termes de données auxquelles l'accès est autorisé, et de délai d'accès, selon la finalité même de l'accès ou l'autorité qui demande l'accès. Ainsi, à titre d'exemple, les services d'urgence n'auront accès qu'aux données d'identification de l'appelant ²², l'accès dans le cadre d'une recherche de personne disparue ne pourra porter que sur les données relatives à cette personne ²³, et le procureur du Roi accède à des données moins étendues que le juge d'instruction ²⁴. Quant au délai d'accès, celui-ci varie de vingt-quatre heures à douze mois, le délai de douze mois étant prévu lorsqu'une autorité judiciaire ou des services de renseignement et de sécurité agissent, pour la première dans le cadre de son action relative à une infraction visée au titre *Iter* du livre II du Code pénal (à savoir les infractions terroristes), et pour les seconds, de menace terroriste ou extrémiste au sens de la loi du 30 novembre 1998 'organique des services de renseignement et de sécurité'.

Le système en projet opère donc une différence de traitement selon la finalité de l'accès et le demandeur d'accès, de nature à tendre vers une plus grande proportionnalité du système au regard du droit au respect de la vie privée.

3.4. Quant au fait que le texte en projet comprenne des règles spécifiques et adaptées destinées à garantir la pleine intégrité et confidentialité des données ainsi que leur destruction irréversible au terme de leur durée de conservation, ce par un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles

3.4.1. L'auteur de l'avant-projet a été particulièrement attentif à cette dimension, étant entendu qu'une garantie accrue de la pleine intégrité des données et de la confidentialité de celles-ci serait, selon lui, de nature à compenser la circonstance que le texte en projet est dans l'impossibilité de faire suite à la première exigence formulée par la Cour de justice, à savoir, la non-généralité en termes de données et de personnes, ainsi que de zone géographique et de période temporelle.

Les mesures contenues par le texte en projet (articles 126 et 126/1 en projet), ainsi que, le cas échéant, par d'autres législations ou réglementations en vigueur peuvent être résumées comme suit.

1° Il convient d'appliquer au premier chef la législation et la réglementation générales en matière de protection des données à caractère personnel et de traitement de celles-ci. Sur ce point, il est prévu que chaque opérateur et chaque fournisseur concerné est considéré comme responsable du traitement au sens de la loi du 8 décembre 1992 'relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel' pour les données traitées sur la base des articles 126 et 126/1 en projet ²⁵.

²² Article 126, § 2, alinéa 1^{er}, 4^o, en projet.

²³ Article 126, § 2, alinéa 1^{er}, 5^o, en projet.

²⁴ Comparez les articles 46*bis* et 88*bis* du Code d'instruction criminelle.

²⁵ Article 126/1, § 2, alinéa 2, en projet.

2° Au sein de chaque opérateur ou fournisseur concerné est en principe créée une Cellule de coordination ²⁶, chargée de fournir aux autorités belges légalement habilitées, à leur demande, les données conservées ; l'accès aux données est réservé aux membres de la Cellule ²⁷, lesquels doivent, chacun, avoir fait l'objet d'un avis de sécurité positif et non périmé ²⁸ conformément à l'article 22quinquies de la loi du 11 décembre 1998 'relative à la classification et aux habilitations, attestations et avis de sécurité' ²⁹ et ne pas avoir fait l'objet d'un refus du Ministre de la Justice, refus qui doit être motivé et peut intervenir en tout temps ³⁰ ; les membres de la Cellule peuvent, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur ou du fournisseur, étant entendu que tant les membres de la cellule que les préposés qui leur apportent un soutien technique sont soumis au secret professionnel ³¹ ; les opérateurs et fournisseurs doivent veiller à la confidentialité des données traitées par la Cellule et informer tant l'IBPT que la Commission pour la protection de la vie privée des coordonnées de la Cellule et de ses membres, ainsi que des modifications de ces données ³² ; en outre, de nouvelles incriminations ³³ sont prévues pour assurer l'effectivité de cette confidentialité (avec le secret professionnel par ailleurs imposé), incriminations qui couvrent des hypothèses non encore couvertes par l'article 550bis du Code pénal, lequel sanctionne pénalement les hackings interne et externe ; s'agissant de la procédure, les opérateurs et fournisseurs sont tenus d'établir une procédure interne de réponse aux demandes d'accès des autorités aux données à caractère personnel des utilisateurs, et les informations relatives à ces procédures, au nombre de demandes reçues, à la base juridique invoquée et à la réponse, sont mises à la disposition de l'IBPT à sa demande ³⁴ ; de surcroît, les opérateurs de réseaux publics et les fournisseurs concernés respectent l'article 114, § 2, de la loi du 13 juin 2005 pour l'accès aux données visées et leur transmission aux autorités ³⁵. Il est également prévu que chaque fournisseur et opérateur concerné doit désigner un ou plusieurs préposés à la protection des données à

²⁶ Les opérateurs et les fournisseurs ont la possibilité de créer une Cellule commune, laquelle doit prévoir, dans ce cas, le même service pour chaque opérateur ou fournisseur individuel (article 126/1, § 1^{er}, alinéa 2, en projet).

²⁷ Article 126, § 4, 3°, en projet.

²⁸ L'avis est considéré comme périmé cinq ans après son octroi.

²⁹ Article 126/1, § 1^{er}, alinéa 3, 1°, en projet.

³⁰ Article 126/1, § 1^{er}, alinéa 3, 2°, en projet.

³¹ Article 126/1, § 1^{er}, alinéas 5 et 6, en projet.

³² Article 126/1, § 1^{er}, alinéa 7, en projet.

³³ Article 145, § 3ter, en projet.

³⁴ Article 126/1, § 2, alinéa 1^{er}, en projet.

³⁵ Article 126/1, § 2, alinéa 3, en projet. L'article 114, § 2, de la loi du 13 juin 2005 dispose comme suit :
« Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les mesures prévues au paragraphe 1^{er} que prennent les entreprises fournissant des services de communications électroniques accessibles au public, lorsqu'elles concernent des données à caractère personnel, visent pour le moins à :

- garantir que seules des personnes habilitées à agir à des fins légalement autorisées puissent avoir accès aux données à caractère personnel ;
- protéger les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites ; et
- assurer la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

L'Institut est habilité à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre ».

caractère personnel, qui sont tenus de répondre aux mêmes conditions que les membres de la Cellule de coordination ; les préposés ne peuvent pas faire partie, en principe, de la Cellule, et leur indépendance est prévue et garantie notamment par le fait que l'exercice de leur mission ne peut entraîner de désavantages pour eux, qu'ils ne peuvent être licenciés ou remplacés à cause de l'exécution des tâches qui leurs sont confiées sans motivation approfondie, et qu'ils doivent avoir la possibilité de communiquer directement avec le management ou le comité de direction ; ces préposés ont pour mission de veiller à ce que les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi, à ce que le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver, à ce que seules les autorités légalement autorisées aient accès aux données conservées et à ce que les mesures de sécurité et de protection des données à caractère personnel décrites dans la loi et dans la politique de sécurité du fournisseur ou de l'opérateur soient mises en œuvre ; enfin, chaque fournisseur et opérateur concerné communique sans délai à l'Institut et à la Commission pour la protection de la vie privée les coordonnées du ou des préposés à la protection des données à caractère personnel, ainsi que toute modification de ces données ³⁶.

3° S'agissant des règles de nature plus technique, destinées à garantir la conservation, la confidentialité et la destruction des données au terme de leur délai de conservation, le texte en projet impose aux opérateurs et aux fournisseurs de garantir que les données conservées sont de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau, de veiller à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, de mettre en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, incompréhensibles et inexploitable par toute personne qui n'est pas autorisée à y avoir accès et de détruire les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé à l'article 126, § 3, en projet, sans préjudice des articles 122 et 123 de la loi du 13 juin 2005 ; enfin, ils sont tenus d'assurer une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données par une autorité habilitée à ce faire, cette traçabilité étant effectuée à l'aide d'un journal, que l'IBPT et la Commission pour la protection de la vie privée peuvent consulter ou dont ils peuvent exiger une copie en tout ou en partie ³⁷.

3.4.2. Des éléments qui précèdent, il ressort que le texte en projet met en place un système extrêmement précis et complet de nature à assurer en droit, et en fait, la pleine intégrité et la confidentialité des données ainsi que leur destruction irrémédiable au terme de leur durée de conservation, système se caractérisant « par un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles » ³⁸.

Toutefois, afin de répondre pleinement aux exigences qui résultent à ce titre de l'arrêt de la Cour de Justice, le texte en projet gagnerait à être revu sur quelques aspects.

³⁶ Article 126/1, § 3, en projet.

³⁷ Article 126, § 4, en projet.

³⁸ C.J.U.E., n° C-293/12, arrêt *Digital Rights Ireland Ltd*, pt 67.

3.4.2.1. Il résulte de l'article 126/1, § 1^{er}, alinéa 4, en projet, que le Roi est habilité par arrêté délibéré en Conseil des ministres, à dispenser certaines catégories d'opérateurs et fournisseurs des exigences imposées aux membres de la Cellule de coordination, relatives à l'avis de sécurité et à l'absence de refus du Ministre de la Justice, telles qu'elles sont prévues par l'alinéa 3 du même paragraphe, ou de fixer des conditions moins strictes pour ces catégories.

Le commentaire de l'article expose à ce sujet que

« Il est toutefois nécessaire de prendre en compte le fait que, en fonction de l'évolution des acteurs, le projet de loi peut s'appliquer à des fournisseurs ou opérateurs de petite taille pour lesquels certaines de ces vérifications deviennent disproportionnées. Le projet de loi prévoit donc la possibilité d'exonérer certaines catégories d'opérateurs ou de fournisseurs de ces obligations ou conditions ».

Par ailleurs, l'article 126/1, § 3, alinéa 2, permet au Roi, par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée, de déterminer des catégories de fournisseurs ou d'opérateurs pour lesquels le préposé à la protection des données à caractère personnel peut être membre de la Cellule de coordination³⁹.

Le commentaire de l'article mentionne à ce propos que

« Il est toutefois nécessaire de prendre en compte le fait que, en fonction de l'évolution des acteurs, le projet de loi peut s'appliquer à des fournisseurs ou opérateurs de petite taille pour lesquels cette incompatibilité, qui implique de désigner deux personnes différentes pour la Cellule de coordination et pour la fonction de préposé à la protection des données, devient disproportionnée. Le projet de loi prévoit donc la possibilité de créer une exception pour certaines catégories d'opérateurs ou de fournisseurs ».

Si l'on peut considérer comme légitime le but poursuivi par l'auteur de l'avant-projet, à savoir ne pas imposer d'obligations disproportionnées ou irréalisables aux opérateurs et fournisseurs disposant de peu de personnel, le système mis en place ne peut aboutir au fait de priver les personnes auxquelles les données conservées, sont relatives de certaines garanties que l'avant-projet leur donne en termes de protection d'un droit fondamental, celui du respect de la vie privée, pour la seule raison que l'opérateur ou le fournisseur qui conserve ces données serait « de petite taille ».

Le texte en projet sera revu de manière à prévoir des garanties équivalentes pour tous, quelle que soit la taille des opérateurs ou fournisseurs concernés et ce notamment par le biais, par exemple, de la possibilité déjà offerte par le texte en projet aux opérateurs de constituer une Cellule de coordination commune.

En tout état de cause, c'est au législateur qu'il appartient de fixer les critères à prendre en considération par le Roi pour mettre en œuvre son habilitation.

³⁹ À la première lecture, ces habilitations semblent être rappelées par l'article 126/1, § 4, 1^o et 4^o. Sur l'intention de l'auteur de l'avant-projet et les difficultés soulevées par le cumul ou la conjonction de l'ensemble de ces habilitations données au Roi, il est renvoyé aux observations particulières faites ci-après sous l'article 5 de l'avant-projet.

3.4.2.2. La destruction des données au terme du délai de conservation est imposée par l'article 126, § 4, 6°, en projet.

3.4.2.2.1. Toutefois, cette destruction s'effectue « sans préjudice des articles 122 et 123 ».

Le commentaire de l'article expose, à ce propos, qu'« en effet, on ne peut pas exclure qu'un fournisseur ou opérateur n'ait établi qu'une seule base de données dans le cadre des articles 122, 123 et 126. Dans ce cas, une donnée ne sera pas détruite en vertu de l'article 126 si elle peut être conservée sur base des articles 122 et 123 de la loi ».

Afin de limiter de manière maximale les risques de non-destruction des données concernées, la question se pose de savoir s'il ne serait pas adéquat de prévoir que les données conservées en vertu de l'article 126 en projet doivent l'être dans une base de données exclusivement consacrées à ces données.

3.4.2.2.2. Le dispositif en projet répondrait mieux aux exigences relatives à la destruction irrémédiable des données si une autorité, telle l'IBPT, était spécifiquement chargée de contrôler la destruction effective et irrémédiable des données.

Certes, l'IBPT est, de manière générale, chargé du contrôle du respect de l'ensemble de la loi du 13 juin 2005 en vertu de l'article 14, § 1^{er}, 3°, de la loi du 17 janvier 2003 'relative au statut du régulateur des secteurs des postes et des télécommunications belges' et le Roi peut conférer aux membres statutaires du personnel de l'Institut, la qualité d'officier de police judiciaire disposant de nombreux pouvoirs, conformément aux articles 24 et 25 de la même loi du 17 janvier 2003. Par ailleurs, l'article 126, § 2, alinéa 1^{er}, 3°, en projet permet à tout officier de police judiciaire de l'IBPT d'accéder aux données concernées en vue de la recherche, de l'instruction et de la poursuite d'infractions notamment à l'article 126 en projet.

Toutefois, la section de législation relève, à titre d'exemples, qu'il n'est prévu aucune incrimination pénale en matière de non-destruction des données au terme de leur délai de conservation. De même, aucune disposition n'impose à l'IBPT d'effectuer des contrôles réguliers et spécifiques en la matière. Or, de telles dispositions permettraient sans doute de mieux garantir l'effectivité de la destruction des données.

3.4.2.2.3. Le dispositif en projet sera réexaminé à la lumière de ces observations.

3.5. Quant au fait que le texte en projet impose la conservation des données en cause sur le territoire de l'Union

L'article 126, § 4, 4°, en projet prévoit que les fournisseurs et les opérateurs concernés « conservent les données sur le territoire de l'Union européenne ».

OBSERVATIONS PARTICULIÈRES

ARRÊTÉ DE PRÉSENTATION

L'arrêté de présentation sera rédigé comme suit :

« PHILIPPE, Roi des Belges,

À tous, présents et à venir, Salut.

Sur la proposition du Ministre de l'Agenda numérique, des Télécommunications et de la Poste, du Ministre de la Justice et du Ministre de la Défense,

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

Le Ministre de l'Agenda numérique, des Télécommunications et de la Poste, le Ministre de la Justice et le Ministre de la Défense 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 : »⁴⁰.

DISPOSITIF

Article 4

1. L'article 4 de l'avant-projet entend remplacer l'article 126 de la loi du 13 juin 2005.

Outre les observations générales ci-avant, cette disposition appelle les observations suivantes.

1.1. L'article 126, § 2, alinéa 1^{er}, en projet prévoit que les opérateurs et fournisseurs communiquent les données sur « simple demande » des autorités habilitées à avoir accès à ces données pour les finalités y énumérées et dans le délai qui leur est éventuellement imparti pour ce faire.

Le commentaire de l'article mentionne à ce propos que « cela ne signifie nullement que les conditions prévues par exemple par les articles 46bis et 88bis du Code d'instruction criminelle ne doivent pas être remplies. Cela signifie par contre que le fournisseur ou l'opérateur qui fournit des services de communication en Belgique doit apporter les données demandées par les autorités belges sur le territoire belge, sans que ces dernières ne doivent adresser une commission rogatoire ».

⁴⁰ *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.

1.2. Par ailleurs, s'agissant des demandes adressées par les services d'urgence en vertu de l'article 126, § 2, alinéa 1^{er}, 4^o, en projet, il est imposé au fournisseur ou à l'opérateur concerné d'« effectue[r] une vérification préalable de l'identité des services d'urgence ». Le commentaire de l'article s'en explique comme suit :

« [...] ce paragraphe oblige l'opérateur ou le fournisseur de convenir avec ces services d'urgence d'un mécanisme de sécurité afin d'éviter que des tiers, qui usurperaient l'identité des services d'urgence offrant de l'aide sur place, puissent obtenir illégalement des données conservées. Il va de soi que les services d'urgence offrant de l'aide sur place et les opérateurs doivent convenir ensemble de ces mécanismes de sécurité, chaque partie devant prendre ses responsabilités pour éviter une usurpation d'identité ».

Alors qu'aucune obligation similaire n'est imposée par le dispositif en projet en cas de demande émanant de la cellule de disparition de la police fédérale, le commentaire de l'article ajoute néanmoins à ce propos :

« Tout comme pour la collaboration avec les services d'urgence offrant de l'aide sur place, les opérateurs et la cellule de disparition de la police fédérale conviendront de modalités ou de procédures pratiques pour garantir que les opérateurs sont bien en contact avec l'officier compétent de la police judiciaire ».

2. Compte tenu des termes dans lesquelles elle est rédigée, et des explications ainsi données dans le commentaire de l'article, la disposition à l'examen appelle les observations suivantes.

Dans le cas où la demande trouve son fondement dans un acte d'une autorité judiciaire ou des services de renseignement, cet acte doit déjà, par définition, et en vertu du texte en projet ⁴¹, répondre aux conditions prévues selon le cas, aux articles 46*bis* ou 88*bis* du Code d'instruction criminelle, ou aux dispositions pertinentes de la loi du 30 novembre 1998.

Dans les autres cas, le texte en projet n'impose aucune exigence formelle, et le commentaire des articles expose, au surplus pour certaines hypothèses seulement ⁴², que les opérateurs et les fournisseurs d'une part, et les autorités qui demandent l'accès aux données, d'autre part, devront trouver les modalités et procédures pratiques permettant de s'assurer que la demande émane bien d'une autorité habilitée.

Une question aussi fondamentale dans la prévention des demandes irrégulières ou abusives, qui a pour objet d'éviter qu'une personne non habilitée puisse avoir accès aux données conservées, ne peut être laissée à l'appréciation des intervenants. Par ailleurs, il ne peut être prévu, sans autre précision, et alors que ceux-ci ne disposent pas de et ne peuvent se voir attribuer aucun pouvoir de police, que le fournisseur ou l'opérateur effectue une « vérification préalable de l'identité des services d'urgence », comme le texte en projet le mentionne.

⁴¹ Voir les mots « et dans les conditions fixées par ces articles », employés dans l'article 126, § 2, alinéa 1^{er}, 1^o et 2^o, en projet.

⁴² Le texte en projet est muet en ce qui concerne les demandes d'accès émanant du Service de médiation pour les télécommunications et ce, alors que la demande de ce Service fait suite à une plainte de « toute personne se prétendant victime d'une utilisation malveillante d'un réseau et d'un service », et, par conséquent, à la demande d'un particulier et non d'une autorité.

Dès lors, le texte en projet sera complété de sorte qu'en tout cas pour les hypothèses où cette garantie ne résulte pas déjà d'autres dispositions législatives, il habilite expressément le Roi à définir le contenu et la forme de la demande, de manière que, sur la base de celle-ci, les opérateurs et les fournisseurs puissent être assurés que celle-ci émane bien d'une autorité ou d'une personne habilitée à demander l'accès aux données, aux fins pour lesquelles et dans les conditions auxquelles l'article 126 en projet autorise cet accès.

