der Regelung des Verfahrens entscheidet, dass zusätzliche gerichtliche Untersuchungshandlungen vorgenommen werden müssen, wenn die Ratskammer im Rahmen der Regelung des Verfahrens infolge eines von der Zivilpartei gemäß den Artikeln 61*quinquies* und 127 § 3 des Strafprozessgesetzbuches eingereichten Antrags das Verfahren nicht regeln kann und wenn das erkennende Gericht die Behandlung der Sache aufschiebt, um zusätzliche gerichtliche Untersuchungshandlungen vorzunehmen, für nichtig;

- weist die Klagen im Übrigen zurück;

- erhält die Folgen der für nichtig erklärten Bestimmung bis zum Inkrafttreten einer neuen Gesetzesbestimmung und spätestens bis zum 31. Dezember 2016 aufrecht;

- erkennt für Recht:

Indem Artikel 7 des vorerwähnten Gesetzes vom 14. Januar 2013 keine Übergangsmaßnahmen vorsieht, verstößt er nicht gegen die Artikel 10, 11 und 12 der Verfassung, an sich oder in Verbindung mit dem Legalitätsprinzip und mit dem Grundsatz der Rechtssicherheit, mit Artikel 14 Absätze 1 und 3 des Internationalen Paktes über bürgerliche und politische Rechte und mit Artikel 6 Absätze 1 und 3 Buchstaben *b),* c) und *d)* der Europäischen Menschenrechtskonvention.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 11. Juni 2015.

Der Kanzler, Der Präsident,

F. Meersschaut J. Spreutels

COUR CONSTITUTIONNELLE

[2015/203125]

Extrait de l'arrêt n° 84/2015 du 11 juin 2015

Numéros du rôle : 5856 et 5859

En cause : les recours en annulation partielle (article 5) ou totale de 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 », introduits respectivement par l'Ordre des barreaux francophones et germanophone et par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme ».

La Cour constitutionnelle,

composée des présidents J. Spreutels et A. Alen, et des juges E. De Groot, L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, F. Daoût, T. Giet et R. Leysen, assistée du greffier F. Meersschaut, présidée par le président J. Spreutels,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet des recours et procédure*

a. Par requête adressée à la Cour par lettre recommandée à la poste le 21 février 2014 et parvenue au greffe le 24 février 2014, l'Ordre des barreaux francophones et germanophone, assisté et représenté par Me E. Lemmens et Me J.-F. Henrotte, avocats au barreau de Liège, a introduit un recours en annulation de l'article 5 de 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 » (publiée au *Moniteur belge* du 23 août 2013).

b. Par requête adressée à la Cour par lettre recommandée à la poste le 24 février 2014 et parvenue au greffe le 25 février 2014, un recours en annulation de la loi du 30 juillet 2013 précitée a été introduit par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », assistées et représentées par Me R. Jespers, avocat au barreau d'Anvers.

Ces affaires, inscrites sous les numéros 5856 et 5859 du rôle de la Cour, ont été jointes.

(...)

II. *En droit*

(...)

B.1.1. L'Ordre des barreaux francophones et germanophone, partie requérante dans l'affaire n° 5856, demande l'annulation de l'article 5 de 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 ».

L'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », parties requérantes dans l'affaire n° 5859, demandent l'annulation des articles 1er à 7 de la même loi.

B.1.2. La loi du 30 juillet 2013 attaquée dispose :

« Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2. La présente loi transpose partiellement en droit belge la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive ' conservation de données ') (*Journal officiel*, 13 avril 2006, L 105/54) et l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive ' vie privée et communications électroniques ') (*Journal officiel*, 31 juillet 2002, L 201/37).

CHAPITRE 2. — Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 3. L'article 1er de la loi du 13 juin 2005 relative aux communications électroniques, modifié par la loi du 10 juillet 2012, est complété par un alinéa rédigé comme suit :

' La présente loi transpose partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive "conservation de données") (*Journal officiel*, 13 avril 2006, L 105/54) et l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques") (*Journal officiel*, 31 juillet 2002, L 201/37). ' ».

Art. 4. A l'article 2 de la même loi, modifié par les lois des 18 mai 2009 et 10 juillet 2012, les modifications suivantes sont apportées :

a) le 11° est remplacé par ce qui suit :

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

b) l'article est complété par un 74° rédigé comme suit :

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

Art. 5. L'article 126 de la même loi est remplacé par ce qui suit :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises à l'alinéa 1er et celles qui le sont à l'alinéa 2.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ces statistiques ne peuvent comprendre des données à caractère personnel.

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

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

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

Art. 6. Dans l'article 145 de la même loi, modifié par la loi du 25 avril 2007, il est inséré un paragraphe 3*ter* rédigé comme suit :

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

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

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

CHAPITRE 3. — Modification de l'article 90*decies* du Code d'instruction criminelle

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

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

B.2.1. La partie requérante dans l'affaire n° 5856 prend un moyen unique de la violation, par l'article 5 de la loi attaquée, des articles 10 et 11 de la Constitution, lus seuls ou en combinaison avec les articles 6 et 8 de la Convention européenne des droits de l'homme ainsi qu'avec les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne.

B.2.2. Elle reproche à l'article 5 précité de traiter de manière identique les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, dont notamment les avocats, et les autres utilisateurs de ces services sans tenir compte du statut particulier de l'avocat, du caractère fondamental du secret professionnel auquel il est soumis et de la nécessaire relation de confiance qui doit l'unir à ses clients.

La disposition attaquée traiterait également à tort de manière identique les justiciables qui font l'objet de mesures d'enquête ou de poursuite pour des faits susceptibles de s'inscrire dans ces finalités et ceux qui ne font pas l'objet de telles mesures.

B.3.1. Le premier moyen dans l'affaire n° 5859 est pris de la violation, par l'article 5 de la loi attaquée, des articles 10, 11, 12, 15, 22 et 29 de la Constitution, lus isolément ou en combinaison avec les articles 5, 8, 9, 10, 11, 14, 15, 17 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne et avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec les principes généraux du droit de la sécurité juridique, de la proportionnalité et de « l'autodétermination informationnelle » ainsi qu'avec l'article 5.4 du Traité sur l'Union européenne (ci-après : TUE).

B.3.2. Dans une première branche du moyen, les parties requérantes renvoient aux conclusions de l'avocat général à la Cour de justice de l'Union européenne rendues le 12 avril 2013 dans les affaires jointes C-293/12 et C-594/12. Dans ces conclusions, l'avocat général a estimé que la directive « conservation des données » était incompatible, dans son ensemble, avec l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne en ce que les limitations à l'exercice des droits fondamentaux qu'elle comporte, du fait de l'obligation de conservation des données qu'elle impose, ne s'accompagnent pas des principes indispensables appelés à régir les garanties nécessaires à l'encadrement de l'accès auxdites données et leur exploitation. L'avocat général était également d'avis que l'article 6 de la directive était incompatible avec les articles 7 et 52.1 de la Charte en ce qu'il imposait aux Etats membres de garantir que les données visées à son article 5 soient conservées pendant une durée pouvant atteindre deux ans. Les parties requérantes constatent encore que, selon ces conclusions, la directive est disproportionnée par rapport à la nécessité alléguée de réguler le marché interne et est par conséquent contraire à l'article 5.4 du TUE.

Les parties requérantes dans l'affaire n° 5859 en déduisent que dans la mesure où l'article 5 de la loi attaquée transpose la directive « conservation des données », elle viole aussi l'article 5.4 du TUE ainsi que les articles 7 et 52.1 de la Charte des droits fondamentaux de l'Union européenne.

B.3.3. Dans une deuxième branche du moyen, les parties requérantes dans l'affaire n° 5859 énoncent encore huit griefs à l'encontre de l'article 5 de la loi attaquée qui remplace l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques. Ainsi, la nature et l'ampleur des données conservées violeraient le droit au respect de la vie privée. Les parties requérantes reprochent également au législateur de ne pas avoir créé de règles distinctes pour la directive 2002/58/CE et pour la directive 2006/24/CE. Elles soutiennent encore que l'article 126, § 2, d), de la loi du 13 juin 2005 aboutirait à des situations où la sécurité juridique et l'interdiction d'arbitraire seraient compromises et où l'ingérence des autorités dans la vie privée ainsi que dans la liberté d'expression, la liberté de presse et le droit de se réunir et de s'associer serait disproportionnée. Le manque de précision de l'article 126, § 2, a), quant à la désignation d'une autorité compétente et de la même disposition en son point d) quant au pouvoir d'appréciation des services de renseignement est également dénoncé. Il est soutenu dans un point e) de la deuxième branche du moyen que la loi ne prévoit pas un contrôle juridictionnel suffisant contre les atteintes arbitraires des autorités. Dans un point f), les parties requérantes soutiennent que la notion d'infraction pénale utilisée par la loi attaquée ne répondrait pas au principe de légalité et serait en tout état de cause disproportionnée. Le point g) de la deuxième branche du même moyen dénonce l'absence de définition des données à conserver par type de service ainsi que l'absence d'exigences auxquelles ces données doivent répondre. Enfin, le délai de conservation des données prévu par la loi attaquée est critiqué dans un point h).

B.4. En ce qu'ils visent tous deux l'article 5 de la loi attaquée, le moyen unique dans l'affaire nº 5856 et le premier moyen dans l'affaire nº 5859 doivent être examinés conjointement.

B.5.1. Avant d'être remplacé par l'article 5 de la loi attaquée, l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après : la loi du 13 juin 2005) disposait :

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

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

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

B.5.2. Comme l'indique l'article 2 de la loi attaquée, celle-ci constitue la transposition partielle en droit belge de la directive « conservation des données » et de l'article 15.1 de la directive « vie privée et communications électroniques ».

L'exposé des motifs de la loi précise à cet égard :

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

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

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

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

La transposition de la directive 2006/24/CE sera complétée en partie par une modification de l'article 126 de la loi du 13 juin 2005 précitée, et en partie par l'adoption d'un arrêté royal d'exécution de ce nouvel article 126, de telle sorte que la liste des données à conserver et les exigences auxquelles ces données doivent répondre seront fixées par le Roi » (*Doc. parl.*, Chambre, 2012-2013, DOC 53-2921/001, pp. 3-4).