En conséquence, à l'article 126, § 2, alinéa 1^{er}, 4°, en projet, la dernière phrase sera omise, et le commentaire de l'article sera revu. De même, l'habilitation conférée au Roi par l'article 126/1, § 4, 6°⁴³, en projet, sera utilement revue et complétée à la lumière de ces observations.

Article 5

Outre les observations générales ci-avant et sous réserve de celles-ci, la disposition à l'examen appelle les observations suivantes.

1. Comme mentionné ci-avant, l'article 126/1, § 1^{er}, alinéa 4, en projet, prévoit que

« Le Roi peut, par arrêté délibéré en Conseil des Ministres, décider que certaines catégories d'opérateurs ou fournisseurs ne sont pas soumises aux conditions visées au troisième alinéa⁴⁴ ou fixer pour ces catégories des conditions moins strictes ».

L'article 126/1, § 3, alinéa 2, en projet, qui a trait au « préposé à la protection des données à caractère personnel » prévoit quant à lui, que

« Ce préposé ne peut pas faire partie de la Cellule de coordination. Le Roi peut toutefois, par arrêté délibéré en Conseil des Ministres et après avis de la Commission pour la protection de la vie privée, déterminer les catégories de fournisseurs ou d'opérateurs pour lesquels cette incompatibilité n'est pas applicable ».

Pour sa part, l'article 126/1, § 4, en projet, prévoit, en ses 1° et 4°, que

« § 4. Le Roi détermine, par arrêté délibéré en Conseil des Ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut :

1° les catégories d'opérateurs et les catégories de fournisseurs visés à l'article 126, § 1^{er}, alinéa, 1^{er}, qui sont dispensés de certaines exigences fixées au paragraphe 1^{er} ;

[...]

4° les catégories de fournisseurs visés à l'article 126, § 1^{er}, alinéa 1^{er}, et les catégories d'opérateurs visés à l'article 126, § 1^{er}, alinéa 1^{er}, qui sont dispensés du respect du paragraphe 3, en tout ou en partie ; ».

Ces dispositions posent des difficultés pour les motifs suivants :

⁴³ Par cette disposition le Roi est habilité à déterminer « les autres règles régissant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1^{er}, alinéa 1^{er}, avec les autorités belges ou avec certaines d'entre elles, pour la fourniture des données visées au paragraphe 1^{er} ».

⁴⁴ À savoir l'obligation, pour les membres de la Cellule de coordination, de disposer d'un avis de sécurité positif non périmé et de ne pas avoir fait l'objet d'un refus du Ministre de la Justice.

Si les habilitations qui figurent au paragraphe 4, 1° et 4°, ont pour seul objet de rappeler celles qui figurent respectivement, au paragraphe 1^{er}, alinéa 4, et paragraphe 3, alinéa 2, alors :

1° d'une part, elles font double emploi avec celles-ci et sont inutiles ;

2° d'autre part et en tout état de cause, elles diffèrent des habilitations qu'elles sont censées rappeler ; ainsi :

– le paragraphe 4, exige, outre la délibération en Conseil des ministres requise par le paragraphe 1^{er}, alinéa 4, l'avis de la Commission pour la protection de la vie privée et celui de l'IBPT ;

– le paragraphe 4, 1°, est rédigé en des termes vagues en ce qu'il permet au Roi de déterminer les catégories d'opérateurs et de fournisseurs qui sont dispensées « de certaines exigences fixées au paragraphe 1^{er} », alors que le paragraphe 1^{er}, alinéa 4, permet au Roi, de manière plus précise, de déterminer les catégories qui « ne sont pas soumises aux conditions visées au troisième alinéa ou fixer pour ces catégories des conditions moins strictes » ;

– le paragraphe 4, 4°, habilite le Roi à déterminer les catégories d'intervenants « qui sont dispensés du respect du paragraphe 3, en tout ou en partie », tandis que la dispense éventuelle prévue au paragraphe 3, alinéa 2, porte uniquement sur l'obligation pour le préposé à la protection de données à caractère personnel de ne pas être membre de la Cellule de coordination.

Si les habilitations qui figurent au paragraphe 4, 1° et 4°, ont pour objet de conférer au Roi le pouvoir de prévoir d'autres dispenses ou dérogations que celles déjà prévues ⁴⁵, respectivement, au paragraphe 1^{er}, alinéa 4, et paragraphe 3, alinéa 2, alors il faut constater que ces habilitations ne précisent pas quels seront l'objet et les destinataires des dispenses considérées.

Quelle que soit l'intention de l'auteur de l'avant-projet, il lui appartient de lever les ambiguïtés ou contradictions ainsi relevées, de sorte que, sous réserve des observations générales ci-avant, ces habilitations portent sur des objets précis et clairement identifiables, en évitant tout double emploi entre les différentes habilitations envisagées. Par ailleurs, comme déjà observé, il appartient au législateur de déterminer les critères à mettre en œuvre par le Roi lorsqu'il fait usage de son habilitation, ainsi que les objets précis sur lesquelles elle porte, de manière à garantir le respect du principe d'égalité et du droit au respect de la vie privée des personnes dont les données sont conservées.

La disposition à l'examen sera revue en conséquence.

⁴⁵ Cette hypothèse n'est nullement à écarter puisque le commentaire de l'article mentionne « Le paragraphe 4 du nouvel article 126/1 prévoit une série de délégations au Roi. Les points 1° et 4° doivent permettre au Roi de prévoir des règles adaptées pour les opérateurs ou fournisseurs qui sont établis à l'étranger ou qui ne reçoivent que peu ou jamais de demandes des autorités en matière de données d'identification, de trafic ou de contenu ».

2. À l'article 126/1, § 3, alinéa 5, en projet, il convient de mieux préciser ce que l'on entend par « management ».

Article 8

1. La question se pose de savoir quelle est la portée exacte de la limitation de six mois prévue par l'article 46*bis*, § 1^{er}, alinéa 4, en projet, du Code d'instruction criminelle : le procureur du Roi est-il habilité à accéder aux données conservées pendant un délai restreint de six mois avant sa décision pour toutes les infractions sauf celles qui peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, infractions pour lesquelles le délai est étendu à douze mois⁴⁶, ou bien, plus probablement, compte tenu de l'article 88*bis*, § 1^{er}, alinéa 1^{er}, en projet, du Code d'instruction criminelle, faut-il comprendre cette disposition comme lui permettant l'accès à ces données uniquement dans le cadre d'infractions pouvant donner à lieu une peine d'emprisonnement correctionnel principal, étant entendu que lorsque la peine d'emprisonnement correctionnel principal atteint ou dépasse un an, le délai est étendu à douze mois ?

La disposition à l'examen sera revue de manière à lever toute ambiguïté à ce propos.

2. Par ailleurs, la section de législation s'interroge sur les motifs pour lesquels le texte en projet n'opère pas également la distinction prévue par l'article 88*bis*, § 2, en projet, du même code, dont il résulte des accès limités à 12 ou 9 mois, selon que la situation concerne une infraction « visée au Titre *I*ter du Livre II du Code pénal » ou bien que l'on se trouve dans une situation d'infraction autre visée à l'article 90*ter*, §§ 2 à 4 du même code, ou qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou qui est de nature à entraîner une peine d'emprisonnement correctionnel principal de cinq ans ou une peine plus lourde.

Selon les explications communiquées par le délégué du ministre, ces différences entre les deux dispositions en projet seraient dues essentiellement au fait que l'article 46*bis*, § 1^{er}, du Code d'instruction criminelle permet au procureur du Roi d'avoir accès uniquement aux données d'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques ou du moyen de communications électroniques utilisé, et d'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, tandis que l'article 88*bis* du même code permet au juge d'instruction d'avoir accès à des données plus larges et complètes puisque le juge d'instruction peut ordonner le repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, ainsi que la localisation de l'origine ou de la destination de télécommunications⁴⁷.

⁴⁶ Dès lors que le délai de conservation est précisément de douze mois.

⁴⁷ Le procureur du Roi ne peut ordonner des mesures similaires qu'en cas d'urgence et pour certaines infractions seulement, et cette mesure doit être confirmée dans les vingt-quatre heures par un juge d'instruction (article 88*bis* du Code d'instruction criminelle).

Si l'on peut effectivement admettre que les limitations de l'accès dans le temps prévues à l'article 88*bis*, § 2, en projet et celles prévues à l'article 46*bis*, § 1^{er}, alinéa 4, en projet, différent, compte tenu de l'objet même des données concernées, la différence de traitement opérée doit néanmoins tenir compte de deux éléments supplémentaires : tout d'abord, l'article 46*bis* concerne l'accès aux données par le ministère public, tandis que l'article 88*bis* concerne l'accès aux données par le juge d'instruction⁴⁸ ; ensuite, il résulte de l'article 126, § 3, en projet, que les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication sont conservées « pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service », avec pour conséquence que si l'accès du procureur du Roi aux données n'est pas limité dans le temps par le texte en projet, il pourrait s'en trouver *de facto* étendu à une période supérieure à douze mois, les données étant conservées dans un délai dont l'expiration ne prend cours qu'à dater du moment où une communication n'est pas possible à l'aide du service utilisé.

L'exposé des motifs doit dès lors mieux faire apparaître les justifications du fait que deux hypothèses de limitation d'accès dans le temps prévues à l'article 88*bis*, § 2, en projet, ne sont pas prévues par l'article 46*bis*, § 1^{er}, alinéa 4, en projet.

Article 9

1. Si, comme l'a précisé le délégué du ministre, dans l'énumération des infractions concernées, l'article 88*bis*, § 2, 2^e tiret, en projet, reproduit des dispositions existantes⁴⁹, il apparaît néanmoins qu'aux fins de refléter plus fidèlement l'intention de l'auteur de l'avant-projet, l'article 88*bis*, § 2, deuxième tiret, sera mieux rédigé comme suit :

« – Pour les autres infractions visées à l'article 90*ter*, §§ 2 à 4, ou qui n'étant pas visées à cette disposition, sont commises dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal ou sont de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde (la suite comme à l'avant-projet) ; ».

2. L'article 9 de l'avant-projet entend insérer un paragraphe 3 nouveau dans l'article 88*bis* du Code d'instruction criminelle, qui tend à limiter les pouvoirs conférés par cet article au juge d'instruction lorsque sont concernés les moyens de communication, paragraphe libellé comme suit :

« § 3. La mesure ne pourra porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées au paragraphe 1^{er} ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées au paragraphes 1^{er}, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront

⁴⁸ Ce qui justifie d'ailleurs que les données auxquelles l'autorité concernée a accès diffèrent d'une disposition à l'autre.

⁴⁹ À savoir l'article 46*quinqies* et l'article 89*ter* du Code d'instruction criminelle.

informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne seront pas consignés au procès-verbal ».

Quant à l'article 12 de l'avant-projet, il entend remplacer le paragraphe 2 de l'article 18/3 de la loi du 30 novembre 1998 par une disposition qui, dans la motivation de la décision du dirigeant du service de recourir à des mesures spécifiques de recueil de données⁵⁰, impose que figurent « le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle ».

Comparant ces deux dispositions, dans son avis favorable n° 33/2015 donné le 9 septembre 2015 sur le texte en projet, la Commission pour la protection de la vie privée « remarque toutefois que l'avant-projet de loi n'a pas repris la catégorie professionnelle des journalistes dans [la mesure d'exception prévue à l'article 9 de l'avant-projet], ce qui était par contre le cas à l'article 12 de l'avant-projet de loi. » En conséquence, la Commission demande « d'également appliquer cette mesure d'exception aux journalistes ».

L'avant-projet n'a pas été modifié à la suite de cette observation. Le commentaire des articles s'en explique comme suit :

« Dans son avis précité, la Commission vie privée demande d'inclure les journalistes parmi les professions protégées par le § 3. Un tel ajout n'est pas jugé nécessaire car les journalistes bénéficient déjà de la protection qui leur est accordée par la loi du 7 avril 2005 relative à la protection des sources journalistes. L'accès aux données n'est possible que si l'information est jugée cruciale pour l'identification et la recherche des auteurs d'infractions mettant en danger l'intégrité physique ou pour éviter ce type d'infraction. En outre, le secret des sources journalistiques ne peut être levé que si l'information demandée ne peut être obtenue autrement. L'intervention du juge garantit le respect de ces exigences (DOC 51-24/001, p. 13).

En application de l'article 5 de la loi du 7 avril 2005, il ne pourra être procédé à aucune mesure d'information ou d'instruction concernant des données relatives aux sources d'information des journalistes, sauf si ces données sont susceptibles de prévenir la commission des infractions constituant une menace grave pour l'intégrité physique d'une ou de plusieurs personnes dans les conditions citées' ci-avant.

Les travaux préparatoires de la loi du 7 avril 2005 précisent que 'Il va de soi que le journaliste doit avoir obtenu ses informations de manière licite. Un journaliste qui a obtenu ses informations en commettant une infraction sera donc passible de poursuites pénales' (DOC 51-24/001, p. 11).

En outre, comme précisé précédemment, l'article 88*bis* reflète ce qui existe déjà dans les articles 56*bis* et 90*octies*. Or, ces deux articles visent uniquement l'avocat ou le médecin ».

Effectivement, le secret des sources des journalistes fait déjà l'objet de mesures de protection particulières en matière d'utilisation judiciaire des données y afférentes.

⁵⁰ Notamment celles prévues aux articles 18/7 et 18/8 de la même loi.

Ainsi, l'article 5 de la loi du 7 avril 2005 'relative à la protection des sources journalistes' dispose en effet comme suit :

« Art. 5. Il ne pourra être procédé à aucune mesure d'information ou d'instruction concernant des données relatives aux sources d'information des personnes visées à l'article 2, sauf si ces données sont susceptibles de prévenir la commission des infractions visées à l'article 4, et dans le respect des conditions qui y sont définies ».

Cette disposition n'ayant trait qu'aux mesures d'information et d'instruction et non pas aux mesures de renseignement et de sécurité, il se justifie que le texte en projet envisage des mesures complémentaires de protection des sources pour le recueil de données en matière de renseignement et de sécurité, sans en prévoir en matière judiciaire.

Article 10

Il convient de remplacer les mots « est joint le rapport dressé en application de l'article 126, § 5, alinéa 4, » par les mots « sont jointes les données visées à l'article 126, § 5, alinéa 4, ».

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de gecoördineerde wetten op de Raad van State, 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.

ALGEMENE OPMERKINGEN

I. STREKKING VAN HET VOORONTWERP, EUROPEES RECHT EN EUROPESE RECHTSPRAAK, INTERNE RECHTSPRAAK

1. Het Hof van Justitie van de Europese Unie heeft bij een arrest van de Grote kamer van 8 april 2014, gewezen naar aanleiding van de prejudiciële vragen van de High Court van Ierland en het Verfassungsgerichtshof van Oostenrijk (HvJ, C-293/12, Digital Rights Ireland Ltd, en C-594/12, Kärntner Landesregierung e.a.), 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) ongeldig verklaard.

De motivering en de beslissing van dat arrest luiden als volgt:

“Bestaan van inmenging in de in de artikelen 7 en 8 van het Handvest neergelegde rechten

(...)

34. (...) de door de artikelen 3 en 6 van richtlijn 2006/24 aan aanbieders van openbaar beschikbare elektronischecommunicatiediensten of een openbaar communicatienetwerk opgelegde verplichting om gegevens betreffende het privéleven van een persoon en zijn communicaties, zoals die welke zijn bedoeld in artikel 5 van deze richtlijn, gedurende een bepaalde tijd te bewaren, [vormt] op zich een inmenging (...) in de door artikel 7 van het Handvest gewaarborgde rechten.

35. Bovendien vormt de toegang van de bevoegde nationale autoriteiten tot de gegevens een aanvullende inmenging in dat fundamentele recht (zie met betrekking tot artikel 8 EVRM, arresten EHRM, Leander/Zweden, 26 maart 1987, reeks A nr. 116, § 48; Rotaru/Roemenië [Grote kamer], nr. 28341/95, § 46, CEDH 2000-V, en Weber en Saravia/Duitsland (dec.), nr. 54934/00, § 79, CEDH 2006-XI). De artikelen 4 en 8 van richtlijn 2006/24, die de toegang van de bevoegde nationale autoriteiten tot de gegevens regelen, vormen dus eveneens een inmenging in de door artikel 7 van het Handvest gewaarborgde rechten.

36. Richtlijn 2006/24 vormt ook een inmenging in het door artikel 8 van het Handvest gewaarborgde fundamentele recht op bescherming van persoonsgegevens, aangezien zij voorziet in de verwerking van persoonsgegevens.

37. Vastgesteld moet worden dat richtlijn 2006/24 een zeer ruime en bijzonder zware inmenging vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde

fundamentele rechten, zoals de advocaat-generaal met name in de punten 77 en 80 van zijn conclusie heeft opgemerkt. Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, zoals de advocaat-generaal in de punten 52 en 72 van zijn conclusie heeft opgemerkt.

Rechtvaardiging van de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten

38. Volgens artikel 52, lid 1, van het Handvest moeten beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen, en kunnen, met inachtneming van het evenredigheidsbeginsel, alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden.

39. Wat de wezenlijke inhoud van het fundamentele recht op eerbiediging van het privéleven en de andere door artikel 7 van het Handvest erkende rechten betreft, moet worden vastgesteld dat de door richtlijn 2006/24 voorgeschreven bewaring van gegevens weliswaar een bijzonder zware inmenging in deze rechten vormt, maar niet raakt aan de inhoud ervan, aangezien deze richtlijn, zoals blijkt uit artikel 1, lid 2, ervan, niet de mogelijkheid biedt om kennis te nemen van de inhoud zelf van de elektronische communicaties.

40. Deze bewaring van gegevens doet evenmin afbreuk aan de wezenlijke inhoud van het door artikel 8 van het Handvest erkende fundamentele recht op bescherming van persoonsgegevens, aangezien richtlijn 2006/24 in artikel 7 ervan een regel inzake gegevensbescherming en -beveiliging bevat op grond waarvan de aanbieders van openbaar beschikbare elektronischecommunicatiediensten of van een publiek communicatienetwerk, onverminderd de bepalingen die zijn goedgekeurd ingevolge de richtlijnen 95/46 en 2002/58, bepaalde beginselen van gegevensbescherming en -beveiliging moeten respecteren. Volgens deze beginselen moeten de lidstaten ervoor zorgen dat passende technische en organisatorische maatregelen worden genomen om te vermijden dat de gegevens per ongeluk of onrechtmatig worden vernietigd dan wel per ongeluk verloren geraken of worden gewijzigd.

41. Met betrekking tot de vraag of deze inmenging voldoet aan een doel van algemeen belang, zij opgemerkt dat richtlijn 2006/24 weliswaar strekt tot harmonisatie van de bepalingen van de lidstaten betreffende de verplichtingen van bovengenoemde aanbieders inzake de bewaring van bepaalde gegevens die door hen worden gegenereerd of verwerkt, maar dat het materiële doel van deze richtlijn, zoals blijkt uit artikel 1, lid 1, ervan, erin bestaat te garanderen dat die gegevens beschikbaar zijn met het oog op het onderzoek, de opsporing en de vervolging van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten. Deze richtlijn heeft dus materieel tot doel om tot de bestrijding van ernstige criminaliteit en aldus uiteindelijk tot de openbare veiligheid bij te dragen.