B.6. 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 (CJUE, 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 « conservation des données ».

B.7. Dans son mémoire, le Conseil des ministres constate qu'en raison de l'autorité de chose jugée attachée aux arrêts rendus par la Cour de justice de l'Union européenne, tout juge est désormais tenu de considérer la directive 2006/24/CE comme invalide. Il soutient toutefois que l'arrêt précité de la Cour de justice n'a d'incidence que sur les articles 2 et 3 de la loi attaquée dans lesquels il est annoncé que la loi transpose partiellement en droit belge la directive. Pour ce qui concerne l'article 5 de la loi attaquée, il y aurait, en revanche, lieu de considérer que celui-ci n'est pas affecté par l'arrêt de la Cour de justice et que les Etats membres sont compétents pour régler la matière de la conservation des données, en l'absence de mesures d'harmonisation en la matière.

B.8. Les entreprises tenues de conserver les données ainsi que la liste des données à conserver sont énumérées à l'article 126, § 1er, de la loi du 13 juin 2005, modifié par l'article 5 de la loi attaquée.

Les entreprises visées par l'obligation de conserver les données sont les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents.

Il ressort des travaux préparatoires de la loi attaquée que le législateur a entendu adapter la terminologie employée afin de la rendre compatible avec la directive 2006/24/CE, les catégories de fournisseurs visées par la loi correspondant à celles énumérées par ladite directive (*Doc. parl.*, Chambre, 2012-2013, DOC 53-2921/001, p. 12).

Quant aux données à conserver, elles ont elles aussi été regroupées en plusieurs catégories, tout comme la liste de données à conserver établie par la directive (*ibid.*, p. 13). D'après l'article 126, § 1er, de la loi du 13 juin 2005, modifié par l'article 5 attaqué, il s'agit des données de trafic, des données de localisation, des données d'identification d'utilisateurs finals, des données d'identification du service de communications électroniques utilisé et des données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées dans le cadre de la fourniture des services de communications concernés.

Les buts dans lesquels ces données sont conservées sont décrits au paragraphe 2 de l'article 126 modifié. Il s'agit de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46*bis* à 88*bis* du Code d'instruction criminelle ou de la répression d'appels malveillants vers les services d'urgence. Il s'agit également de permettre 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, ou encore de l'accomplissement des missions de renseignement en application des articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Un délai minimum de douze mois pour la conservation des données est fixé à l'article 126, § 3, de la loi du 13 juin 2005 modifié, ce délai pouvant être porté à dix-huit mois en vertu du paragraphe 4 de la même disposition, voire à plus de vingt-quatre mois dans les circonstances visées à l'article 4, § 1er, lu en combinaison avec l'article 4, § 4, alinéas 2 et 3, de la loi du 13 juin 2005.

L'article 126, § 5, de la loi du 13 juin 2005, modifié par l'article 5 de la loi attaquée, charge les fournisseurs de réseaux ou de services de communications électroniques de garantir la qualité des données conservées ainsi que leur sécurité et leur protection. Les fournisseurs doivent également veiller aux mesures qui doivent être prises pour éviter leur destruction accidentelle ou illicite, leur perte, leur altération accidentelle ou un stockage, un traitement, un accès ou une divulgation qui ne serait pas autorisé ou serait illicite.

Les fournisseurs doivent encore garantir 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 » ainsi que par les agents et préposés de ces fournisseurs autorisés par ladite Cellule.

Enfin, la destruction des données conservées est également mise à la charge des fournisseurs.

B.9. Comme la Cour de justice de l'Union européenne l'a jugé par son arrêt précité du 8 avril 2014 (point 34), l'obligation imposée par les articles 3 et 6 de la directive 2006/24/CE 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.

La Cour de justice a également jugé au point 35 de l'arrêt que « 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 ».

Cette ingérence de la directive a été qualifiée de particulièrement grave (point 37), bien que la directive ne permette pas de prendre connaissance du contenu en tant que tel des communications électroniques conservées (point 39). Contrôlant la proportionnalité de l'ingérence constatée, la Cour de justice a conclu ce qui suit :

« 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. A 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 1er 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. A 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 1er, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque Etat 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 Etat 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 ».

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°, 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 1er à 4, 6 et 7 de la loi du 30 juillet 2013 attaquée et donc l'intégralité de ladite loi.

B.13. Compte tenu de ce qu'ils ne peuvent conduire à une annulation plus étendue, il n'y a pas lieu d'examiner les autres moyens dans l'affaire nº 5859.

Par ces motifs,

la Cour

annule 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 ».

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 11 juin 2015.

Le greffier, Le président,

F. Meersschaut J. Spreutels

GRONDWETTELIJK HOF

[2015/203125]

Uittreksel uit arrest nr. 84/2015 van 11 juni 2015

Rolnummers : 5856 en 5859

In zake : de beroepen tot gedeeltelijke (artikel 5) of gehele vernietiging van 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 », ingesteld respectievelijk door de « Ordre des barreaux francophones et germanophone » en door de vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme ».