42. Volgens de rechtspraak van het Hof vormt de bestrijding van terrorisme ter handhaving van de internationale vrede en veiligheid een doel van algemeen belang van de Unie (zie in die zin arresten Kadi en Al Barakaat International Foundation/Raad en Commissie, C-402/05 P en C-415/05 P, EU:C:2008:461, punt 363, en Al-Aqsa/Raad, C-539/10 P en C-550/10 P, EU:C:2012:711, punt 130). Hetzelfde geldt voor de bestrijding van ernstige criminaliteit ter waarborging van de openbare veiligheid (zie in die zin arrest Tsakouridis, C-145/09, EU:C:2010:708, punten 46 en 47). In dit verband zij

voorts opgemerkt dat artikel 6 van het Handvest bepaalt dat eenieder niet alleen recht heeft op vrijheid, maar ook op veiligheid.

43. Dienaangaande blijkt uit punt 7 van de considerans van richtlijn 2006/24 dat de Raad justitie en binnenlandse zaken van 19 december 2002 wegens de opmerkelijke toename van de mogelijkheden van elektronische communicatie heeft geoordeeld dat gegevens betreffende het gebruik daarvan van bijzonder belang zijn en dus een waardevol instrument vormen bij het voorkomen van strafbare feiten en het bestrijden van criminaliteit, met name van de georganiseerde misdaad.

44. De door richtlijn 2006/24 voorgeschreven bewaring van gegevens, die de bevoegde nationale autoriteiten de mogelijkheid moet bieden om deze eventueel te raadplegen, beantwoordt dus daadwerkelijk aan een doel van algemeen belang.

45. In deze omstandigheden moet worden nagegaan of de vastgestelde inmenging evenredig is.

46. Dienaangaande zij eraan herinnerd dat het evenredigheidsbeginsel volgens vaste rechtspraak van het Hof vereist dat handelingen van de instellingen van de Unie geschikt zijn om de door de betrokken regeling nagestreefde legitieme doelstellingen te verwezenlijken en niet verder gaan dan wat daarvoor geschikt en noodzakelijk is (zie in die zin arresten *Afton Chemical*, C-343/09, EU:C:2010:419, punt 45; *Volker und Markus Schecke en Eifert*, EU:C:2010:662, punt 74; *Nelson e.a.*, C-581/10 en C-629/10, EU:C:2012:657, punt 71; *Sky Österreich*, C-283/11, EU:C:2013:28, punt 50, en *Schaible*, C-101/12, EU:C:2013:661, punt 29).

47. Wat het rechterlijk toezicht op de naleving van deze voorwaarden betreft, zij opgemerkt dat wanneer sprake is van een inmenging in fundamentele rechten, de omvang van de beoordelingsbevoegdheid van de wetgever van de Unie beperkt kan zijn. Dit hangt af van een aantal factoren, waaronder met name het betrokken domein, de aard van het door het Handvest gewaarborgde recht dat aan de orde is, alsook de aard, de ernst en het doel van de inmenging (zie naar analogie met betrekking tot artikel 8 EVRM, arrest EHRM, *S en Marper/Verenigd Koninkrijk [Grote kamer]*, nrs. 30562/04 en 30566/04, § 102, CEDH 2008-V).

48. Gelet op de belangrijke rol die de bescherming van persoonsgegevens speelt in het licht van het fundamentele recht op bescherming van het privéleven, alsook op de omvang en de ernst van de door richtlijn 2006/24 veroorzaakte inmenging in dit recht is de beoordelingsbevoegdheid van de Uniewetgever in casu beperkt, zodat een strikt toezicht moet worden uitgeoefend.

49. Met betrekking tot de vraag of het door richtlijn 2006/24 nagestreefde doel kan worden verwezenlijkt door de bewaring van de gegevens, moet worden vastgesteld dat de gegevens die op grond van deze richtlijn moeten worden bewaard, gelet op het groeiende belang van elektronische communicatiemiddelen de nationale strafvervolgingsautoriteiten extra mogelijkheden bieden om ernstige gevallen van criminaliteit op te helderen en in die zin dus een waardevol instrument vormen bij strafonderzoeken. De bewaring van dergelijke gegevens is derhalve geschikt voor de verwezenlijking van het door deze richtlijn nagestreefde doel.

50. Aan deze beoordeling wordt niet afgedaan door de omstandigheid dat er verschillende vormen van elektronische communicatie bestaan die niet binnen de werkingssfeer van richtlijn 2006/24 vallen of die anonieme communicatie mogelijk maken, zoals met name *Tschohl en Seitlinger* alsook de Portugese regering in hun bij het Hof ingediende schriftelijke opmerkingen hebben aangevoerd. Dit heeft weliswaar tot gevolg dat de bewaring van gegevens niet volstrekt geschikt is om het nagestreefde doel

te bereiken, maar dat betekent nog niet dat deze maatregel daarvoor ongeschikt is, zoals de advocaat-generaal in punt 137 van zijn conclusie heeft opgemerkt.

51. Wat de noodzaak van de door richtlijn 2006/24 voorgeschreven bewaring van gegevens betreft, zij vastgesteld dat de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, weliswaar van primordiaal belang is om de openbare veiligheid te waarborgen, en dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd.

52. Wat het recht op eerbiediging van het privéleven betreft, zij opgemerkt dat de bescherming van dit fundamentele recht volgens vaste rechtspraak van het Hof hoe dan ook vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (arrest IPI, C-473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).

53. Dienaangaande zij eraan herinnerd dat de bescherming van persoonsgegevens, die uitdrukkelijk wordt voorgeschreven door artikel 8, lid 1, van het Handvest, van bijzonder belang is voor het in artikel 7 van dit Handvest verankerde recht op eerbiediging van het privéleven.

54. De betrokken Unieregeling moet dus duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens (zie naar analogie met betrekking tot artikel 8 EVRM, arresten EHRM, *Liberty e.a./Verenigd Koninkrijk*, nr. 58243/00, § 62 en 63, van 1 juli 2008; *Rotaru/Roemenië*, reeds aangehaald, § 57-59, en *S en Marper/Verenigd Koninkrijk*, reeds aangehaald, § 99).

55. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens, zoals is bepaald in richtlijn 2006/24, automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd (zie naar analogie met betrekking tot artikel 8 EHRM, arresten EHRM, *S en Marper/Verenigd Koninkrijk*, reeds aangehaald, § 103, en *M. K./Frankrijk*, nr. 19522/09, § 35, van 18 april 2013).

56. Met betrekking tot de vraag of de inmenging die richtlijn 2006/24 meebrengt, beperkt is tot het strikt noodzakelijke, zij opgemerkt dat artikel 3 van deze richtlijn, gelezen in samenhang met artikel 5, lid 1, ervan, voorschrijft om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren. Deze richtlijn strekt zich dus uit tot alle wijdverspreide elektronischecomunicatiemiddelen, die een steeds belangrijker plaats innemen in het dagelijkse leven van de mensen. Bovendien ziet deze richtlijn ingevolge artikel 3 ervan op alle abonnees en geregistreerde gebruikers. Zij leidt dus tot inmenging in de fundamentele rechten van bijna de gehele Europese bevolking.

57. Dienaangaande zij in de eerste plaats vastgesteld dat richtlijn 2006/24 algemeen van toepassing is op alle personen, alle elektronischecomunicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel, zware criminaliteit te bestrijden.

58. Richtlijn 2006/24 is om te beginnen algemeen van toepassing op alle personen die gebruikmaken van elektronische communicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met zware criminaliteit. Bovendien bevat de richtlijn geen uitzonderingen, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het zakengeheim vallen.

59. Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.

60. In de tweede plaats bevat richtlijn 2006/24 niet alleen geen beperkingen, maar ook geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. Integendeel, richtlijn 2006/24 verwijst in artikel 1, lid 1, ervan enkel op algemene wijze naar ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.

61. Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. Artikel 4 van deze richtlijn, dat de toegang van deze autoriteiten tot de bewaarde gegevens regelt, bepaalt niet uitdrukkelijk dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen, maar bepaalt enkel dat elke lidstaat de procedure en de te vervullen voorwaarden vaststelt voor toegang tot de bewaarde gegevens overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid.

62. In het bijzonder bevat richtlijn 2006/24 geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel. Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Aan de lidstaten is evenmin enige specifieke verplichting opgelegd om dergelijke beperkingen vast te stellen.

63. Wat in de derde plaats de termijn betreft gedurende welke de gegevens worden bewaard, bepaalt artikel 6 van richtlijn 2006/24 dat deze gedurende ten minste zes maanden moeten worden bewaard, zonder dat enig onderscheid wordt gemaakt tussen de in artikel 5 van deze richtlijn genoemde categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen.

64. Bovendien varieert de bewaringstermijn van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is.

65. Uit het bovenstaande volgt dat richtlijn 2006/24 geen duidelijke en precieze regels bevat betreffende de omvang van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten. Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke.

66. Bovendien moet met betrekking tot de regels inzake de beveiliging en de bescherming van de gegevens die worden bewaard door de aanbieders van openbaar beschikbare elektronischecomunicatiediensten of een openbaar communicatienetwerk worden vastgesteld dat richtlijn 2006/24 onvoldoende garanties biedt dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan, zoals wordt vereist door artikel 8 van het Handvest. In de eerste plaats bevat artikel 7 van richtlijn 2006/24 geen specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die volgens deze richtlijn moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd, en die met name ertoe strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen. Bovendien is aan de lidstaten ook geen specifieke verplichting opgelegd om dergelijke regels vast te stellen.

67. Artikel 7 van richtlijn 2006/24, gelezen in samenhang met artikel 4, lid 1, van richtlijn 2002/58 en artikel 17, lid 1, tweede alinea, van richtlijn 95/46, waarborgt niet dat bovengenoemde aanbieders via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden, maar verleent deze aanbieders met name de mogelijkheid om bij de vaststelling van het door hen geboden beschermingsniveau rekening te houden met economische overwegingen, meer bepaald met de kosten voor het uitvoeren van de veiligheidsmaatregelen. In het bijzonder waarborgt richtlijn 2006/24 niet dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd.

68. In de tweede plaats schrijft deze richtlijn niet voor dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard, zodat niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest. Een dergelijk toezicht op basis van het Unierecht is evenwel van wezenlijk belang voor de bescherming van personen bij de verwerking van persoonsgegevens (zie in die zin arrest Commissie/Oostenrijk, C-614/10, EU:C:2012:631, punt 37).

69. Gelet op een en ander moet worden geoordeeld dat de wetgever van de Unie met de vaststelling van richtlijn 2006/24 de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest in acht dient te nemen”.

2. Als gevolg van dat arrest van het Hof van Justitie heeft het Grondwettelijk Hof bij arrest 84/2015 van 11 juni 2015 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' vernietigd, die ertoe strekte richtlijn 2006/24/EG gedeeltelijk om te zetten.

Het arrest van het Grondwettelijk Hof steunt op de volgende motivering:

“B.10.1. Zoals het Hof van Justitie heeft opgemerkt in de punten 56 en 57 van zijn arrest, schrijft de richtlijn voor om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren, waardoor zij algemeen van toepassing is op alle personen en alle elektronische communicatiemiddelen, zonder onderscheid op basis van het doel, namelijk zware criminaliteit bestrijden, dat de Uniewetgever wilde nastreven.

De bestreden wet verschilt op dat punt niet van de richtlijn. Zoals in B.8 is vermeld, zijn immers de categorieën van gegevens die moeten worden bewaard identiek aan die welke zijn opgesomd in de richtlijn, terwijl geen enkel onderscheid wordt gemaakt met betrekking tot de betrokken personen of de bijzondere regels die moeten worden bepaald op basis van het doel van bestrijding van de inbreuken beschreven in artikel 126, § 2, van de wet van 13 juni 2005, dat bij de bestreden wet werd vervangen. Net zoals het Hof van Justitie heeft vastgesteld met betrekking tot de richtlijn (punt 58), is de wet dus ook van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met de in de bestreden wet opgesomde inbreuken. Op dezelfde wijze is de wet, zonder enige uitzondering, ook van toepassing op personen van wie de communicaties onder het beroepsgeheim vallen.

B.10.2. Niet méér dan het geval is voor de richtlijn, vereist het bestreden artikel 5 enig verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Het beperkt evenmin de bewaring van de desbetreffende gegevens tot een bepaalde periode of een bepaalde geografische zone of nog tot een kring van personen die betrokken kunnen zijn bij een door de wet beoogde inbreuk, of die zouden kunnen helpen, door het bewaren van de gegevens, bij het voorkomen, opsporen of vervolgen van die inbreuken.

B.10.3. Ook al worden de autoriteiten die gemachtigd zijn tot toegang tot de bewaarde gegevens, opgesomd in artikel 126, § 5, 3°, van de wet van 13 juni 2005, vervangen bij artikel 5 van de bestreden wet, toch wordt bij de wet geen enkele materiële of procedurele voorwaarde vastgelegd met betrekking tot die toegang.

B.10.4. Wat ten slotte de bewaarperiode van de gegevens betreft, maakt de wet geen enkel onderscheid tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken personen.

B.11. Om dezelfde redenen als die welke het Hof van Justitie van de Europese Unie ertoe hebben gebracht de ‘Dataretentierichtlijn’ ongeldig te verklaren, dient te worden vastgesteld dat de wetgever, met de aanneming van artikel 5 van de bestreden wet, de grenzen heeft overschreden die worden opgelegd door de eerbiediging van het evenredigheidsbeginsel in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Het voormelde artikel 5 schendt bijgevolg de artikelen 10 en 11 van de Grondwet, in samenhang gelezen met die bepalingen. Het enige middel in de zaak nr. 5856 en het eerste middel in de zaak nr. 5859 zijn gegrond.

B.12. Wegens hun ondeelbaar karakter met artikel 5, dienen ook de artikelen 1 tot 4, 6 en 7 van de bestreden wet van 30 juli 2013, en dus de wet in haar geheel, te worden vernietigd”.

Het voorliggende voorontwerp strekt ertoe gevolg te geven aan dat arrest 84/2015 van het Grondwettelijk Hof van 11 juni 2015, dat zelf gevolg geeft aan het arrest van het Hof van Justitie van 8 april 2014.

3. Wat het Europees recht betreft, moet worden opgemerkt dat het arrest van het Hof van Justitie van de Europese Unie, waarbij uitspraak wordt gedaan naar aanleiding van een vraag om de geldigheid van afgeleid recht van de Unie te beoordelen en waarin tot de ongeldigheid van een Europese norm wordt besloten, niet als gevolg heeft dat de ongeldig verklaarde norm uit de rechtsorde verdwijnt, noch dat de normen die eventueel bij de ongeldig verklaarde tekst zijn opgeheven, opnieuw van toepassing worden.

Niettemin moeten alle nationale rechtscolleges zich richten naar het feit dat de ongeldigheid is vastgesteld,¹ moeten de overheden van de Unie de ongeldig verklaarde handeling wijzigen of opheffen en moeten de nationale overheden, met inachtneming van de nationale procedures, de eigen regels wijzigen of opheffen die ingevolge de ongeldig verklaarde handeling zijn vastgesteld.²

Aangezien richtlijn 2006/24/EG, die de verschillende wetgevingen van de lidstaten over de bewaring van de gegevens betreffende elektronische communicatie onderling in overeenstemming beoogde te brengen, ongeldig is verklaard, mag niet de richtlijn, maar enkel het recht dat vóór de inwerkingtreding van de richtlijn van toepassing was, in aanmerking genomen worden, niettegenstaande de bevoegde overheden van de Europese Unie die richtlijn nog niet hebben opgeheven of gewijzigd.

Wat dat betreft, moet rekening worden gehouden met artikel 15 van richtlijn 2002/85/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), zoals dat van toepassing was voordat het bij richtlijn 2006/24/EG is gewijzigd.³

¹ Waarbij die rechtscolleges zich eventueel opnieuw tot het Hof moeten wenden indien er nog twijfels zijn over wat die ongeldigheid precies inhoudt.

² Zie hierover C. SOULARD, A. RIGAUX, D. SIMON en R. MUNOZ, « *Contentieux de l'Union européenne. Renvoi préjudiciel, recours en manquement / 3* », Parijs, Lamy & Wolters Kluwer France, 2011, 108 e.v.

³ Wat betreft de vraag of het recht van de Europese Unie en meer bepaald het Handvest van de grondrechten van de Europese Unie toepasselijk is op de maatregelen inzake de bewaring van metagegevens die met het oog op de openbare veiligheid, de landsverdediging en de staatsveiligheid door de lidstaten worden genomen, moet rekening worden gehouden met de artikelen 72 en 73 van het Verdrag betreffende de werking van de Europese Unie. Die bepalingen bevinden zich in titel V van het derde deel van het Verdrag, betreffende de ruimte van vrijheid, veiligheid en recht. Artikel 72 bepaalt dat “[d]eze titel (...) de uitoefening van de verantwoordelijkheid van de lidstaten voor de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid onverlet [laat]”, terwijl artikel 73 bepaalt dat “[h]et (...) de lidstaten vrij[staat] onderling en onder hun verantwoordelijkheid vormen van samenwerking en coördinatie te organiseren zoals zij het passend achten tussen hun bevoegde overheidsdiensten die verantwoordelijk zijn voor het verzekeren van de nationale veiligheid”. De Raad van State van Frankrijk heeft evenwel opgemerkt dat het afgeleid recht van de Unie dienaangaande soms complexer blijkt te zijn. Zo stelt hij in verband met artikel 15 van richtlijn 2002/58/EG, in “Les rapports du Conseil d’Etat – Le numérique et les droits fondamentaux” het volgende: “(...) tant la directive n° 95/46/CE que la directive n° 2002/58/CE excluent de leur champ la matière pénale et les traitements ayant pour objet la sécurité publique, la défense et la sûreté de l’État. Et l’existence de ces actes, mettant en œuvre le droit de l’Union, est une condition d’application de la Charte. La

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.

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

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

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

directive n° 2002/58/CE est cependant ambiguë à cet égard: si son article 1.3 restreint son champ d'application, son article 15.1 dispose que les États ne peuvent déroger aux droits garantis par la directive pour les finalités énumérées ci-dessus que s'il s'agit de mesures nécessaires et proportionnées, prises dans le respect des 'principes généraux du droit communautaire'. Il traite en particulier de la conservation des données, en prévoyant que 'les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié' par l'une des finalités énumérées ci-dessus. Il est donc possible de soutenir que la directive n° 2002/58/CE régit les législations des États relatives à la conservation des métadonnées. Les usages des métadonnées en matière de sécurité nationale échappent au champ d'application du droit de l'Union, mais la conservation porte atteinte par elle-même, indépendamment de l'usage, aux droits garantis par la directive, puisque l'article 5 impose en principe l'effacement des données. En outre, si la proposition de directive relative à la protection des données personnelles en matière pénale était adoptée, les traitements de données personnelles à des fins de police judiciaire entreraient pleinement dans le champ du droit de l'Union européenne. Dès lors, en raison de l'ambiguïté du champ d'application de la directive n° 2002/58/CE, la question de la conformité de la législation nationale à la Charte des droits fondamentaux de l'Union européenne, telle qu'elle a été interprétée par la C.J.U.E. dans l'arrêt Digital Rights Ireland, reste posée” (<http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>, 199-200).