Het Grondwettelijk Hof,

samengesteld uit de voorzitters J. Spreutels en A. Alen, en de rechters E. De Groot, L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, F. Daoût, T. Giet en R. Leysen, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter J. Spreutels,

wijst na beraad het volgende arrest :

I. *Onderwerp van de beroepen en rechtspleging*

1. Bij verzoekschrift dat aan het Hof is toegezonden bij op 21 februari 2014 ter post aangetekende brief en ter griffie is ingekomen op 24 februari 2014, heeft de « Ordre des barreaux francophones et germanophone », bijgestaan en vertegenwoordigd door Mr. E. Lemmens en Mr. J.-F. Henrotte, advocaten bij de balie te Luik, beroep tot vernietiging ingesteld van artikel 5 van 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 » (bekendgemaakt in het *Belgisch Staatsblad* van 23 augustus 2013).

2. Bij verzoekschrift dat aan het Hof is toegezonden bij op 24 februari 2014 ter post aangetekende brief en ter griffie is ingekomen op 25 februari 2014, is beroep tot vernietiging ingesteld van de voormelde wet van 30 juli 2013 door de vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme », bijgestaan en vertegenwoordigd door Mr. R. Jespers, advocaat bij de balie te Antwerpen.

Die zaken, ingeschreven onder de nummers 5856 en 5859 van de rol van het Hof, werden samengevoegd.

(...)

II. *In rechte*

(...)

B.1.1. De « Ordre des barreaux francophones et germanophone », verzoekende partij in de zaak nr. 5856, vordert de vernietiging van artikel 5 van 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 ».

De vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme », verzoekende partijen in de zaak nr. 5859, vorderen de vernietiging van de artikelen 1 tot 7 van dezelfde wet.

B.1.2. De bestreden wet van 30 juli 2013 bepaalt :

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

Art. 2. Deze wet zet Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (' Dataretentierichtlijn ') (*Publicatieblad*, 13 april 2006, L 105/54) en artikel 15.1 van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (' richtlijn betreffende privacy en elektronische communicatie ') (*Publicatieblad*, 31 juli 2002, L 201/37) gedeeltelijk om in Belgisch recht.

HOOFDSTUK 2. — Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 3. Artikel 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, gewijzigd bij de wet van 10 juli 2012, wordt aangevuld met een lid luidende :

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

Art. 4. In artikel 2 van dezelfde wet, gewijzigd bij de wetten van 18 mei 2009 en 10 juli 2012, worden de volgende wijzigingen aangebracht :

a) het 11º wordt vervangen door wat volgt :

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

b) het artikel wordt aangevuld met een 74º luidende als volgt :

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

Art. 5. Artikel 126 van dezelfde wet wordt vervangen als volgt :

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

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

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

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

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

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

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

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

§ 2. De gegevens 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;

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

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

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

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

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

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

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

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

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

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

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

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

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

3° hij garandeert dat de toegang tot de bewaarde gegevens enkel 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;

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

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

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

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

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

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

3° de gevallen waarin verzoeken niet konden worden ingewilligd.

Deze statistische informatie mag geen persoonsgegevens omvatten.

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

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

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

Art. 6. In artikel 145 van dezelfde wet, gewijzigd bij de wet van 25 april 2007, wordt een paragraaf 3*ter* ingevoegd, luidende :

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

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

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

HOOFDSTUK 3. — Wijziging van artikel 90*decies* van het Wetboek van strafvordering

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

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

B.2.1. De verzoekende partij in de zaak nr. 5856 leidt een enig middel af uit de schending, door artikel 5 van de bestreden wet, van de artikelen 10 en 11 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 47 van het Handvest van de grondrechten van de Europese Unie.

B.2.2. Het voormelde artikel 5 wordt in die zin bekritiseerd dat het de gebruikers van telecommunicatie- of elektronische communicatiediensten die onderworpen zijn aan het beroepsgeheim, waaronder met name de advocaten, en de andere gebruikers van die diensten identiek behandelt zonder rekening te houden met het bijzondere statuut van de advocaat, het fundamentele karakter van het beroepsgeheim waaraan hij onderworpen is en de noodzakelijke vertrouwensrelatie tussen hem en zijn cliënten.

De bestreden bepaling zou eveneens de rechtzoekenden die het voorwerp uitmaken van onderzoeks- of vervolgingsmaatregelen wegens feiten die mogelijk beantwoorden aan die doeleinden, en die welke niet het voorwerp uitmaken van zulke maatregelen, ten onrechte op identieke wijze behandelen.

B.3.1. Het eerste middel in de zaak nr. 5859 is afgeleid uit de schending, door artikel 5 van de bestreden wet, van de artikelen 10, 11, 12, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie en met artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, met de algemene rechtsbeginselen van rechtszekerheid, evenredigheid en « informationele zelfbeschikking », alsook met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie (hierna : VEU).

B.3.2. In een eerste onderdeel van het middel verwijzen de verzoekende partijen naar de conclusie van de advocaat-generaal bij het Hof van Justitie van de Europese Unie, verstrekt op 12 april 2013 in de samengevoegde zaken C-293/12 en C-594/12. In die conclusie oordeelde de advocaat-generaal dat de « Dataretentierichtlijn » in haar geheel onverenigbaar was met artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aangezien de beperkingen die zij aan de uitoefening van de grondrechten stelt door de opgelegde verplichting tot het bewaren van gegevens, niet gepaard gaan met de onmisbare beginselen die moeten gelden voor de waarborgen waarmee de toegang tot die gegevens en de exploitatie ervan behoren te zijn omkleed. De advocaat-generaal was eveneens van mening dat artikel 6 van de richtlijn onverenigbaar was met de artikelen 7 en 52, lid 1, van het Handvest, in zoverre het de lidstaten verplichtte ervoor te zorgen dat de in artikel 5 ervan bedoelde gegevens worden bewaard gedurende een termijn die tot twee jaar kan oplopen. De verzoekende partijen stellen verder nog vast dat volgens de conclusie de richtlijn onevenredig is in het licht van de noodzaak die wordt aangevoerd om de interne markt te reguleren, en bijgevolg strijdig is met artikel 5, lid 4, van het VEU.

De verzoekende partijen in de zaak nr. 5859 leiden eruit af dat, in zoverre artikel 5 van de bestreden wet de « Dataretentierichtlijn » omzet, de bestreden wet ook artikel 5, lid 4, van het VEU, alsmede de artikelen 7 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie schendt.

B.3.3. In een tweede onderdeel van het middel formuleren de verzoekende partijen in de zaak nr. 5859 nog acht grieven tegen artikel 5 van de bestreden wet, dat artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie vervangt. Zo zouden de aard en de omvang van de bewaarde gegevens het recht op eerbiediging van het privéleven schenden. De verzoekende partijen verwijten de wetgever eveneens dat hij niet in aparte regels heeft voorzien voor de richtlijn 2002/58/EG en voor de richtlijn 2006/24/EG. Zij voeren nog aan dat artikel 126, § 2, d), van de wet van 13 juni 2005 zou leiden tot situaties waarbij de rechtszekerheid en het verbod van willekeur in het gedrang zouden komen en waarbij de inmenging van de overheid in de privacy, maar ook in de vrijheid van meningsuiting, in de persvrijheid en in het recht op vergadering en op vereniging onevenredig zou zijn. Er wordt ook kritiek geleverd op het gebrek aan precisie van artikel 126, § 2, a), wat de aanwijzing van een bevoegde overheid betreft, en van dezelfde bepaling in punt d) ervan, wat de beoordelingsbevoegdheid van de inlichtingendiensten betreft.

Er wordt aangevoerd, in een punt e) van het tweede onderdeel van het middel, dat de wet niet voorziet in een afdoend jurisdictioneel toezicht tegen willekeurige aantastingen door de overheid. In een punt f) voeren de verzoekende partijen aan dat het begrip « strafbaar feit » dat in de bestreden wet wordt gebruikt, niet zou beantwoorden aan het wettigheidsbeginsel, en in ieder geval onevenredig zou zijn. In punt g) van het tweede onderdeel van hetzelfde middel wordt kritiek geuit op het ontbreken van een definitie van de te bewaren gegevens per type dienst, en van vereisten waaraan die gegevens moeten beantwoorden. Ten slotte wordt de bij de bestreden wet bepaalde termijn voor bewaring van de gegevens bekritiseerd in een punt h).

B.4. In zoverre zij beide betrekking hebben op artikel 5 van de bestreden wet, dienen het enige middel in de zaak nr. 5856 en het eerste middel in de zaak nr. 5859 samen te worden onderzocht.

B.5.1. Vóór de vervanging ervan bij artikel 5 van de bestreden wet, bepaalde artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna : de wet van 13 juni 2005) :

« § 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 ».

B.5.2. Zoals artikel 2 van de bestreden wet aangeeft, vormt deze de gedeeltelijke omzetting, in Belgisch recht, van de « Dataretentierichtlijn » en van artikel 15, lid 1, van de « richtlijn betreffende privacy en elektronische communicatie ».

In de memorie van toelichting van de wet wordt in dat verband het volgende gepreciseerd :

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

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

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

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

De omzetting van Richtlijn 2006/24/EG zal deels aan de hand van een wijziging van artikel 126 van de voornoemde wet van 13 juni 2005 voltooid worden en deels door de aanneming van een koninklijk besluit ter uitvoering van dat nieuwe artikel 126, zodat de lijst van te bewaren gegevens en de vereisten waaraan deze gegevens moeten beantwoorden, zullen worden vastgelegd door de Koning » (*Parl. St.*, Kamer, 2012-2013, DOC 53-2921/001, pp. 3-4).

B.6. Bij een arrest van 8 april 2014 van de grote kamer in antwoord op prejudiciële vragen vanwege het Hooggerechtshof van Ierland en het Grondwettelijk Hof van Oostenrijk (HvJ, C-293/12, *Digital Rights Ireland Ltd* en C-594/12, *Kärntner Landesregierung e.a.*) heeft het Hof van Justitie van de Europese Unie de « Dataretentierichtlijn » ongeldig verklaard.