⁴ Lid ingevoegd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 ‘tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming’.

4. Wat het interne recht betreft, worden de bepalingen van de wet van 30 juli 2013, zoals in de memorie van toelichting van het voorliggende voorontwerp wordt onderstreept, geacht nooit te hebben bestaan, aangezien ze vernietigd zijn, en worden de bepalingen die bij die wet zijn opgeheven opnieuw toepasselijk.

Als gevolg van de vernietiging van de wet van 30 juli 2013 is meer bepaald de versie van artikel 126 van de wet van 13 juni 2005 ‘betreffende de elektronische communicatie’⁵ toepasselijk die vóór de inwerkingtreding van de wet van 30 juli 2013 van kracht was en die luidt 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”.

Volgens de memorie van toelichting bij de ontworpen tekst “schenkt” het hierboven weergegeven artikel 126 “geen voldoening”.

5. In die context beoogt de steller van het voorontwerp derhalve niet meer de richtlijn om te zetten die het Hof van Justitie ongeldig heeft verklaard, maar wil veeleer een regeling voor gegevensbewaring invoeren die de doelstellingen dient die het Hof van Justitie en het Grondwettelijk Hof legitiem hebben geacht en die in overeenstemming is met het dictum en de motivering van de beslissingen van die hoge rechtscolleges.

Bovendien moet worden opgemerkt dat in de ontworpen tekst, evenals in het geldende artikel 126 en in het artikel 126 dat bij arrest 84/2015 van het Grondwettelijk Hof is vernietigd, wordt voorgeschreven dat gegevens worden bewaard met een doel dat verder gaat dan de doelstellingen waarin richtlijn 2006/24/EG voorziet en die bestaan in “het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten”.

⁵ Hierna “de wet van 13 juni 2005” genoemd.

Zo bijvoorbeeld zullen de te bewaren gegevens aan de bevoegde overheden worden meegedeeld met het oog op welbepaalde doeleinden, waaronder inzonderheid de identificatie van de personen die een hulpdienst hebben opgeroepen zodat de dienst in kwestie tijdig kan handelen, de opsporing van personen van wie de verdwijning onrustwekkend is en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is, of de identificatie van de persoon die kwaadwillig gebruik heeft gemaakt van een netwerk of een dienst voor elektronische communicatie.⁶

Hetzelfde geldt voor de doeleinden die de ontworpen tekst vermeldt betreffende het voorkomen en bestraffen van criminaliteit in het algemeen, betreffende de gevaren voor het menselijk leven of voor de fysieke integriteit van personen en goederen, of betreffende het onrechtmatige gebruik van systemen voor elektronische communicatie, en die in de lijn liggen van de doelstellingen die in artikel 15 van richtlijn 2002/58/EG worden opgenoemd.

II. BEPALINGEN INGEVOERD BIJ DE ONTWORPEN TEKST OM TEGEMOET TE KOMEN AAN DE VEREISTEN WAARAAN VOLGENS DE ARRESTEN VAN HET HOF VAN JUSTITIE EN VAN HET GRONDWETTELIJK HOF VOLDAAN MOET ZIJN

1. Uit het arrest van het Hof van Justitie, waarop het arrest van het Grondwettelijk Hof aansluit, moet voornamelijk het volgende worden onthouden:

1° De bewaring van gegevens met de bedoeling dat de bevoegde nationale overheden eventueel tot die gegevens toegang hebben, zoals richtlijn 2006/24/EG voorschrijft, vormt een inmenging in het fundamentele recht op eerbiediging van de persoonlijke levenssfeer en in de andere rechten die zijn neergelegd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, met als verzwarende omstandigheid dat de overheden kennis moeten kunnen nemen van die gegevens.

2° De wezenlijke inhoud van die rechten kan evenwel niet door die inmenging worden aangetast, aangezien artikel 1, lid 2, van richtlijn 2006/24/EG niet toestaat dat van de inhoud zelf van de elektronische communicatie kennis wordt genomen.

3° Die inmenging beantwoordt voorts aan een doelstelling van algemeen belang, namelijk de bestrijding van het internationale terrorisme, de bestrijding van de zware criminaliteit met het oog op de openbare veiligheid en het recht van eenieder op veiligheid, en bewaring van de gegevens in kwestie kan worden beschouwd als een geschikt middel om de doelstelling te verwezenlijken die richtlijn 2006/24/EG nastreeft.

4° De vraag rijst dus of de beoogde inmenging evenredig is met het nagestreefde doel, namelijk of het gaat om maatregelen die absoluut noodzakelijk zijn om dat doel te bereiken. Wat dat betreft moet de regeling in kwestie “duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van

⁶ Ontworpen artikel 126, § 2.

misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens”.

Dienaangaande moet het volgende in aanmerking worden genomen.

1° Het feit dat de regeling algemeen van toepassing is op alle personen, alle middelen voor elektronische communicatie en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel zware criminaliteit te bestrijden. Dat blijkt uit het volgende:

a) enerzijds schrijft de regeling niet voor dat de personen van wie de gegevens worden bewaard zich, zelfs niet indirect, in een situatie moeten bevinden die aanleiding kan geven tot strafrechtelijke vervolging, en bevat ze geen uitzonderingen, zodat ze zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het beroepsgeheim vallen;

b) anderzijds schrijft de regeling niet voor dat er een verband moet bestaan tussen de te bewaren gegevens en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.

2° Het feit dat de regeling niet alleen geen beperkingen oplegt, maar ook “geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen”. Wat dat betreft, bevat de regeling “[niet de desbetreffende] materiële en procedurele voorwaarden” en “bepaalt [ze] niet uitdrukkelijk dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen”. Er zijn inzonderheid “geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel”, en “de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens [is] niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten”.

3° Het feit dat de gegevens gedurende een termijn van ten minste zes maanden moeten worden bewaard “zonder dat enig onderscheid wordt gemaakt tussen de (...) categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen”. “Bovendien varieert de bewaringstermijn van ten minste zes maanden tot

ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is”.

Derhalve kan, volgens het Hof van Justitie, niet worden aangenomen “dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke”.

Bovendien,

4° is er niet voorzien in “specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die volgens deze richtlijn moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd, en die met name ertoe strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen”. Er wordt van de aanbieders meer bepaald niet vereist dat ze “via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden”: er wordt inzonderheid niet gewaarborgd dat “de gegevens na de bewaarperiode onherroepelijk worden vernietigd”.

5° wordt nergens voorgeschreven dat de gegevens in kwestie op het grondgebied van de Unie moeten worden bewaard, zodat “niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest”.

2. Hoewel de doelstellingen die het voorliggende voorontwerp nastreeft, verder reiken dan die van richtlijn 2006/24/EG dat door het Hof van Justitie ongeldig is verklaard, blijkt niet, zoals hierboven is uiteengezet, niet dat elk van die doelen legitiem zou zijn en, meer bepaald, dat ze niet in overeenstemming zouden kunnen zijn met artikel 15, lid 1, van richtlijn 2002/58/EG.

Bij het onderzoek van het voorontwerp van wet moet dus rekening worden gehouden met de omstandigheid dat de vereisten waaraan volgens het arrest van het Hof van Justitie voldaan moet zijn, betrekking hebben op de bewaring van en de daaropvolgende toegang tot gegevens zoals bedoeld in richtlijn 2006/24/EU, namelijk de bewaring en de toegang tot gegevens “teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit”. De strekking van het arrest van het Hof en de gevolgtrekkingen die daaruit moeten worden gemaakt, hoe strikt deze ook zijn, hebben dus enkel betrekking op het bewaren van gegevens waarvan het uiteindelijke doel erin bestaat gedragingen en handelingen die zware overtredingen vormen, strafrechtelijk te bestraffen, wat per definitie geen lichte bestraffing kan zijn.

De strekking van dat arrest kan dus *a priori* niet worden uitgebreid tot een bewaring van gegevens of een toegang tot bewaarde gegevens die andere doeleinden zouden dienen, zoals het opsporen door een ombudsdienst van een persoon die kwaadwillige oproepen pleegt, de identificatie van de persoon die een hulpdienst belt of van de plaats van waaruit zo’n

oproep wordt gedaan zodat de hulpdienst kan optreden en kan zorgen voor de bescherming van goederen en personen, of het opsporen buiten iedere strafrechtelijke context van een persoon van wie de verdwijning onrustwekkend is wanneer blijkt dat zijn leven in onmiddellijk gevaar zou kunnen zijn. De strekking van het arrest kan zelfs niet tot de activiteiten van de inlichtingendiensten worden uitgebreid.

Deze laatste gevallen zullen dus alleen worden onderzocht in het licht van het recht op eerbiediging van het privéleven dat bij artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en bij artikel 22 van de Grondwet is gewaarborgd.⁷

3. Gelet op het aldus in herinnering gebrachte juridisch kader, geeft de ontworpen tekst aanleiding tot de volgende algemene opmerkingen.

3.1. Het feit dat de ontworpen tekst in het algemeen betrekking heeft op alle personen, zonder dat enig onderscheid wordt gemaakt tussen personen, periode en geografische zone en zonder dat vereist is dat enig verband bestaat tussen de gegevens die zouden worden bewaard en een bedreiging van de openbare veiligheid

3.1.1. In de memorie van toelichting wordt in dat verband melding gemaakt van het volgende:

“De behoefte om de houder van een gsm-nummer of van een IP-adres te identificeren, is een gebruikelijk aspect van de onderzoeken en een absoluut noodzakelijk onderdeel ervan geworden. De toegang tot het overzicht van de communicaties of de lokalisatie *a posteriori* van de verdachte of van het slachtoffer zijn maatregelen die de persoonlijke levenssfeer meer aantasten en die minder worden gebruikt dan de identificatie, maar zij zijn niettemin zeer vaak absoluut noodzakelijk in bepaalde soorten zaken.

Het ontwerp van wet heeft geen betrekking op de inhoud van de communicaties.

De sector van het terrorisme is uiteraard bijzonder actueel. De toegang tot de communicatiegegevens is een noodzakelijke stap voor het identificeren van de personen en de banden die zij onderling hebben. Wanneer bij een huiszoeking een hele zak simkaarten wordt ontdekt of een draagbare computer in beslag wordt genomen, wordt vervolgens een groot aantal onderzoekshandelingen verricht om de communicaties na te trekken die met die elementen zijn verricht en daarna met andere aldus geïdentificeerde elementen, enz. Dergelijke maatregelen zijn ook onontbeerlijk wanneer een persoon die nog niet bekend was bij de politie- of inlichtingendiensten zich blijkt te hebben aangesloten bij een terroristische organisatie in Syrië bijvoorbeeld. Tot slot is het bij het onderzoek na een aanslag uiteraard noodzakelijk om terug te gaan in de communicaties van de verdachte, inzonderheid om na te gaan of hij alleen heeft gehandeld of om medeplichtigen te identificeren.

⁷ Zie onder meer L. TASSONE, “La protection des données dans la jurisprudence de la Cour européenne des droits de l’homme” in A. GROSJEAN (ed.), *Enjeux européens et mondiaux de la protection des données personnelles*, verzamelwerk, Larcier, coll. Création Information Communication, 53 e.v., en de verwijzingen aldaar; over de inlichtingen- en veiligheidsdiensten zie onder meer advies 42.178/2, op 19 februari 2007 gegeven over een voorontwerp dat ontstaan gegeven heeft aan de wet van 4 februari 2010 ‘betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten’ (*Parl.St.* Senaat 2006-07, nr. 3-2138/1, 279-297).

De andere sector die zeer vaak wordt vermeld om het belang van die gegevens te illustreren is die van de kinderpornografie. Ook hier moet kunnen worden teruggegaan in de tijd om op basis van de detectie van een element op het internet het volledige criminele netwerk te kunnen blootleggen.

Maar uit die bijzonder sprekende voorbeelden mag niet worden afgeleid dat de gegevens enkel noodzakelijk zijn voor het bestrijden van weliswaar choquerende maar in aantal relatief beperkte fenomenen van criminaliteit. De realiteit is dat de communicatiegegevens nodig zijn in zeer veel verschillende situaties waarin men zich evenwel gemakkelijk kan inbeelden dat die gegevens vaak zowel het vertrekpunt als een fase van het onderzoek zijn, bijvoorbeeld:

- de reactie op een onrustwekkende verdwijning;
- de illegale handel in verdovende middelen;
- de verkoop van namaakgeneesmiddelen op het internet;
- het aanzetten tot haat of geweld;
- belaging, ook bij jongeren;
- spionage, die, net als rekrutering, over verschillende jaren kan zijn gespreid, en hacking voor spionagedoeleinden, kan pas verschillende maanden na de feiten aan het licht komen;
- hacking van bankrekeningen;
- identiteitsdiefstal;
- hacking waarbij bijvoorbeeld wordt gechanteerd met de bekendmaking van de verzamelde persoonsgegevens of commerciële gegevens;
- enz.

Daaraan moet een belangrijke factor worden toegevoegd die het tijdslement en de behoefte om terug te gaan in de tijd beïnvloedt. Die factor is de lokalisatie van de aanbieders van diensten via het internet en het gegeven dat sommige van die diensten die in het buitenland gebaseerd zijn, eisen dat een beroep wordt gedaan op de formele justitiële samenwerking met het oog op de overzending van gegevens. De justitiële samenwerking, inzonderheid met de Verenigde Staten, is echter een zeer zwaar en zeer traag proces. België probeert de situatie te verbeteren maar heeft uiteraard niet alle kaarten in handen. Met dat gegeven moet dan ook rekening worden gehouden.

Door die situatie duurt het vaak verschillende maanden om van een aanbieder van diensten via het internet het IP-adres te krijgen vanwaar een bericht bijvoorbeeld werd verstuurd. Pas vanaf dat moment kunnen de Belgische onderzoekers toegang vragen tot de identificatiegegevens op basis van het betrokken IP-adres.

De toegang tot de communicatiegegevens is dus onontbeerlijk, net als de mogelijkheid om voor een bepaalde periode te kunnen teruggaan in de tijd. Dat hangt uiteraard af van de bewaartermijn van de gegevens.

[...]

De argumentatie van het Grondwettelijk Hof is zeer kort en verwijst vooral naar de beslissing van het Hof van Justitie van de EU betreffende de richtlijn 2006/24/EG.

Het Hof besluit dat het bestreden artikel 126 WEC, net als de richtlijn, een onevenredige beperking van het recht op de eerbiediging van de persoonlijke levenssfeer inhoudt. Die schending van het evenredigheidsbeginsel vloeit voort uit de combinatie van vier elementen:

- het gegeven dat de bewaring van de gegevens voor alle personen geldt;
- het gebrek aan differentiatie op grond van de categorieën van bewaarde gegevens en het nut ervan;
- het gebrek aan of de ontoereikendheid van regels inzake de toegang van de overheden tot de betrokken gegevens;
- en tot slot, hoewel dit element enkel wordt aangehaald door het Hof van Justitie en niet door het Grondwettelijk Hof, het gebrek aan of het tekortschieten van de regels inzake de beveiliging van de gegevens bij de aanbieders of de operatoren.

Die elementen en de antwoorden die het ontwerp van wet daarop biedt, worden hierna overlopen.

[...] Onderscheid op grond van de personen, periodes en geografische zones

Het eerste van de drie elementen waarvan de combinatie het evenredigheidsbeginsel schendt, betreft het beginsel zelf van de verplichting tot het bewaren van de gegevens. Het gaat erom dat de gegevens van alle personen op ongedifferentieerde wijze worden bewaard. Na grondige analyse blijkt dat [...] een *a priori* differentiatie van dit element niet mogelijk is.

De Commissie [voor de bescherming van de persoonlijke levenssfeer] is dezelfde mening toegedaan, aangezien zij er in [...] advies 33-2015 met betrekking tot de ontworpen tekst op wijst dat ‘bepaalde aspecten van [de] arresten [van het Hof van justitie en het grondwettelijke Hof] de Commissie evenwel moeilijk toepasbaar [lijken] te zijn, in het bijzonder het onderscheid op grond van personen, periodes en/of geografische zones’.

a) Alle personen, ook al zijn zij nog niet betrokken bij een onderzoek

De bewaring van de gegevens beperken tot de gegevens betreffende personen ten aanzien van wie reeds een strafonderzoek of een onderzoek met het oog op inlichtingen loopt, heeft geen zin want die mogelijkheid bestaat overigens reeds. De gerechtelijke overheden en de inlichtingendiensten kunnen het ‘doen opsporen’ van de communicaties reeds opleggen in het kader van een specifiek onderzoek en dus de operatoren en aanbieders van toegang verplichten tot het bewaren van de gegevens voor de toekomst, zodra de persoon of een communicatiedienst is geïdentificeerd in een strafonderzoek. Het doel van artikel 126 WEC bestaat erin zich ervan te vergewissen dat een bepaald aantal gegevens ook voor een beperkte periode van het verleden beschikbaar zijn. Artikel 126 heeft dus enkel zin indien het betrekking heeft op de personen ten aanzien van wie nog niet noodzakelijkerwijs een strafonderzoek of een onderzoek met het oog op inlichtingen loopt.

Die dimensie is absoluut noodzakelijk, zoals de in punt 2 vermelde voorbeelden aantonen.

Er moet trouwens erop worden gewezen dat de maatregel zowel in het voordeel kan zijn van het slachtoffer, voor zijn eigen gegevens (in zaken met betrekking tot belaging bijvoorbeeld is het van belang om in het verleden van de gegevens van het slachtoffer te kunnen teruggaan met het oog op het identificeren van de oorsprong van een oproep, een e-mail of een sms), als van de beschuldigde (de lokalisatiegegevens kunnen aantonen dat de beschuldigde niet op de plaats van het misdrijf was op het tijdstip waarop het werd gepleegd). Het kan ook van belang zijn om getuigen te identificeren, wat zowel à charge als à décharge kan meespelen.

b) Geen differentiatie op grond van de periode, de geografische zone of een kring van personen

Het Grondwettelijk Hof, dat verwijst naar het arrest van het Hof van Justitie, wijst erop dat het bestreden artikel 126 ‘de bewaring van de desbetreffende gegevens [evenmin beperkt] tot een bepaalde periode of een bepaalde geografische zone of nog tot een kring van personen die betrokken kunnen zijn bij een door de wet beoogde inbreuk, of die zouden kunnen helpen, door het bewaren van de gegevens, bij het voorkomen, opsporen of vervolgen van die inbreuken’.

Dit deel van het arrest van het Hof van Justitie leidde tot nogal wat vragen over de draagwijdte ervan. De werkgroep die dit ontwerp van wet heeft voorbereid, heeft zich eveneens vragen gesteld over de mogelijkheid de impact van artikel 126 te beperken door te werken aan de door het Hof van Justitie aangehaalde criteria, te weten ‘een bepaalde periode’, ‘een bepaalde geografische zone’ of nog ‘een kring van personen’.

Het besluit is dat dit deel van het arrest van het Hof van Justitie moet worden gelezen als een verklaring voor de gevoeligheid van het beginsel van veralgemeende bewaring van de gegevens. Het is evenwel niet mogelijk een oplossing eraan te ontleen om een differentiatie toe te passen.