B.7. In zijn memorie stelt de Ministerraad vast dat, wegens het gezag van gewijsde verbonden aan de arresten van het Hof van Justitie van de Europese Unie, iedere rechter voortaan de richtlijn 2006/24/EG als ongeldig moet beschouwen. Hij voert niettemin aan dat het voormelde arrest van het Hof van Justitie alleen een weerslag heeft op de artikelen 2 en 3 van de bestreden wet, waarin wordt aangekondigd dat de wet de richtlijn gedeeltelijk in Belgisch recht omzet. Wat artikel 5 van de bestreden wet betreft, zou men daarentegen ervan moeten uitgaan dat het niet door het arrest van het Hof van Justitie wordt geraakt en dat de lidstaten bevoegd zijn om de aangelegenheid van bewaring van gegevens te regelen, bij ontstentenis van harmonisatiemaatregelen op dat gebied.

B.8. De ondernemingen die verplicht zijn tot gegevensbewaring alsook de lijst van de te bewaren gegevens worden opgesomd in artikel 126, § 1, van de wet van 13 juni 2005, gewijzigd bij artikel 5 van de bestreden wet.

De ondernemingen die verplicht zijn tot gegevensbewaring zijn de aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten en internet-telefoniediensten, en de aanbieders van de onderliggende openbare elektronische communicatienetwerken.

Uit de parlementaire voorbereiding van de bestreden wet blijkt dat de wetgever de gebruikte terminologie heeft willen aanpassen om ze te laten overeenstemmen met die van de richtlijn 2006/24/EG, waarbij de door de wet beoogde categorieën van dienstenaanbieders overeenstemmen met die welke in de genoemde richtlijn zijn opgesomd (*Parl. St.*, Kamer, 2012-2013, DOC 53-2921/001, p. 12).

De te bewaren gegevens werden ook in verschillende categorieën onderverdeeld, net zoals de lijst van te bewaren gegevens die bij de richtlijn werd opgesteld (*ibid.*, p. 13). Volgens artikel 126, § 1, van de wet van 13 juni 2005, gewijzigd bij het bestreden artikel 5, gaat het om de verkeersgegevens, de locatiegegevens, de gegevens voor identificatie van de eindgebruikers, de gegevens voor identificatie van de gebruikte elektronische communicatiedienst en de gegevens voor identificatie van de vermoedelijk gebruikte eindapparatuur, die worden gegenereerd of verwerkt bij het leveren van de betreffende communicatiediensten.

De doeleinden van die gegevensbewaring worden beschreven in paragraaf 2 van het gewijzigde artikel 126. Het gaat om 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, of om de beteugeling van kwaadwillige oproepen naar de nooddiensten. Het gaat

eveneens erom het onderzoek mogelijk te maken, door de Ombudsdienst voor telecommunicatie, naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een netwerk of dienst voor elektronische communicatie, of nog de vervulling van de inlichtingenopdrachten met toepassing van de artikelen 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.

Een minimumtermijn van twaalf maanden voor de bewaring van de gegevens wordt vastgelegd bij het gewijzigde artikel 126, § 3, van de wet van 13 juni 2005, waarbij die termijn tot achttien maanden kan worden gebracht op grond van paragraaf 4 van dezelfde bepaling, en zelfs tot meer dan vierentwintig maanden in de omstandigheden bedoeld in artikel 4, § 1, in samenhang gelezen met artikel 4, § 4, tweede en derde lid, van de wet van 13 juni 2005.

Artikel 126, § 5, van de wet van 13 juni 2005, gewijzigd bij artikel 5 van de bestreden wet, belast de aanbieders van een netwerk of dienst voor elektronische communicatie ermee de kwaliteit van de bewaarde gegevens alsook de beveiliging en de bescherming ervan te waarborgen. De aanbieders moeten eveneens ervoor zorgen dat maatregelen worden genomen om de vernietiging ervan, hetzij per ongeluk, hetzij onrechtmatig, het verlies of, per ongeluk, de wijziging ervan, of een opslag, verwerking, toegang of openbaarmaking die niet zou zijn toegelaten of die onrechtmatig zou zijn, te vermijden.

De aanbieders moeten voorts waarborgen 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 modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, en door het personeel en de aangestelden van die aanbieders die door die cel gemachtigd zijn.

Ten slotte wordt de vernietiging van de bewaarde gegevens eveneens ten laste gelegd van de aanbieders.

B.9. Zoals het Hof van Justitie van de Europese Unie heeft geoordeeld bij zijn voormelde arrest van 8 april 2014 (punt 34), vormt de door de artikelen 3 en 6 van de richtlijn 2006/24/EG aan aanbieders van openbaar beschikbare elektronische communicatiediensten 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 die richtlijn, gedurende een bepaalde tijd te bewaren, op zich een inmenging in de door artikel 7 van het Handvest gewaarborgde rechten.

Het Hof van Justitie oordeelde eveneens, in punt 35 van het arrest, dat « de toegang van de bevoegde nationale autoriteiten tot de gegevens een aanvullende inmenging in dat fundamentele recht [vormt] (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 ».

Die inmenging van de richtlijn werd bijzonder zwaar genoemd (punt 37), hoewel de richtlijn niet de mogelijkheid biedt om kennis te nemen van de inhoud zelf van de bewaarde elektronische communicatie (punt 39). Bij de toetsing van de evenredigheid van de vastgestelde inmenging, heeft het Hof van Justitie het volgende geconcludeerd :

« 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 elektronischecommunicatiemiddelen 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 elektronische communicatiemiddelen, 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 elektronischecommunicatiemiddelen 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 elektronischecommunicatiediensten, 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 elektronischecommunicatiediensten 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 ».

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.

B.13. Rekening houdend met het feit dat zij niet kunnen leiden tot een ruimere vernietiging, dienen de andere middelen in de zaak nr. 5859 niet te worden onderzocht.

Om die redenen,

het Hof

vernietigt 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 ».

Aldus gewezen in het Frans, het Nederlands en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 11 juni 2015.

De griffier, De voorzitter,

F. Meersschaut J. Spreutels

VERFASSUNGSGERICHTSHOF

[2015/203125]

Auszug aus dem Entscheid Nr. 84/2015 vom 11. Juni 2015

Geschäftsverzeichnisnummern. 5856 und 5859

In Sachen: Klagen auf teilweise (Artikel 5) oder völlige Nichtigerklärung des Gesetzes vom 30. Juli 2013 «zur Abänderung der Artikel 2, 126 und 145 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und des Artikels 90*decies* des Strafprozessgesetzbuches», erhoben von der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften bzw. von der VoG «Liga voor Mensenrechten» und der VoG «Ligue des Droits de l'Homme».

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten J. Spreutels und A. Alen, und den Richtern E. De Groot, L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, F. Daoût, T. Giet und R. Leysen, unter Assistenz des Kanzlers F. Meersschaut, unter dem Vorsitz des Präsidenten J. Spreutels,

erlässt nach Beratung folgenden Entscheid:

I. *Gegenstand der Klagen und Verfahren*

a. Mit einer Klageschrift, die dem Gerichtshof mit am 21. Februar 2014 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 24. Februar 2014 in der Kanzlei eingegangen ist, erhob die Kammer der französisch-sprachigen und deutschsprachigen Rechtsanwaltschaften, unterstützt und vertreten durch RA E. Lemmens und RA J.-F. Henrotte, in Lüttich zugelassen, Klage auf Nichtigerklärung von Artikel 5 des Gesetzes vom 30. Juli 2013 «zur Abänderung der Artikel 2, 126 und 145 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und des Artikels 90*decies* des Strafprozessgesetzbuches» (veröffentlicht im *Belgischen Staatsblatt* vom 23. August 2013).

b. Mit einer Klageschrift, die dem Gerichtshof mit am 24. Februar 2014 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 25. Februar 2014 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung des vorerwähnten Gesetzes vom 30. Juli 2013: die VoG «Liga voor Mensenrechten» und die VoG «Ligue des Droits de l'Homme», unterstützt und vertreten durch RA R. Jespers, in Antwerpen zugelassen.

Diese unter den Nummern 5856 und 5859 ins Geschäftsverzeichnis des Gerichtshofes eingetragenen Rechtssachen wurden verbunden.

(...)

II. *Rechtliche Würdigung*

(...)

B.1.1. Die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, klagende Partei in der Rechtssache Nr. 5856, beantragt die Nichtigerklärung von Artikel 5 des Gesetzes vom 30. Juli 2013 «zur Abänderung der Artikel 2, 126 und 145 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und des Artikels 90*decies* des Strafprozessgesetzbuches».

Die VoG «Liga voor Mensenrechten» und die VoG «Ligue des Droits de l'Homme», klagende Parteien in der Rechtssache Nr. 5859, beantragen die Nichtigerklärung der Artikel 1 bis 7 desselben Gesetzes.

B.1.2. Das angefochtene Gesetz vom 30. Juli 2013 bestimmt:

«Artikel 1. Vorliegendes Gesetz regelt eine in Artikel 78 der Verfassung erwähnte Angelegenheit.

Art. 2. Vorliegendes Gesetz dient der teilweisen Umsetzung in belgisches Recht der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze

erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Vorratsdatenspeicherungsrichtlinie) (*Amtsblatt* vom 13. April 2006, L 105/54) und von Artikel 15.1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (*Amtsblatt* vom 31. Juli 2002, L 201/37).