De verwijzing naar de ‘periode’ zou bijvoorbeeld een specifieke en tijdelijke situatie van bedreiging van de openbare orde of veiligheid kunnen beogen. Enerzijds is dit type criterium evenwel niet coherent met een groot aantal situaties en types van criminaliteit waarvoor de bewaring van de gegevens doorslaggevend blijkt te zijn (bijvoorbeeld inzake kinderpornografie) en anderzijds zou dit type criterium, daar waar het van toepassing zou kunnen zijn, geen rekening houden met het gegeven dat er niet noodzakelijkerwijs kan worden vooruitgelopen op de betrokken situatie (bijvoorbeeld in geval van een terroristische dreiging die wordt geconcretiseerd door een aanslag). Met betrekking tot de verwijzing naar een ‘geografische zone’ of een ‘kring van personen’ zou een activering van artikel 126 WEC op grond van dit type criterium op profilering lijken, met de risico's van discriminatie die eruit voortvloeien.

c) Geen uitsluiting van bepaalde beroepen

Het Grondwettelijk Hof wijst, nog steeds met betrekking tot dat gebrek aan differentiatie tussen de personen van wie de gegevens worden bewaard, ten slotte erop dat ‘de wet, zonder enige uitzondering, ook van toepassing [is] op personen van wie de communicaties onder het beroepsgeheim vallen’.

Ook hier rees de vraag naar de mogelijkheid te voorzien in een differentiatie om gevolg te geven aan dit deel van het arrest. Het zou erom gaan *a priori* bepaalde personen op grond van hun beroep niet in aanmerking te nemen voor de bewaring van de gegevens.

Die differentiatie is niet mogelijk. Hoewel het klopt dat bepaalde beroepen worden beschermd inzake het verzamelen van bewijzen of inlichtingen, is die bescherming nooit absoluut. Langs de andere kant moet hier nog worden opgemerkt dat de bewaring van de gegevens niet mag worden gezien als een maatregel die strekt tot een toegang *a posteriori* tot de gegevens, noodzakelijkerwijs ‘tegen’ de persoon. Het betrokken gegeven kan worden gebruikt om die persoon vrij te pleiten of nog nuttig zijn wanneer de betrokken persoon het slachtoffer is van een misdrijf. Er moet opnieuw worden opgemerkt dat de bewaring van de gegevens geen betrekking heeft op de inhoud van de communicaties.

Verder in de tekst zal evenwel blijken dat de bescherming van bepaalde beroepen wordt versterkt in dit ontwerp van wet maar op het niveau van de regelgeving inzake de toegang tot de bewaarde gegevens.

Er kan worden geconcludeerd dat het niet mogelijk is artikel 126 WEC nader toe te passen op grond van het door het Grondwettelijk Hof en het Hof van Justitie

aangehaalde eerste element (geen differentiatie op grond van de personen). Alle Europese landen waarmee contact werd opgenomen, zijn tot dezelfde conclusie gekomen.

Noch in het arrest van het Grondwettelijk Hof, noch in dat van het Hof van Justitie van de EU wordt evenwel geconcludeerd dat slechts één van de vier elementen volstaat om een schending van het evenredigheidsbeginsel in te houden. Indien dit het geval zou zijn en aangezien het gebrek aan differentiatie tussen de personen het essentiële element vormt van de vernietigde Europese en nationale wetgeving, kan worden gedacht dat het Hof van Justitie en het Grondwettelijk Hof enkel dit aspect zouden hebben onderzocht en tot een schending van het recht op eerbiediging van de persoonlijke levenssfeer zouden hebben besloten zonder de andere elementen te onderzoeken.

In voormeld advies over onderhavig wetsontwerp steunt de Commissie deze interpretatie en stelt ze: ‘evenwel wordt, zoals de Memorie van toelichting aangeeft, in geen van beide arresten geconcludeerd dat slechts één van de vier elementen volstaat om een schending van het evenredigheidsbeginsel in te houden. Indien een bepaald element van de arresten niet kan worden weerhouden, dient dit gecompenseerd te worden door een striktere regeling inzake de andere aspecten.’

De verschillende elementen aangehaald door het Hof van Justitie van de EU en het Grondwettelijk Hof moeten dan ook worden gecombineerd. Aangezien het beginsel van de veralgemeende bewaring (met andere woorden zonder differentiatie tussen de personen) van de communicatiegegevens op zich een zeer belangrijke beperking van het recht op eerbiediging van de persoonlijke levenssfeer vormt, moet dit element worden ‘gecompenseerd’ door een striktere regeling inzake de andere aspecten.”

3.1.2. In verband met de onmogelijkheid om alleen gegevens aangaande bepaalde personen, of aangaande bepaalde groepen van personen te bewaren, meer bepaald aangaande personen die al betrokken zouden zijn bij een onderzoek, welke onmogelijkheid eveneens vastgesteld is door de Commissie voor de bescherming van de persoonlijke levenssfeer in haar advies over de ontworpen tekst, is het de afdeling Wetgeving niet duidelijk om welke redenen de in de memorie van toelichting gegeven verantwoording in twijfel zou kunnen worden getrokken. Bijvoorbeeld, indien voor de operatoren en de aanbieders geen enkele algemene verplichting zou gelden tot bewaring van gegevens, zou de regeling die daarvan het gevolg zou zijn impliceren dat de bewaring van en de toegang tot de gegevens alleen *a posteriori* mogelijk zouden zijn, terwijl de overheid geen toegang zou kunnen hebben tot de gegevens uit het verleden (of de *a priori*-gegevens) die nochtans noodzakelijk of zelfs onontbeerlijk zijn voor het halen van de legitieme doelstellingen bepaald in de ontworpen tekst.

Zo ook is het, in verband met een eventuele beperking van de bewaringsplicht tot een bepaalde geografische zone of een bepaalde periode, voor de afdeling Wetgeving niet duidelijk om welke redenen de in de memorie van toelichting gevolgde redenering in twijfel zou kunnen worden getrokken. Wat deze laatste twee beperkingen betreft, rijst evenwel de vraag of niet zou kunnen worden overwogen om, zonder afbreuk te doen aan de nagestreefde legitieme doelstellingen, een kortere algemene bewaartermijn te bepalen en tegelijk een regeling in te voeren waarbij de Koning, mits voorzien wordt in bepaalde procedurele waarborgen,⁸ zou kunnen worden gemachtigd om in objectieve omstandigheden van een specifieke potentiële bedreiging die nauwkeurig moeten worden afgebakend, de bewaartermijn van de gegevens te verlengen

⁸ Bijvoorbeeld bij een besluit vastgesteld na overleg in de Ministerraad dat vooraf voor advies is voorgelegd aan de Commissie voor de bescherming van de persoonlijke levenssfeer en aan het Instituut.

(waarbij de wetgever evenwel een bovengrens vaststelt voor die verlenging van de termijn) en om, in voorkomend geval, gelet op de aard of de omvang van de bedreiging, meteen ook een bepaalde geografische zone af te bakenen.

Wat, ten slotte, de beperking betreft tot bepaalde beroepen in het kader van de beoefening waarvan een beroepsgeheim geldt, kan los van de in de memorie van toelichting vermelde gegevens niet worden uitgesloten dat de beoefenaars van deze beroepen dezelfde dienst voor elektronische communicatie gebruiken zowel voor privécommunicaties, of in het algemeen voor communicaties die niet onder het beroepsgeheim vallen, als voor communicaties die wel onder het beroepsgeheim vallen. Gelet op die mogelijkheid, komt het er dus niet zozeer op aan te voorzien in een beperking van de te bewaren gegevens, maar te voorkomen dat die gegevens worden bekendgemaakt in omstandigheden die, voor zover het gaat om gegevens die onder het beroepsgeheim vallen, niet in overeenstemming zouden zijn met de beginselen ter zake.

3.1.3. Hoewel er duidelijk logica zit in de redenen waarom de steller van het voorontwerp verklaart dat het hem onmogelijk is tegemoet te komen aan de meest strikte uitlegging van de hier bedoelde vereisten, neemt zulks niet weg dat de ontworpen tekst er per definitie niet toe strekt aan die vereisten te voldoen, wat het dispositief blootstelt aan kritiek.

De mate waarin het dispositief aan kritiek blootstaat, hangt evenwel af van de draagwijdte die dient te worden toegekend aan de arresten in kwestie en dan vooral aan het arrest van het Hof van Justitie.

Wat het laatstgenoemde arrest betreft, heeft de Raad van State van Frankrijk het volgende opgemerkt:

“L’arrêt *Digital Rights Ireland*, dont la Cour n’a pas différé les effets, soulève deux questions: celle de la possibilité de continuer à appliquer les législations nationales sur la conservation des données et celle du cadre qui devrait être défini pour se substituer à la directive n° 2006/24/CE. Les deux questions procèdent en réalité d’une même interrogation sur l’interprétation de l’arrêt. De manière schématique, deux lectures peuvent en être faites: celle d’une condamnation de l’insuffisance des garanties prévues par la directive; celle d’une condamnation de tout système de conservation générale des métadonnées, quel qu’il soit.

[...]

La première interprétation de cet arrêt peut se fonder sur le fait que la Cour a fait masse de trois éléments pour juger que le principe de proportionnalité était méconnu, et que le second avait trait à l’absence de toute précision sur les conditions d’accès des États aux métadonnées conservées par les opérateurs.

Selon cette interprétation, si la directive avait fixé des garanties concernant l’accès, l’appréciation de la Cour aurait peut-être été différente. Elle aurait également pu être influencée par l’existence de restrictions concernant la conservation, par exemple une durée maximale plus courte que celle de deux ans fixée par la directive. Les conclusions de l’avocat général peuvent conforter une telle interprétation. L’avocat général déplore le fait que la directive n’ait défini ni la nature des infractions pouvant justifier l’accès aux métadonnées, ni les autorités pouvant obtenir cet accès, ni les garanties relatives à l’effacement des données par les autorités après leur utilisation et à l’information des personnes concernées (§ 125 à 129 des conclusions). Il relevait aussi qu’il y avait une différence entre une durée de conservation se mesurant en mois et une durée se mesurant

en années (§ 148). Cependant, si la Cour est parvenue à la même solution que l'avocat général, la construction de son raisonnement est assez différente, et il n'est donc pas évident que les conclusions permettent d'éclairer la portée de l'arrêt sur la condamnation du système de conservation en tant que tel.

La seconde interprétation se fonde en premier lieu sur ce que deux des trois éléments pris en compte par la Cour pour juger que le principe de proportionnalité est méconnu tiennent au caractère général et indiscriminé de la conservation: dans le premier élément, la Cour critique le fait que les métadonnées de tous les utilisateurs des communications soient collectées, indépendamment de l'existence d'un soupçon quant à la participation à une infraction grave; dans le troisième élément, c'est le fait que la durée de conservation soit fixée de manière indiscriminée qui est contesté. C'est donc le caractère systématique et uniformément durable de la conservation des métadonnées qui est en cause. En second lieu, l'arrêt qualifie sévèrement la conservation systématique des métadonnées, en y voyant une 'ingérence particulièrement grave' dans les droits garantis par les articles 7 et 8 de la Charte, l'absence d'information des intéressés étant en outre 'susceptible de générer dans l'esprit des personnes concernées (...) le sentiment que leur vie privée fait l'objet d'une surveillance constante'. Si la Cour admet que la conservation préventive des données poursuit un but d'intérêt général, elle juge que l'ingérence ne peut être admise que si elle est proportionnée.

À l'issue de son contrôle de proportionnalité, elle conclut que la directive 'comporte une ingérence dans des droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire' (§ 65). On peut donc en déduire que l'ingérence résultant d'un système de conservation systématique peut difficilement être considérée comme limitée au strict nécessaire".⁹

Dat het moeilijk is om een duidelijke draagwijdte te kennen aan het arrest van het Hof van Justitie en het feit dat een van de mogelijke interpretaties van dit arrest afbreuk doet aan het beginsel zelf van de verplichting om *a priori*-gegevens te bewaren zijn trouwens als volgt aan bod gekomen in de rechtsleer:

"[...] il est difficile de voir quelle garantie pourrait être prévue pour répondre à ce défaut de l'instrument sans changer fondamentalement le principe même de la conservation a priori contenu dans la directive. Cette partie du raisonnement de la Cour laisse donc perplexe: d'un côté, la Cour semble insister sur le fait que l'important est d'apporter des garanties compensatoires mais en même temps une des 'garanties' à apporter remet en cause le principe même contenu dans la directive.

La Cour ne facilite donc pas l'intervention du législateur européen¹⁰ pour 'réparer' la directive 2006/24/CE: faut-il changer complètement d'approche voire abroger purement et simplement la directive (mais alors pourquoi la Cour ne l'a-t-elle pas clairement exprimé) ou cette critique adressée à la directive rend-elle seulement les autres garanties évoquées par la Cour d'autant plus importantes?

⁹ "Les rapports du Conseil d'État – Le numérique et les droits fondamentaux", bron: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>, 198-201.

¹⁰ De Europese Commissie heeft tot op heden geen enkel officieel initiatief genomen dat strekt tot opheffing of wijziging van richtlijn 2006/24/EG.

Ces questions rendent le sort du dossier très incertain”.¹¹

3.1.4. De steller van het voorontwerp heeft voor de eerste van de twee hierboven vermelde interpretaties gekozen en heeft in dat verband tegelijk gepoogd in vergelijking met de opgeheven wet¹² strengere vereisten en voorwaarden te verbinden aan de ingevoerde regeling wat betreft de garantie van vertrouwelijkheid en beveiliging van de gegevensbewaring, de procedure en de termijn gedurende welke de gegevens toegankelijk zijn, de bedoeling van deze toegang tot de gegevens en de overheden die gemachtigd zijn om toegang te hebben tot de gegevens alsook wat betreft de vernietiging van de gegevens zodra de bewaartermijn verstreken is, en daarbij schrijft hij bijzondere beschermingsmaatregelen voor met betrekking tot de gegevens die verband houden met de uitoefening van bepaalde beroepen die onder het beroepsgeheim vallen.¹³

Tot staving van die soepeler interpretatie kan voornamelijk in aanmerking worden genomen dat het Hof van Justitie in zijn arrest het beginsel van de *a priori*-bewaring van gegevens niet uitdrukkelijk veroordeeld heeft, aangezien het heeft vastgesteld dat dit beginsel geen afbreuk deed aan de wezenlijke inhoud van de fundamentele vrijheden die in het geding zijn en tegemoetkomt aan een doelstelling van algemeen belang, namelijk de bescherming van de openbare veiligheid.¹⁴

De veroordeling van de *a priori*-bewaring van gegevens op zich, als daarbij geen onderscheid zou worden gemaakt wat betreft de onderscheiden wijzen waarop wordt gecommuniceerd en wat betreft de omstandigheden en de personen in kwestie, blijkt niet uit de latere rechtspraak van het Hof van Justitie. In die zin blijkt uit het arrest-Schrems van 6 oktober 2015¹⁵ dat er alleen strijdigheid is met het recht van de Europese Unie, wanneer die veralgemeende gegevensbewaring gepaard gaat met de omstandigheid dat er geen objectief criterium bestaat voor de toegang van de overheden tot de aldus bewaarde gegevens en voor het gebruik ervan:

“Niet beperkt tot het strikt noodzakelijke is dan ook een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie

¹¹ S. DE BILLEY en A. WEYEMBERGH, “Chronique de jurisprudence consacrée à l’espace de liberté, de sécurité et de justice II – Jurisprudence de la Cour de justice relative à la coopération policière et judiciaire en matière pénale (2009-2014)” in *Cahiers de droit européen*, 50^e jaargang (2014), nr. 2, 430-434. Zie ook P.-Y. DETHY, noot onder HvJEU 8 april 2014, C-293/12, *Digital Rights Ireland Ltd* en C-594/12, *Kärntner Landesregierung e.a.*, “Quelques réflexions sur l’arrêt C-293/12 et C-594/12”, *Revue du droit des industries de réseau*, 2014/3, 338-349.

¹² De steller van het voorontwerp sluit zich aldus aan bij de aanbevelingen van de Raad van State van Frankrijk die het volgende stelt: “L’arrêt de la C.J.U.E. soulève la question de la conformité au droit de l’Union européenne des législations nationales, telles que la législation française, qui prévoient une telle obligation de conservation générale des données de connexion. Compte tenu des enjeux de la surveillance des communications pour la protection de la sécurité nationale, l’étude du Conseil d’État ne propose pas de supprimer cette obligation mais préconise de renforcer les garanties concernant l’accès et l’utilisation de ces données.” (“*Les rapports du Conseil d’État – Le numérique et les droits fondamentaux*”, bron: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>, 20).

¹³ In de hiernavolgende opmerkingen wordt elke maatregel onderzocht die in aanmerking wordt genomen voor die uitbreiding van de garanties; er wordt aangegeven wegens welke aspecten die maatregelen als ontoereikend zouden kunnen worden beschouwd in het licht van de rechtspraak van het Hof van Justitie en van het Grondwettelijk Hof en waar mogelijk worden verbeteringen voorgesteld, uiteraard binnen de grenzen van de wettigheidstoetsing die overeenkomstig de wet door de afdeling Wetgeving is verricht.

¹⁴ Zie de punten 39, 42 en 44 van het arrest C-293/12 van het Hof van Justitie van de Europese Unie, *Digital Rights Ireland Ltd*, 8 april 2014.

¹⁵ Zie HvJEU C-362/14, *Maximilian Schrems v. Data Protection commissioner*, 6 oktober 2015, punt 93.

naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens [zie in die zin, aangaande 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 elektronischecomunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (Pb.L. 105, 54), arrest *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 57-61].”

De afdeling Wetgeving stelt ten slotte dat tussen twee mogelijke interpretaties van de arresten van het Hof van Justitie en van het Grondwettelijk Hof in het licht van de rechtsregels die door beide hoven worden gehanteerd, gekozen moet worden voor de interpretatie waardoor de tegenstrijdige vereisten van het recht op eerbiediging van het privéleven van personen die gebruikmaken van elektronische communicatiemiddelen enerzijds en van de bescherming van personen die worden bedreigd door criminele praktijken van een ander anderzijds het best verzoend kunnen worden. De afdeling Wetgeving wijst er in dit verband op dat bij artikel 2 van het Europees Verdrag tot bescherming van de rechten van de mens aan de overheden de verplichting wordt opgelegd het leven van personen te beschermen tegen dergelijke praktijken,¹⁶ inzonderheid wanneer die de vorm aannemen van terrorisme.¹⁷ Artikel 8 van hetzelfde verdrag, zijnerzijds, legt onder meer de verplichting op om de seksuele integriteit van kinderen inzonderheid in relaties naar behoren te beschermen en om te voorzien in een effectieve strafbaarstelling als die integriteit wordt aangetast, terwijl de anonimiteit die de internetgebruikers gegarandeerd wordt daaraan niet in de weg mag staan. In het arrest *K.U. v. Finland* van 2 december 2008, waarin uitspraak wordt gedaan over de bescherming van een kind dat nadeel had ondervonden van een seksueel getinte advertentie die op zijn naam gepubliceerd was op een datingsite, wordt (in punt 49) het volgende gesteld:

“Une protection pratique et effective du requérant impliquait l’adoption de mesures efficaces pour identifier et poursuivre l’auteur, c’est-à-dire la personne qui avait passé l’annonce. Or pareilles mesures n’ont pas été prises. La prépondérance ayant été accordée à l’exigence de confidentialité, il n’a jamais été possible de procéder à une enquête efficace. Même si la liberté d’expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d’expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s’effacer devant d’autres impératifs légitimes tels que la défense de l’ordre et la prévention des infractions pénales ou la protection des droits et libertés d’autrui. Sans préjudice de la question de savoir si, compte tenu de sa nature répréhensible, la conduite de la personne ayant passé l’annonce illégale sur Internet relève ou non de la protection des articles 8 et 10, le législateur aurait dû en tout cas prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte”.

¹⁶ Zie EHRM, *Van Colle v. United Kingdom*, 13 november 2012.

¹⁷ Zie EHRM, beslissing *Finogenov and Others v. Russia*, 18 maart 2010, verzoekschrift 18299/03.

Niettemin zal de vraag over de werkelijke draagwijdte van arrest C-293/12, *Digital Rights Ireland Ltd* maar kunnen worden beantwoord in de toekomstige rechtspraak van het Hof van Justitie, wanneer dit Hof, zoals reeds het geval is,¹⁸ uitspraak zal moeten doen over de wetgeving ter zake van de verschillende lidstaten, inzonderheid in het licht van artikel 15, lid 1, van de richtlijn 2002/58/EG en van de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie.

3.2. De vraag of de ontworpen tekst objectieve criteria vaststelt om de toegang van de bevoegde overheden tot de gegevens en het gebruik van die gegevens overeenkomstig de nagestreefde doelstellingen af te bakenen, inzonderheid wat de procedure betreft

3.2.1. In eerste instantie dient erop te worden gewezen dat richtlijn 2006/24/EG geen enkele bepaling bevatte waarbij de toegang tot de gegevens door de overheden van de lidstaten rechtstreeks werd geregeld. Aldus werd in artikel 4 van de richtlijn alleen het volgende bepaald:

“De lidstaten nemen bepalingen aan om te waarborgen dat de overeenkomstig deze richtlijn bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde nationale autoriteiten worden verstrekt. De procedure en de te vervullen voorwaarden voor toegang tot gegevens die bewaard worden overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid, worden door elke lidstaat vastgesteld in de nationale wetgeving, rekening houdend met de relevante bepalingen van de wetgeving van de Europese Unie of publiek internationaal recht, met name het EVRM, zoals geïnterpreteerd door het Europees Hof voor de Rechten van de Mens.”

De wet van 30 juli 2013 die door het Grondwettelijk Hof is vernietigd, somde alleen de doeleinden van de bewaring op, zonder dat nauwkeurig was vastgesteld welke autoriteiten gemachtigd waren te vragen om toegang te krijgen tot de bewaarde gegevens of welke procedure daartoe moest worden gevolgd. Artikel 126, § 2, van de wet van 13 juni 2005, zoals ingevoegd bij de wet van 30 juli 2013, luidde immers als volgt:

“§ 2. De gegevens bedoeld 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;

¹⁸ Zie in dit verband het verzoek om een prejudiciële beslissing ingediend door Kamarrätten i Stockholm (Zweden) op 4 mei 2015 – Tele2 Sverige AB/Post- och telestyrelsen (Zaak C-203/15) (*Pb.C.* 2015, afl. 221/06), waarin door het Zweedse gerecht de volgende prejudiciële vragen worden gesteld:

“1) Is een algemene verplichting (zoals beschreven [in het verzoek om een prejudiciële beslissing]), om met het oog op wetshandhaving op strafrechtelijk gebied verkeersgegevens te bewaren, welke verplichting zich zonder enig onderscheid, enige beperking of uitzondering uitstrekt tot alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, verenigbaar met artikel 15, lid 1, van richtlijn 2002/58/EG(1), gelezen in samenhang met de artikelen 7, 8 en 52, lid 1, van het Handvest van de Grondrechten van de Europese Unie?

2) Indien de eerste vraag ontkennend wordt beantwoord, kan de bewaring dan niettemin toegestaan zijn

a) wanneer de toegang van de nationale instanties tot de gegevens die worden bewaard, is geregeld zoals [beschreven in het verzoek om een prejudiciële beslissing],

b) wanneer de veiligheidseisen worden geregeld zoals [beschreven in het verzoek om een prejudiciële beslissing], en

c) alle relevante gegevens moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd, en daarna moeten worden gewist, zoals [beschreven in het verzoek om een prejudiciële beslissing]?”.

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 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

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

De diensten- en netwerkaanbieders bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de gegevens opgenomen in paragraaf 1, eerste lid, onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en op eenvoudig verzoek aan de autoriteiten belast met de opdrachten bedoeld in de punten a) tot d) kunnen worden meegedeeld en uitsluitend aan deze laatsten.”¹⁹

3.2.2. De ontworpen tekst strekt ertoe te bepalen welke autoriteiten of instanties gemachtigd zijn te vragen om toegang te krijgen tot de bewaarde gegevens, welke de doeleinden van deze toegang zijn en, afhankelijk van het doeleinde en van degene die om toegang vraagt, voor welke periode in het verleden deze autoriteiten of instanties toegang kunnen vragen. In bepaalde gevallen, zoals wanneer een nooddienst wordt opgeroepen of men de identiteit wil achterhalen van degene van wie een kwaadwillige oproep uitgaat, worden in de ontworpen tekst ook termijnen, te rekenen vanaf een welbepaald feit, bepaald waarbinnen de aanvragen bij de operator of aanbieder moeten worden ingediend.

3.2.2.1. Met betrekking tot de doelstellingen die erin bestaan actie te ondernemen om gevolg te geven aan een oproep naar een nooddienst of een vermiste persoon op te sporen wiens fysieke integriteit in onmiddellijk gevaar is, lijkt de inmenging in de uitoefening van fundamentele vrijheden minder ver te gaan dan in het kader van een optreden van de rechterlijke macht of de inlichtingen- en veiligheidsdiensten teneinde, naargelang het geval, inbreuken te voorkomen en te bestraffen of in het geheim inlichtingen in te winnen. Hetzelfde geldt wanneer een officier van gerechtelijke politie van het Instituut toegang vraagt met het oog op het opsporen, onderzoeken en vervolgen van schendingen van de artikelen 114 en 124 en het ontworpen artikel 126 van de wet van 13 juni 2005, aangezien het doeleinde er dan juist in bestaat te waarborgen dat de operatoren en de aanbieders de desbetreffende bepalingen naleven en dat zodoende de fundamentele rechten van de gebruikers in acht worden genomen.

¹⁹ In artikel 126, § 5, 3°, dat bij de vernietigde wet in de wet van 13 juni 2005 werd ingevoegd, werd voorts bepaald dat de aanbieders in kwestie moesten “garande[ren] dat de toegang tot de bewaarde gegevens enkel gebeurt door een of meer leden van de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 houdende de modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie en door het personeel en de aangestelden van deze aanbieders die specifiek door deze cel gemachtigd zijn”. In tegenstelling tot wat uit het arrest van het Grondwettelijk Hof (B.10.3) zou kunnen worden afgeleid, werden daarmee niet de bevoegde “autoriteiten” bedoeld die gemachtigd zijn om tot de bewaarde gegevens toegang te hebben, maar wel de personeelsleden van de operator of aanbieder in kwestie, die gemachtigd worden toegang te hebben tot de gegevens om ze aan de autoriteit te kunnen verzenden, aangezien die bepaling niet moest zorgen voor de omzetting van artikel 4, maar wel van artikel 7, c), van richtlijn 2006/24/EG.

In verband met de procedures voor de voornoemde aanvragen om toegang te krijgen, waarop de lering van het arrest van het Hof van Justitie om de hiervoor genoemde redenen *a priori* geen toepassing vindt, lijkt het niet overdreven om niet te voorzien in het voorafgaande optreden van een rechterlijke instantie of een administratieve overheid die waarborgen biedt inzake autonomie en onafhankelijkheid ten opzichte van de aanvrager van de toegang.

Dit neemt evenwel niet weg dat de procedurele waarborgen waarin de ontworpen tekst voorziet, niet toereikend blijken te zijn. In dat verband wordt verwezen naar de bijzondere opmerkingen die hierna worden gemaakt over artikel 3 van het voorontwerp (ontworpen artikel 126).

3.2.2.2. Hoewel de vraag die uitgaat van de Ombudsdienst voor Telecommunicatie volgens de ontworpen tekst alleen betrekking mag hebben op de identificatiegegevens, kan ze worden beschouwd als een meer ingrijpende aantasting van de rechten en vrijheden van de oproeper van wie de identificatie wordt gevraagd, aangezien artikel 43*bis*, § 3, eerste lid, 7°, van de wet van 21 maart 1991 'betreffende de hervorming van sommige economische overheidsbedrijven' aan de ombudsdienst de opdracht toevertrouwt om "van elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronische-communicatienetwerk of -dienst, het verzoek [te] onderzoeken om inlichtingen te krijgen over de identiteit en het adres van de gebruikers van elektronische-communicatienetwerken of -diensten die deze persoon hebben lastiggevallen, voorzover die gegevens beschikbaar zijn."²⁰

Voor de toegang tot de gegevens die aldus aan de ombudsdienst zou worden verleend, moeten in die context specifieke waarborgen gelden. Er wordt eveneens verwezen naar de bijzondere opmerkingen over artikel 3 van het voorontwerp (ontworpen artikel 126).

²⁰ Er dient op gewezen te worden dat het feit dat de aanvraag die van de ombudsdienst uitgaat, ertoe kan leiden dat de identiteit en het adres van de oproeper worden meegedeeld aan een particulier, en niet aan een autoriteit, voortvloeit uit het voornoemde artikel 43*bis*, welke bepaling bij het voorontwerp niet wordt gewijzigd en die, samen met andere wetsbepalingen die vervat zijn in de wet van 13 juni 2005, bijdraagt tot de omzetting van artikel 10 van richtlijn 2002/58/EG, waarin met name het volgende wordt bepaald:

“De lidstaten zorgen ervoor dat er transparante procedures zijn waarin is vastgelegd hoe de aanbieder van een openbaar communicatienetwerk en/of een openbare elektronische-communicatiedienst de volgende dienstelementen kan opheffen: (...) de uitschakeling van de weergave van de identificatie van het oproepende nummer op tijdelijke basis, op verzoek van een abonnee die kwaadwillige of hinderlijke oproepen wil traceren. In dat geval worden de identificatiegegevens van de oproepende abonnee overeenkomstig de nationale wetgeving opgeslagen en beschikbaar gesteld door de aanbieder van een openbaar communicatienetwerk en/of van een openbare elektronische-communicatiedienst;”.

3.2.2.3. Voor het geval waarin de aanvraag door de gerechtelijke instanties wordt ingediend om strafbare feiten op te sporen, te onderzoeken en te vervolgen met het doel uitvoering te geven aan de maatregelen bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering, voorzien deze artikelen in een precieze procedure voor de aanvragen om toegang, op het gebied van de gegevens waartoe toegang kan worden verkregen, de motivering van de beslissing, de evenredigheid van de toegang ten aanzien van de eerbiediging van het privéleven en de subsidiariteit ten opzichte van andere onderzoeksverrichtingen, de toegangsvoorwaarden en het beroepsgeheim, hetgeen waarborgen oplevert die bij de artikelen 8 en 9 van het voorontwerp uitgebreid worden, inzonderheid door de termijn voor toegang tot de bewaarde gegevens te beperken.

Gelet op de lering die kan worden getrokken uit de arresten van het Hof van Justitie en van het Grondwettelijk Hof, moet de steller van het voorontwerp erop toezien dat de ernst van de strafbare feiten waarvoor de toegang wordt aangevraagd, beter wordt gerechtvaardigd. Op dat punt dient de steller van het voorontwerp na te gaan of het, uiteraard rekening houdend met de in acht te nemen doeleinden, niet beter zou zijn de lijst van de strafbare feiten waarvoor de toegang toegestaan wordt, te beperken door van deze strafbare feiten een nauwkeuriger opsomming te geven, zoals in artikel 90*ter* van het Wetboek van Strafvordering.²¹

Voor het overige wordt verwezen naar de bijzondere opmerkingen over de artikelen 8 en 9 van het voorontwerp.

3.3. Het feit dat de ontworpen tekst in het algemeen betrekking heeft op alle middelen voor elektronische communicatie en op alle gegevens betreffende het verkeer en het feit dat de ontworpen tekst niet voorziet in een bewaringstermijn waarbij tussen de categorieën van gegevens een onderscheid zou worden gemaakt op basis van hun eventuele nut voor de nagestreefde doelstelling of naargelang van de betrokken personen.

3.3.1. Hier rijst in de eerste plaats de vraag enerzijds te voorzien in een algemene verplichting om alle gegevens betreffende het verkeer voor alle middelen voor elektronische communicatie te bewaren en anderzijds niet te voorzien in verschillende bewaringstermijnen naargelang van de categorieën van gegevens ingedeeld op basis van hun nut, het evenredigheidsbeginsel eerbiedigen.

Zowel in het arrest van het Hof van Justitie als in het arrest van het Grondwettelijk Hof is er vóór elke andere opmerking op gewezen dat richtlijn 2006/24/EG en de Belgische wet op zeer algemene wijze betrekking hadden op alle verkeersgegevens betreffende vaste telefonie, mobiele telefonie, toegang tot internet, e-mail via internet en internettelefonie.

In antwoord op een vraag over de situatie op het vlak van gegevensbewaring in andere lidstaten van de Europese Unie, van welke situatie in de memorie van toelichting gewag

²¹ Als een dergelijke lijst kan worden opgesteld, zal deze uitgebreider kunnen zijn dan de lijst die in artikel 90*ter* is opgenomen, aangezien dat artikel betrekking heeft op een meer ingrijpende inmenging in het privéleven en de gegevensbescherming, daar de onderzoeksrechter zich op grond van die bepaling toegang mag verschaffen tot de inhoud van privécommunicatie en -telecommunicatie, daarvan kennis kan nemen en ze kan opnemen: deze bepaling staat dus de toegang tot de inhoud toe, wat niet het geval is met de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering of met de ontworpen artikelen 126 en 126/1 van de wet van 13 juni 2005.

wordt gemaakt en op welke situatie men zich wil baseren, heeft de gemachtigde van de minister aan de afdeling Wetgeving informatie bezorgd waaruit blijkt dat bepaalde lidstaten, die weliswaar een minderheid vormen, het plan hebben opgevat of overwogen om, naargelang van de aard van de gegevens, te voorzien in een verschillende aanpak op het gebied van verplichting tot en termijn van bewaring: zo zou in Duitsland de ontworpen bewaringstermijn variëren naargelang het gaat om verkeers- of om lokalisatiegegevens, waarbij voor de lokalisatiegegevens wordt voorzien in een kortere bewaringstermijn, met dien verstande dat gegevens betreffende de e-mails niet onder de bewaarplicht zouden vallen; in Nederland zou de ontworpen wetgeving voorzien in een bewaringstermijn van twaalf maanden voor telefoniegegevens en van zes maanden voor internetgegevens.

Over deze kwesties wordt in de memorie van toelichting het volgende vermeld:

“Dit ontwerp van wet voert een onderscheid in op grond van drie categorieën van gegevens.

De eerste categorie betreft de identificatiegegevens (wie is houder van een bepaald gsm-nummer, wat is het gsm-nummer van een bepaalde persoon, wie zit er achter een bepaald IP-adres, enz.). Die gegevens, worden het meest gevraagd en tasten de persoonlijke levenssfeer op matige wijze aan, in vergelijking met inzonderheid de tweede en derde categorie.

De tweede categorie betreft de verbindings- en lokalisatiegegevens (wat is inzonderheid de plaats en de duur van een communicatie).

De derde categorie betreft de persoonlijke communicatiegegevens (wie heeft gebeld of gecorrespondeerd met wie).

De tweede en derde categorie tasten de persoonlijke levenssfeer meer aan dan de eerste. De toegangen tot die gegevens zijn minder talrijk dan die tot de identificatiegegevens maar blijven frequent.

Na veelvuldige besprekingen in de Regering en met de diensten en overheden in kwestie, en na een differentiatie in de bewaringstermijnen overwogen te hebben in functie van de categorieën van gegevens, is de conclusie dat, gelet op de noodwendigheden inzake de strijd tegen terroristische misdrijven, een bewaringsperiode van 12 maanden noodzakelijk is voor elk van de 3 categorieën.”

3.3.2. Door af te stappen van het idee dat alle gegevens bewaard moeten worden of door de bewaringstermijn van de gegevens aan te passen naar gelang van de categorieën van gegevens, zou wellicht een regeling worden ingevoerd die betere waarborgen biedt om ervoor te zorgen dat de overwogen maatregelen, die een inmenging vormen in het recht op eerbiediging van het privéleven, conform aan het evenredigheidsbeginsel zijn.

Indien geopteerd zou worden voor een strikte uitlegging van de hiervoor in herinnering gebrachte vereisten, zou er dan ook van uit kunnen worden gegaan dat de ontworpen regeling blootstaat aan kritiek wegens de keuze die de steller van het voorontwerp gemaakt heeft.

In het licht van de onderscheiden doelstellingen die nagestreefd worden, en inzonderheid van de bestrijding van terrorisme en kinderpornografie, van de actie die ondernomen wordt naar aanleiding van een dringende oproep of van de opsporing van vermiste personen wier leven geacht wordt in onmiddellijk gevaar te zijn, dient evenwel te worden vastgesteld dat het de afdeling Wetgeving niet echt duidelijk is hoe die doelstellingen, die alle

gerechtvaardigd zijn, efficiënt zouden kunnen worden gehaald als bijvoorbeeld zou worden bepaald dat alleen de telefoniegegevens en niet de internetgegevens moeten worden bewaard of door te voorzien in verschillende bewaringstermijnen voor bepaalde categorieën van gegevens. Bovendien stuit de invoering van een regeling waarbij, naargelang van het doel of de betrokken personen, een verschil in behandeling wordt ingevoerd op het stuk van de bewaarplicht zelf en van de duur ervan, voorts op dezelfde hinderpalen als die welke hiervoor in opmerking 3.1. zijn vermeld.

Om ervoor te zorgen dat overwogen maatregelen conform aan het evenredigheidsbeginsel zijn, voorziet de ontworpen tekst bovendien in verschillende toegangsregelingen qua toegangstermijn en qua gegevens waarvoor de toegang wordt verleend, naargelang van het doel zelf van de toegang of van de autoriteit die om toegang verzoekt. Zo zullen de hulpdiensten bijvoorbeeld alleen toegang hebben tot de identificatiegegevens van de oproeper²², zal de toegang in het kader van de opsporing van een vermiste persoon alleen betrekking kunnen hebben op de gegevens met betrekking tot die persoon²³, en zijn de gegevens waartoe de procureur des Koning toegang kan hebben minder uitgebreid dan de gegevens waartoe de onderzoeksrechter toegang heeft²⁴. De toegangstermijn, zijnerzijds, varieert van vierentwintig uur tot twaalf maanden, waarbij in de termijn van twaalf maanden wordt voorzien voor een gerechtelijke overheid die optreedt in het kader van haar actie met betrekking tot een strafbaar feit bedoeld in titel I ter van boek II van het Strafwetboek (te weten de terroristische misdrijven) en voor inlichtingen- en veiligheidsdiensten die optreden in het kader van een terroristische of extremistische bedreiging in de zin van de wet van 30 november 1998 'houdende regeling van de inlichtingen- en veiligheidsdienst'.

Bij de ontworpen regeling wordt dus een verschil in behandeling ingevoerd naargelang van het doel de toegang en van de aanvrager van de toegang, om een grotere evenredigheid te garanderen ten aanzien van het recht op eerbiediging van het privéleven.

3.4. Het feit dat de ontworpen tekst specifieke en aangepaste regels bevat die bedoeld zijn om de volle integriteit en vertrouwelijkheid van de gegevens te waarborgen en ervoor te zorgen dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd door een bijzonder hoog niveau van bescherming en beveiliging te bieden via technische en organisatorische maatregelen

3.4.1. De steller van het voorontwerp heeft aan deze dimensie bijzondere aandacht besteed, met dien verstande dat het beter waarborgen van de volle integriteit en vertrouwelijkheid van de gegevens volgens hem de omstandigheid zou kunnen compenseren dat de ontworpen tekst onmogelijk kan voldoen aan het eerste vereiste dat door het Hof van Justitie is geformuleerd, te weten dat een onderscheid zou moeten worden gemaakt qua categorie van gegevens en qua personen, alsook qua geografische zone en quaperiode.

²² Ontworpen artikel 126, § 2, eerste lid, 4°.

²³ Ontworpen artikel 126, § 2, eerste lid, 5°.

²⁴ Vergelijk de artikelen 46bis en 88bis van het Wetboek van Strafvordering.

De maatregelen die vervat zijn in de ontworpen tekst (ontworpen artikelen 126 en 126/1) en, in voorkomend geval, in andere geldende wet- of regelgeving, kunnen als volgt worden samengevat:

1° In de eerste plaats dient de algemene wet- en regelgeving inzake de bescherming van de persoonsgegevens en de verwerking ervan te worden toegepast. In dat verband wordt bepaald dat elke betrokken operator en aanbieder wordt beschouwd als verantwoordelijke voor de verwerking in de zin van de wet van 8 december 1992 'tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van de persoonsgegevens' voor de gegevens die worden verwerkt op grond van de ontworpen artikelen 126 en 126/1.²⁵

2° In principe wordt binnen elke betrokken operator of aanbieder een Coördinatiecel opgericht²⁶ die ermee belast is aan de wettelijk bevoegde Belgische autoriteiten op hun verzoek de bewaarde gegevens te verstrekken; toegang tot de gegevens kan alleen verleend worden aan de leden van de cel²⁷ die elk het voorwerp moeten hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies²⁸, conform artikel 22*quinquies* van de wet van 11 december 1998 'betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen'²⁹, en niet het voorwerp mogen hebben uitgemaakt van een weigering door de Minister van Justitie, welke weigeringsbeslissing moet worden gemotiveerd en ten allen tijde kan worden genomen³⁰; de leden van de cel mogen, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator of de aanbieder, met dien verstande dat zowel de leden van de cel als de aangestelden die aan hen technische bijstand verlenen, onderworpen zijn aan het beroepsgeheim³¹; de operatoren en aanbieders moeten waken over de vertrouwelijkheid van de gegevens die verwerkt worden door de cel en moeten zowel het BIPT als de Commissie voor de bescherming van de persoonlijke levenssfeer op de hoogte brengen van de contactgegevens van de cel en van haar leden en van de wijzigingen van die gegevens³²; om ervoor te zorgen dat de gegevens daadwerkelijk vertrouwelijk verwerkt worden (waarbij tevens een beroepsgeheim geldt), wordt voorts voorzien in nieuwe strafbaarstellingen³³ die betrekking hebben op gedragingen die nog niet vallen onder artikel 550*bis* van het Strafwetboek, waarbij strafrechtelijke straffen worden gesteld op interne en externe hacking; wat de procedure betreft, zijn de operatoren en aanbieders verplicht om een interne procedure uit te werken om te antwoorden op de verzoeken vanwege de autoriteiten om toegang te krijgen tot de persoonsgegevens van de gebruikers; de gegevens over deze procedures,

²⁵ Ontworpen artikel 126/1, § 2, tweede lid.

²⁶ De operatoren en aanbieders kunnen ervoor kiezen een gemeenschappelijke Coördinatiecel op te richten die in dat geval moet voorzien in dezelfde dienst voor elke operator of aanbieder individueel (ontworpen 126/1, § 1, tweede lid).

²⁷ Ontworpen artikel 126, § 4, 3°.

²⁸ Het advies wordt vijf jaar na het verlenen ervan als vervallen beschouwd.

²⁹ Ontworpen artikel 126/1, § 1, derde lid, 1°.

³⁰ Ontworpen artikel 126/1, § 1, derde lid, 2°.

³¹ Ontworpen artikel 126/1, § 1, vijfde en zesde lid.

³² Ontworpen artikel 126/1, § 1, zevende lid.

³³ Ontworpen artikel 145, § 3*ter*.

over het aantal ontvangen verzoeken, over de aangevoerde rechtsgrond en over het antwoord worden op verzoek van het BIPT aan dat Instituut verstrekt³⁴; bovendien moeten de operatoren van openbare netwerken en de betrokken aanbieders artikel 114, § 2, van de wet van 13 juni 2005 in acht nemen voor de toegang tot de bedoelde gegevens en het bezorgen ervan aan de autoriteiten³⁵. Voorts wordt bepaald dat elke betrokken aanbieder en operator één of meer aangestelden voor de bescherming van persoonsgegevens moeten aanwijzen die moeten voldoen aan dezelfde voorwaarden als de leden van de Coördinatiecel; de aangestelden mogen in principe geen deel uitmaken van de cel en zij moeten in hun handelen onafhankelijk zijn, welke onafhankelijkheid inzonderheid wordt gewaarborgd door het feit dat de uitoefening van hun opdrachten voor hen geen nadelen met zich mag brengen en dat ze zonder grondige motivering niet mogen worden ontslagen of vervangen wegens de uitvoering van de taken die aan hen zijn toevertrouwd en dat ze de mogelijkheid moeten hebben om rechtstreeks te communiceren met het management of het directiecomité; deze aangestelden hebben tot taak ervoor te zorgen dat de verwerkingen door de Coördinatiecel conform de wet geschieden, dat de aanbieder of de operator alleen die gegevens verzamelt en bewaart die hij wettelijk mag bewaren, dat alleen de wettelijk gemachtigde autoriteiten toegang hebben tot de bewaarde gegevens en dat de maatregelen voor beveiliging en bescherming van de persoonsgegevens die zijn beschreven in de wet en in het veiligheidsbeleid van de aanbieder of de operator, worden uitgevoerd tenslotte deelt elke betrokken aanbieder en operator onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer de contactgegevens van de aangestelde(n) voor de bescherming van persoonsgegevens mee, alsook elke wijziging van die gegevens³⁶.

3° Met betrekking tot de veeleer technische regels die de bewaring, de vertrouwelijkheid en de vernietiging van de gegevens na afloop van de bewaringstermijn ervan moeten waarborgen, legt de de ontworpen tekst aan de operatoren en aanbieders de verplichting op te garanderen dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk, ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen onopzettelijke of onrechtmatige vernietiging, tegen onopzettelijk verlies of onopzettelijke wijziging, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, van bij hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er inzage in te hebben, en ervoor

³⁴ Ontworpen artikel 126/1, § 2, eerste lid.

³⁵ Ontworpen artikel 126/1, § 2, derde lid. Artikel 114, § 2, van de wet van 13 juni 2005 luidt als volgt:

“Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zorgen de in de eerste paragraaf bedoelde maatregelen die genomen worden door de ondernemingen die openbare elektronische-communicatiediensten aanbieden wanneer het persoonsgegevens betreft, ervoor dat in ieder geval:

– wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens;

– opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; en - een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Het Instituut kan de door de aanbieders van openbare elektronische-communicatiediensten genomen maatregelen controleren en aanbevelingen formuleren over de beste praktijken betreffende het beveiligings-peil dat met deze maatregelen moet worden gehaald.”

³⁶ Ontworpen artikel 126/1, § 3.

te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt, zoals vastgelegd in het ontworpen artikel 126, § 3, worden verwijderd van elke drager, onverminderd de artikelen 122 en 123 van de wet van 13 juni 2005; ten slotte moeten ze ervoor zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit die hiertoe is gemachtigd; deze opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek dat het BIPT en de Commissie voor de bescherming van de persoonlijke levenssfeer mogen raadplegen of waarvan ze een volledige of gedeeltelijke kopie mogen eisen.³⁷

3.4.2. Uit het voorgaande volgt dat met het ontwerp een bijzonder sterk uitgewerkte en alomvattende regeling wordt ingevoerd die zowel in rechte als in feite de volle integriteit en vertrouwelijkheid van de gegevens waarborgt en garandeert dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd welke regeling gekenmerkt wordt door “een bijzonder hoog niveau van bescherming en beveiliging” dat tot stand gebracht wordt door “technische en organisatorische maatregelen”.³⁸

Om volledig tegemoet te komen aan de vereisten waaraan volgens het arrest van het Hof van Justitie in dat verband moet worden voldaan, zou het ontwerp evenwel op enkele punten moeten worden herzien.

3.4.2.1. Uit het ontworpen artikel 126/1, § 1, vierde lid, blijkt dat de Koning gemachtigd is om bij een besluit vastgesteld na overleg in de Ministerraad bepaalde categorieën van operatoren en aanbieders vrij te stellen van de verplichting om te voldoen aan de vereisten die wat de leden van de Coördinatiecél betreft, worden gesteld in het derde lid van dezelfde paragraaf, in verband met het veiligheidsadvies en een niet-weigering van de Minister van Justitie, of om voor die categorieën minder strikte voorwaarden vast te stellen.

In de bespreking van het artikel wordt daaromtrent het volgende gezegd:

“Er moet echter rekening worden gehouden met het feit dat afhankelijk van de evolutie van de actoren, het wetsontwerp van toepassing kan zijn op kleine aanbieders of operatoren, voor wie sommige van deze verificaties disproportioneel worden. Het wetsontwerp voorziet dus in de mogelijkheid om bepaalde categorieën van operatoren of aanbieders vrij te stellen van deze verplichtingen of voorwaarden.”

Bovendien bepaalt artikel 126/1, § 3, tweede lid, dat de Koning bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, mag bepalen bij welke categorieën van aanbieders of operatoren de aangestelde voor de bescherming van de persoonsgegevens wel lid mag zijn van de Coördinatiecél.³⁹

³⁷ Ontworpen artikel 126, § 4.

³⁸ HvJ, C-293/12, *Digital Rights Ireland Ltd*, punt 67.

³⁹ Op het eerste gezicht lijken die machtigingen herhaald te worden in artikel 126/1, § 4, 1° en 4°. Wat betreft de bedoeling van de steller van het voorontwerp en de problemen die ontstaan door de cumulatie of de dubbele vermelding van al deze machtigingen die aan de Koning worden verleend, wordt verwezen naar de bijzondere opmerkingen die hierna worden gemaakt met betrekking tot artikel 5 van het voorontwerp.

In de bespreking van het artikel wordt daaromtrent het volgende gezegd:

“Er moet echter rekening worden gehouden met het feit dat afhankelijk van de evolutie van de actoren, het wetsontwerp van toepassing kan zijn op kleine aanbieders of operatoren, voor wie deze incompatibiliteit, die inhoudt dat twee verschillende personen moeten worden aangewezen voor de Coördinatiecél en voor de functie van aangestelde voor de bescherming van de gegevens, disproportioneel wordt. Het wetsontwerp voorziet dus in de mogelijkheid om een uitzondering te maken voor sommige categorieën van operatoren of aanbieders.”

Hoewel het doel dat door de steller van het voorontwerp wordt nagestreefd, namelijk dat geen onevenredige of onmogelijk na te komen verplichtingen worden opgelegd aan operatoren en aanbieders die over weinig personeel beschikken, als legitiem kan worden beschouwd, mag de ingevoerde regeling er niet toe leiden dat de personen op wie de bewaarde gegevens betrekking hebben, verstoken blijven van een aantal waarborgen die het voorontwerp aan hen biedt op het stuk van de bescherming van een fundamenteel recht, het recht op eerbieding van het privéleven, louter en alleen omdat de operator of de aanbieder die die gegevens bewaart, “klein” is.

Het ontwerp moet aldus worden herzien dat iedereen vergelijkbare waarborgen krijgt ongeacht de grootte van de betrokken operatoren of aanbieders, bijvoorbeeld onder meer via de mogelijkheid die het ontwerp reeds aan de operatoren biedt om een gemeenschappelijke Coördinatiecél op te richten.

Het staat hoe dan ook aan de wetgever om te bepalen met welke criteria de Koning rekening moet houden om uitvoering te geven aan de hem verleende machtiging.

3.4.2.2. Het ontworpen artikel 126, § 4, 6°, bepaalt dat de gegevens na afloop van de bewaringstermijn van elke drager moeten worden verwijderd.

3.4.2.2.1. Die verwijdering vindt evenwel plaats “onverminderd de artikelen 122 en 123”.

In de bespreking van het artikel wordt daaromtrent het volgende uiteengezet: “Men kan immers niet uitsluiten dat een aanbieder of operator slechts één databank heeft aangelegd in het kader van de artikelen 122, 123 en 126. In dat geval zal een gegeven niet worden vernietigd op grond van artikel 126 als die nog kan worden bewaard op basis van de artikelen 122 en 123 van de wet.”

De vraag rijst of het niet beter zou zijn te bepalen dat de gegevens die krachtens het ontworpen artikel 126 bewaard worden, bewaard moeten worden in een databank die enkel bedoeld is voor die gegevens om het gevaar dat de desbetreffende gegevens niet verwijderd worden zoveel mogelijk in te perken.

3.4.2.2.2. De ontworpen bepalingen zouden beter tegemoetkomen aan de vereisten inzake de onherroepelijke vernietiging van de gegevens indien een overheidsinstantie, zoals het BIPT, specifiek belast zou worden met de controle op de daadwerkelijke en onherroepelijke vernietiging van de gegevens.

Weliswaar is het BIPT krachtens artikel 14, § 1, 3°, van de wet van 17 januari 2003 'met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector' in het algemeen belast met het toezicht op de naleving van de wet van 13 juni 2005 in haar geheel en kan de Koning aan de statutaire personeelsleden van het Instituut de hoedanigheid verlenen van officier van gerechtelijke politie, die overeenkomstig de artikelen 24 en 25 van dezelfde wet van 17 januari 2003 over heel wat bevoegdheden beschikt. Bovendien verleent het ontworpen artikel 126, § 2, eerste lid, 3° aan elke officier van gerechtelijke politie van het BIPT toegang tot de desbetreffende gegevens met het oog op het opsporen, het onderzoek en de vervolging van onder meer inbreuken op het ontworpen artikel 126.

De afdeling Wetgeving wijst er evenwel op dat bijvoorbeeld in geen enkele strafbaarstelling is voorzien met betrekking tot het niet vernietigen van gegevens na het verstrijken van de bewaartermijn. Zo ook verplicht geen enkele bepaling het BIPT om op dat vlak regelmatig specifieke controles uit te voeren. Zulke bepalingen zouden evenwel een grotere garantie bieden dat de gegevens daadwerkelijk vernietigd worden.

3.4.2.2.3. De ontworpen tekst dient in het licht van deze opmerkingen te worden herzien.

3.5. Het feit dat het ontwerp de verplichting wordt opgelegd, om de desbetreffende gegevens op het grondgebied van de Unie te bewaren.

Luidens het ontworpen artikel 126, § 4, 4°, moeten de betrokken aanbieders en operatoren “de gegevens op het grondgebied van de Europese Unie (...) bewaren”.

BIJZONDERE OPMERKINGEN

INDIENINGSBESLUIT

Het indieningsbesluit dient te worden gesteld als volgt:

“FILIP, Koning der Belgen,

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

Op de voordracht van de Minister van Digitale Agenda, Telecommunicatie en Post, van de Minister van Justitie en van de Minister van Defensie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De Minister van Digitale Agenda, Telecommunicatie en Post, de Minister van Justitie en de Minister van Defensie 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.”⁴⁰

DISPOSITIEF

Artikel 4

1. Artikel 4 van het voorontwerp strekt ertoe artikel 126 van de wet van 13 juni 2005 te vervangen.

Naast de bovenstaande algemene opmerkingen, behoren bij die bepaling de volgende opmerkingen te worden gemaakt.

1.1. Het ontworpen artikel 126, § 2, eerste lid, bepaalt dat de operatoren en aanbieders de gegevens mededelen op “eenvoudig verzoek” van de overheden die toegang kunnen krijgen tot die gegevens om de redenen die in die bepaling worden opgesomd en binnen de termijn die hun daartoe eventueel is toegemeten.

In de bespreking van het artikel staat in dat verband het volgende: “Dit betekent geenszins dat de voorwaarden die opgenomen zijn in bijvoorbeeld de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering, niet moeten worden vervuld. Dit betekent daarentegen dat de aanbieder of de operator die in België communicatiediensten verstrekt, de gegevens moet leveren die worden gevraagd door de Belgische overheden op het Belgische grondgebied, zonder dat zij een rogatoire commissie moeten sturen”.

1.2. Wat anderzijds de aanvragen betreft die krachtens het ontworpen artikel 126, § 2, eerste lid, 4°, door de hulpdiensten worden gedaan, wordt de betrokken aanbieder of operator verplicht “een voorafgaande controle [...] van de identiteit van de hulpdiensten” uit te voeren. In de bespreking van het artikel wordt daarvoor de volgende uitleg gegeven:

“Deze paragraaf verplicht de operator of aanbieder [...] wel om met deze hulpdiensten een veiligheidsmechanisme overeen te komen om te vermijden dat derden, die misbruik zouden maken van de identiteit van de nooddiensten die ter plaatse hulp bieden, op illegale wijze bewaarde gegevens in handen kunnen krijgen. Het spreekt voor zich dat de hulpdiensten die ter plaatse hulp bieden en de operatoren samen veiligheidsmechanismen moeten overeenkomen, waarbij elke partij haar verantwoordelijkheid neemt om een misbruik van identiteit te voorkomen”.

Hoewel bij de ontworpen regeling geen enkele vergelijkbare verplichting wordt opgelegd in het geval van een aanvraag komende van de Cel Vermiste Personen van de federale politie, wordt in de bespreking van het artikel daarover niettemin het volgende gezegd:

“Net zoals het geval is voor de samenwerking met de hulpdiensten die ter plaatse hulp bieden, komen de operatoren en de Cel vermiste personen van de federale politie modaliteiten of praktische procedures overeen teneinde te garanderen dat de operatoren effectief in contact staan met de bevoegde officier van de gerechtelijke politie.”

⁴⁰ *Beginnelsen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbeveling 226 en 227, formule F 5.

2. Gelet op de bewoordingen waarin de bepaling is gesteld, en gelet op de bovenstaande uitleg gegeven in de bespreking van het artikel, geeft de voorliggende bepaling aanleiding tot de volgende opmerkingen.

Ingeval een aanvraag steunt op een handeling van een gerechtelijke overheid of van de inlichtingendiensten, moet die handeling, per definitie, en krachtens de ontworpen tekst,⁴¹ al beantwoorden aan de voorwaarden die, naargelang het geval, worden opgesomd in de artikelen 46*bis* of 88*bis* van het Wetboek van Strafvordering of in de relevante bepalingen van de wet van 30 november 1998.

In de andere gevallen wordt bij de ontworpen tekst geen enkele formele voorwaarde gesteld, en in de bespreking van de artikelen wordt, overigens alleen voor bepaalde gevallen,⁴² gezegd dat enerzijds de aanbieders en de operatoren, en anderzijds de overheden die toegang vragen tot de gegevens, de modaliteiten en praktische procedures moeten uitwerken om zich ervan te vergewissen dat de aanvraag wel degelijk uitgaat van een gemachtigde overheid.

De beoordeling van een kwestie die dermate belangrijk is bij het voorkomen van onregelmatige en onrechtmatige aanvragen en die als doel heeft te vermijden dat een niet gemachtigd persoon toegang zou kunnen hebben tot de bewaarde gegevens, mag niet worden overgelaten aan de betrokkenen. Bovendien kan ook niet zonder meer worden bepaald dat de aanbieder of de operator, die beide helemaal geen politiebevoegdheid hebben en die ook niet kunnen krijgen, “een voorafgaande controle [...] van de identiteit van de hulpdiensten” uitvoeren, zoals in de ontworpen tekst staat.

De ontworpen tekst dient dan ook zodanig te worden aangevuld dat daarbij, tenminste voor de gevallen waar die garantie niet reeds voortvloeit uit andere wetsbepalingen, de Koning uitdrukkelijk wordt gemachtigd de inhoud en de vorm van de aanvraag vast te leggen, zodat de operatoren en de aanbieders op basis van die aanvraag er zeker van mogen zijn dat ze wel degelijk uitgaat van een overheid of een persoon die gemachtigd is om toegang tot de gegevens te vragen voor de doeleinden waarvoor en onder de voorwaarden waaronder het ontworpen artikel 126 die toegang toestaat.

Bijgevolg dient de laatste zin van het ontworpen artikel 126, § 2, eerste lid, 4°, te worden weggelaten en dient de bespreking van het artikel te worden herzien. De machtiging die bij het ontworpen artikel 126/1, § 4, 6°,⁴³ aan de Koning wordt verleend, dient eveneens te worden herzien en dient te worden aangevuld in het licht van deze opmerkingen.

⁴¹ Zie de woorden “en volgens de voorwaarden bepaald in die artikelen”, die worden gebruikt in het ontworpen artikel 126, § 2, eerste lid, 1° en 2°.

⁴² In de ontworpen tekst wordt niets gezegd in verband met de aanvragen uitgaande van de Ombudsdienst voor telecomunicatie, en dat terwijl de aanvraag van die dienst volgt op een klacht van “elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een [...] netwerk of dienst” en, bijgevolg, op een verzoek van een privépersoon en niet van een overheid.

⁴³ Die bepaling machtigt de Koning tot het vaststellen van “de overige regels die de samenwerking van de operatoren en van de aanbieders bedoeld in artikel 126, § 1, eerste lid, met de Belgische autoriteiten of met sommige van hen, regelen, voor de verstrekking van de in paragraaf 1 beoogde gegevens”.

Artikel 5

Los van de bovenstaande algemene opmerkingen en onder voorbehoud daarvan, behoren bij de voorliggende bepaling de volgende opmerkingen te worden gemaakt.

1. Zoals hierboven vermeld, bepaalt het ontworpen artikel 126/1, § 1, vierde lid, dat “de Koning (...), bij een in Ministerraad overlegd besluit, [kan] beslissen dat bepaalde categorieën van operatoren of aanbieders niet onderworpen zijn aan de voorwaarden die worden beoogd in het derde lid⁴⁴ of (...) voor deze categorieën minder strikte voorwaarden [kan] vastleggen”.

Het ontworpen artikel 126/1, § 3, tweede lid, dat betrekking heeft op de “aangestelde voor de bescherming van de persoonsgegevens” bepaalt zijnerzijds:

“Deze aangestelde mag geen deel uitmaken van de Coördinatiecel. De Koning mag evenwel, bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de categorieën bepalen van aanbieders of operatoren waarvoor deze onverenigbaarheid niet van toepassing is”.

De bepalingen onder 1° en 4° van het ontworpen artikel 126/1, § 4, luiden dan weer als volgt:

“§ 4. De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut:

1° de categorieën van operatoren en de categorieën van aanbieders bedoeld in artikel 126, § 1, eerste lid, die zijn vrijgesteld van bepaalde eisen vastgelegd in paragraaf 1;

(...)

4° de categorieën van aanbieders bedoeld in artikel 126, § 1, eerste lid, en de categorieën van operatoren bedoeld in artikel 126, § 1, eerste lid, die zijn vrijgesteld van de naleving van een deel of van het geheel van paragraaf 3;”.

Die bepalingen zijn problematisch om de volgende redenen:

Als de machtigingen die zijn opgenomen in paragraaf 4, 1° en 4°, enkel tot doel hebben de machtigingen in herinnering te brengen die respectievelijk verleend worden in paragraaf 1, vierde lid, en paragraaf 3, tweede lid,

1° zijn ze enerzijds een herhaling ervan en bijgevolg overbodig;

2° verschillen ze anderzijds hoe dan ook van de machtigingen die ze in herinnering zouden moeten brengen;

– wordt in paragraaf 4, naast het overleg in de Ministerraad voorgeschreven in paragraaf 1, vierde lid, het advies vereist van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het BIPT;

⁴⁴ Namelijk de verplichting dat de leden van de Coördinatiecel over een niet-achterhaald positief veiligheidsadvies beschikken en niet geweigerd zijn door de Minister van Justitie.

– is paragraaf 4, 1° gesteld in vage bewoordingen in zoverre hij de Koning de mogelijkheid biedt de categorieën van aanbieders en operatoren te bepalen die zijn vrijgesteld van “bepaalde eisen vastgelegd in paragraaf 1”, terwijl paragraaf 1, vierde lid, nauwkeuriger is geformuleerd, aangezien daarbij aan de Koning de mogelijkheid wordt geboden de categorieën te bepalen die “niet onderworpen zijn aan de voorwaarden die worden beoogd in het derde lid” of “voor deze categorieën minder strikte voorwaarden” vast te leggen;

– wordt in paragraaf 4, 4° de Koning gemachtigd categorieën te bepalen van aanbieders en operatoren “die zijn vrijgesteld van de naleving van een deel of van het geheel van paragraaf 3”, terwijl de eventuele vrijstelling zoals bedoeld in paragraaf 3, tweede lid, enkel betrekking heeft op het vereiste dat de aangestelde voor de bescherming van persoonsgegevens geen lid mag zijn van de Coördinatiecél.

Als de machtigingen vervat in paragraaf 4, 1° en 4°, tot doel hebben aan de Koning de bevoegdheid te verlenen om te voorzien in andere vrijstellingen en afwijkingen dan die waarin respectievelijk al in paragraaf 1, vierde lid, en paragraaf 3, tweede lid is voorzien⁴⁵, moet worden vastgesteld dat wat die machtigingen betreft, niet wordt gepreciseerd wie wordt vrijgesteld en waarvan juist vrijstelling wordt verleend.

Wat ook de bedoeling is van de steller van het voorontwerp, hij dient de aldus gesignaleerde dubbelzinnigheden of contradicties weg te werken zodanig dat, onder voorbehoud van de bovenstaande algemene opmerkingen, het voorwerp van die machtigingen welomlijnd en duidelijk is, waarbij hij overlapping tussen de verschillende machtigingen die hij wenst te verlenen moet vermijden. Zoals overigens reeds is opgemerkt, moet de wetgever de criteria bepalen die de Koning moet hanteren wanneer hij zijn machtiging ten uitvoer legt, alsook het precieze voorwerp ervan, teneinde te waarborgen dat het gelijkheidsbeginsel en het recht op de eerbiediging van de persoonlijke levenssfeer van de personen van wie de gegevens worden bewaard, in acht worden genomen.

De voorliggende bepaling moet dienovereenkomstig worden herzien.

2. In het ontworpen artikel 126/1, § 3, vijfde lid, dient te worden verduidelijkt wat moet worden verstaan onder het begrip “management”.

Artikel 8

1. De vraag rijst wat de exacte strekking is van de beperking zoals bedoeld in het ontworpen artikel 46bis, § 1, vierde lid, van het Wetboek van Strafvordering: kan de procureur des Konings toegang krijgen tot de bewaarde gegevens voor een beperkte periode van zes maanden voorafgaand aan zijn beslissing voor alle strafbare feiten behalve die welke een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben,

⁴⁵ Dat geval is geenszins uit te sluiten aangezien in de bespreking van het artikel het volgende wordt vermeld: “Paragraaf 4 van het nieuwe artikel 126/1 voorziet in een reeks delegaties aan de Koning. De punten 1° en 4° moeten de Koning in staat stellen om regels vast te stellen die aangepast zijn voor de operatoren of aanbieders die in het buitenland gevestigd zijn of die maar weinig of geen verzoeken van de overheden inzake identificatie-, verkeers- of inhoudelijke gegevens ontvangen.”

voor welke strafbare feiten de termijn wordt uitgebreid tot twaalf maanden,⁴⁶ of moet die bepaling – en zulks is waarschijnlijker – gelet op het ontworpen artikel 88*bis*, § 1, eerste lid, van het Wetboek van Strafvordering, zo worden begrepen dat aan de procureur enkel toegang wordt verleend tot die gegevens in het kader van strafbare feiten die een correctionele hoofdgevangenisstraf tot gevolg kunnen hebben, met dien verstande dat wanneer de correctionele hoofdgevangenisstraf één jaar of meer bedraagt, de termijn wordt uitgebreid tot twaalf maanden?

De voorliggende bepaling dient aldus te worden herzien dat elke dubbelzinnigheid dienaangaande wordt weggewerkt.

2. De afdeling Wetgeving vraagt zich voorts ook af waarom in de ontworpen tekst niet hetzelfde onderscheid wordt gemaakt als dat waarin is voorzien in het ontworpen artikel 88*bis*, § 2, van hetzelfde wetboek, waaruit volgt dat de toegang beperkt is tot 12 of 9 maanden naargelang de situatie een strafbaar feit betreft “bedoeld in Titel I*ter* van Boek II van het Strafwetboek”, dan wel een ander strafbaar feit zoals bedoeld in artikel 90*ter*, § 2 tot § 4 van hetzelfde wetboek, een strafbaar feit dat begaan is in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een correctionele hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben.

Volgens de uitleg die de gemachtigde van de minister heeft gegeven, zouden die verschillen tussen de twee ontworpen bepalingen voornamelijk te wijten zijn aan het feit dat bij artikel 46*bis*, § 1, van het Wetboek van Strafvordering de procureur des Konings enkel toegang krijgt tot de gegevens voor de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst voor elektronische communicatie of van het gebruikte middel voor elektronische communicatie en voor de identificatie van de diensten voor elektronische communicatie waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden, terwijl bij artikel 88*bis* van hetzelfde wetboek de onderzoeksrechter toegang krijgt tot ruimere en vollediger gegevens, aangezien de onderzoeksrechter de oproepgegevens kan laten opsporen van telecommunicatiemiddelen van waaruit of waarnaar oproepen worden of werden gedaan, alsook de oorsprong of de bestemming van telecommunicatie kan laten lokaliseren.⁴⁷

Hoewel inderdaad aanvaard kan worden dat de beperking van de toegang in de tijd zoals bepaald in het ontworpen artikel 88*bis*, § 2, en die waarin is voorzien in het ontworpen artikel 46*bis*, § 1, vierde lid, verschillen gelet op de inhoud zelf van de betrokken gegevens, moet wat betreft het verschil in behandeling niettemin met nog twee andere zaken rekening worden gehouden: vooreerst betreft artikel 46*bis* de toegang van het openbaar ministerie tot de gegevens, terwijl artikel 88*bis* de toegang van de onderzoeksrechter tot de gegevens betreft;⁴⁸ vervolgens volgt uit het ontworpen artikel 126, § 3, dat de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen “gedurende twaalf maanden [worden] bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst”, met als

⁴⁶ Aangezien de bewaringstermijn precies twaalf maanden is.

⁴⁷ De procureur des Konings kan dergelijke maatregelen alleen bevelen in spoedeisende gevallen en enkel voor bepaalde strafbare feiten, en die maatregel moet binnen vierentwintig uur worden bekrachtigd door een onderzoeksrechter (artikel 88*bis* van het Wetboek van Strafvordering).

⁴⁸ Wat overigens verklaart waarom de gegevens waartoe de betrokken overheid toegang heeft, verschillen van de ene bepaling tot de andere.

gevolg dat als de toegang van de procureur des Konings tot de gegevens niet door de ontworpen tekst in de tijd wordt beperkt, die toegang *de facto* uitgebreid zou kunnen worden tot een periode van meer dan twaalf maanden, aangezien de gegevens worden bewaard voor een termijn waarvan het verstrijken pas ingaat vanaf het ogenblik dat communicatie niet mogelijk is via de gebruikte dienst.

In de memorie van toelichting moet derhalve specifieker worden uitgelegd waarom twee gevallen van beperking van de toegang in de tijd waarin wordt voorzien in het ontworpen artikel 88*bis*, § 2, niet zijn opgenomen in het ontworpen artikel 46*bis*, § 1, vierde lid.

Artikel 9

1. Al worden, zoals de gemachtigde van de minister heeft aangegeven, wat betreft de opsomming van de betreffende strafbare feiten, in het ontworpen artikel 88*bis*, § 2, tweede streepje, bestaande bepalingen overgenomen,⁴⁹ lijkt het toch beter, teneinde de bedoeling van de steller van het voorontwerp getrouwer weer te geven, dat artikel 88*bis*, § 2, tweede streepje, gesteld wordt als volgt:

“– Voor andere strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4, of strafbare feiten die niet opgenomen zijn in die bepaling en gepleegd zijn in het kader van een criminele organisatie zoals bedoeld in artikel 324*bis* van het Strafwetboek, of strafbare feiten die een gevangenisstraf van 5 jaar of een zwaardere straf tot gevolg kunnen hebben (voorts zoals in het voorontwerp);”.

2. Bij artikel 9 van het voorontwerp wordt een nieuwe paragraaf 3 ingevoegd in artikel 88*bis* van het Wetboek van Strafvordering, die ertoe strekt de bevoegdheden in te perken die bij dat artikel aan de onderzoeksrechter worden verleend wanneer het gaat om communicatiemiddelen, welke paragraaf luidt als volgt:

“§ 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in § 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in § 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is. Diezelfde zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal.”

Artikel 12 van het voorontwerp strekt er zijnerzijds toe paragraaf 2 van artikel 18/3 van de wet van 30 november 1998 te vervangen door een bepaling waarbij wordt opgelegd dat, in de motivering van de beslissing van het diensthoofd om specifieke maatregelen aan te wenden

⁴⁹ Te weten artikel 46*quinquies* en artikel 89*ter* van het Wetboek van Strafvordering.

voor het verzamelen van gegevens,⁵⁰ “in voorkomend geval, de ernstige aanwijzingen [worden opgenomen] waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële bedreiging.”

In haar gunstig advies nr. 33/2015, op 9 september 2015 gegeven over de ontworpen tekst, merkt de Commissie voor de bescherming van de persoonlijke levenssfeer, bij de vergelijking van die twee bepalingen, “wel op dat het voorontwerp van wet de beroepsgroep van de journalisten niet heeft opgenomen in [de uitzonderingsmaatregel vervat in artikel 9 van het voorontwerp], hetgeen daarentegen wel is gebeurd in artikel 12 van het voorontwerp van wet.” Bijgevolg vraagt de Commissie om “tevens de journalisten in deze uitzonderingsmaatregel op te nemen”.

Het voorontwerp is niet gewijzigd ten gevolge van die opmerking. In de artikelsgewijze bespreking wordt daarvoor de volgende uitleg gegeven:

“In haar voormelde advies vraagt de Privacycommissie om journalisten op te nemen bij de beroepen die door § 3 worden beschermd. Zo’n toevoeging wordt niet nodig geacht omdat journalisten al het voordeel hebben van de bescherming die hun wordt geboden door de wet van 7 april 2005 tot bescherming van de journalistieke bronnen. De toegang tot de gegevens is maar mogelijk als de informatie als cruciaal wordt geacht voor de identificatie van en zoektocht naar de daders van misdrijven die de fysieke integriteit in gevaar brengen of om dergelijke feiten te voorkomen. Bovendien kan het journalistieke brongeheime maar worden opgeheven indien de gevraagde informatie op geen andere manier kan worden verkregen. De tussenkomst van de rechter waarborgt de naleving van deze vereisten (DOC 51-24/001, p. 13).

Overeenkomstig artikel 5 van de wet van 7 april 2005 mogen gegevens die betrekking hebben op de informatiebronnen van journalisten, niet het voorwerp uitmaken van enige opsporings- of onderzoeksmaatregel, tenzij die gegevens kunnen voorkomen dat misdrijven worden gepleegd die de fysieke integriteit van een of meer personen ernstig in het gedrang brengen, in de hierboven vermelde omstandigheden.

In de voorbereiding van de wet van 7 april 2005 wordt duidelijk gezegd: ‘Het spreekt vanzelf dat de journalist zijn informatie op wettige wijze moet verkregen hebben. Dit houdt in dat een journalist die zijn informatie verkreeg door middel van een misdrijf strafrechtelijk vervolgd kan worden.’ (DOC 51-24/001, p. 11)

Zoals bovendien eerder is gepreciseerd, weerspiegelt artikel 88bis hetgeen reeds bestaat in de artikelen 56bis en 90octies. Welnu, deze twee artikelen doelen enkel op advocaten of artsen.”

Het geheim van de journalistieke bronnen wordt inderdaad reeds door bijzondere maatregelen beschermd wat betreft het gebruik van gegevens in dat verband door gerechtelijke instanties.

⁵⁰ Inzonderheid die waarin is voorzien in de artikelen 18/7 en 18/8 van dezelfde wet.

Zo bepaalt artikel 5 van de wet van 7 april 2005 ‘tot bescherming van de journalistieke bronnen’ immers wat volgt:

“Art. 5. Gegevens die betrekking hebben op de informatiebronnen van de personen bedoeld in artikel 2, mogen niet het voorwerp uitmaken van enige opsporings- of onderzoeksmaatregel, tenzij die gegevens kunnen voorkomen dat de in artikel 4 bedoelde misdrijven worden gepleegd, en met naleving van de daarin bepaalde voorwaarden.”

Aangezien die bepaling enkel betrekking heeft op opsporings- en onderzoeksmaatregelen, en dus niet op de inlichtingen- en veiligheidsmaatregelen, is het gerechtvaardigd dat in de ontworpen tekst voorzien wordt in aanvullende maatregelen tot bescherming van de bronnen tegen het verzamelen van gegevens in het kader van inlichtingen en veiligheid, zonder te voorzien in maatregelen op gerechtelijk vlak.

Artikel 10

De woorden “wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 5, vierde lid,” moeten worden vervangen door de woorden “worden tevens de gegevens gevoegd bedoeld in artikel 126, § 5, vierde lid,”.

LE GREFFIER – DE GRIFFIER

LE PRÉSIDENT – DE VOORZITTER

Colette GIGOT

Pierre LIÉNARDY