KAPITEL 2 - Abänderungen des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation

Art. 3. Artikel 1 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, abgeändert durch das Gesetz vom 10. Juli 2012, wird durch einen Absatz mit folgendem Wortlaut ergänzt:

' Vorliegendes Gesetz dient der teilweisen Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Vorratsdatenspeicherungsrichtlinie) (*Amtsblatt* vom 13. April 2006, L 105/54) und von Artikel 15.1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (*Amtsblatt* vom 31. Juli 2002, L 201/37). '

Art. 4. Artikel 2 desselben Gesetzes, abgeändert durch die Gesetze vom 18. Mai 2009 und 10. Juli 2012, wird wie folgt abgeändert:

a) Nummer 11 wird wie folgt ersetzt:

' 11. "Betreibern": Personen, die verpflichtet sind, eine Meldung gemäß Artikel 9 einzureichen, '.

b) Der Artikel wird durch eine Nr. 74 mit folgendem Wortlaut ergänzt:

' 74. "erfolglosen Anrufversuchen": Telefonanrufe, bei denen die Verbindung erfolgreich aufgebaut wurde, die aber unbeantwortet geblieben sind, oder bei denen das Netzwerkmanagement eingegriffen hat. '

Art. 5. Artikel 126 desselben Gesetzes wird wie folgt ersetzt:

' Art. 126. § 1. Unbeschadet des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten speichern öffentliche Anbieter von Festnetztelefon-, Mobilfunk-, Internetzugangs-, Internet-E-Mail- und Internet-Telefonie-Diensten sowie Anbieter der zugrunde liegenden öffentlichen elektronischen Kommunikationsnetze auf Vorrat Verkehrsdaten, Standortdaten, Identifizierungsdaten von Endnutzern, Identifizierungsdaten des genutzten elektronischen Kommunikationsdienstes und Identifizierungsdaten der vermutlich genutzten Endeinrichtung, die bei der Bereitstellung der betreffenden Kommunikationsdienste von ihnen erzeugt oder verarbeitet werden.

Im Sinne des vorliegenden Artikels versteht man unter Anbietern ebenfalls Weiterverkäufer in eigenem Namen und für eigene Rechnung.

Im Sinne des vorliegenden Artikels versteht man unter Telefondienst Anrufe - einschließlich Sprachtelefonie, Sprachspeicherdienst, Konferenzschaltungen und Datenabrufungen -, Zusatzdienste - einschließlich Rufweiterleitung und Rufumleitung - und Mitteilungsdienste und Multimediadienste - einschließlich Kurznachrichtendienste (SMS), erweiterte Nachrichtendienste (EMS) und Multimediadienste (MMS).

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass die in Anwendung von Absatz 1 nach Art des Dienstes auf Vorrat zu speichernden Daten und die Anforderungen, die diese Daten erfüllen müssen, fest.

Vorbehaltlich anders lautender Gesetzesbestimmungen dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

Die Verpflichtung zur Vorratsspeicherung der in Absatz 1 erwähnten Daten gilt ebenfalls für erfolglose Anrufversuche, sofern diese Daten bei der Bereitstellung der betreffenden Kommunikationsdienste:

1. von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste beziehungsweise eines öffentlichen Kommunikationsnetzes erzeugt, verarbeitet oder gespeichert werden, wenn es sich um Telefoniedaten handelt, oder

2. von diesen Anbietern protokolliert werden, wenn es sich um Internetdaten handelt.

§ 2. Die in § 1 Absatz 1 erwähnten Daten werden zu folgenden Zwecken auf Vorrat gespeichert:

a) zur Ermittlung, Untersuchung und Verfolgung der in den Artikeln 46*bis* und 88*bis* des Strafprozessgesetzbuches erwähnten strafrechtlichen Verstöße,

b) zu der in Artikel 107 erwähnten Ahndung böswilliger Anrufe bei Hilfsdiensten,

c) zur Ermittlung durch den Ombudsdienst für Telekommunikation der Identität von Personen, die wie in Artikel 43*bis* § 3 Nr. 7 des Gesetzes vom 21. März 1991 zur Umstrukturierung bestimmter öffentlicher Wirtschaftsunternehmen erwähnt böswillig ein elektronisches Kommunikationsnetz beziehungsweise einen elektronischen Kommunikationsdienst genutzt haben,

d) zur Erfüllung von nachrichtendienstlichen Aufträgen unter Einsatz der in den Artikeln 18/7 und 18/8 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Methoden zur Datensammlung.

Die in § 1 Absatz 1 erwähnten Dienste- und Netzanbieter sorgen dafür, dass die in § 1 Absatz 1 erwähnten Daten von Belgien aus unbeschränkt zugänglich sind und dass diese Daten und alle anderen notwendigen Informationen zu diesen Daten unverzüglich und auf einfaches Verlangen den Behörden, die für die unter den Buchstaben *a)* bis *d)* erwähnten Aufträge zuständig sind, und nur diesen übermittelt werden.

§ 3. Daten zur Identifizierung von Endnutzern, des genutzten elektronischen Kommunikationsdienstes und der vermutlich genutzten Endeinrichtung werden ab Zeichnung des Dienstes, solange der gezeichnete Dienst eingehende und ausgehende Kommunikation ermöglicht und während zwölf Monaten ab dem Datum der letzten registrierten eingehenden oder ausgehenden Kommunikation auf Vorrat gespeichert.

Verkehrs- und Standortdaten werden zwölf Monate ab dem Datum der Kommunikation auf Vorrat gespeichert.

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass die Daten fest, die Absatz 1 unterliegen, und die Daten, die Absatz 2 unterliegen.

§ 4. Aufgrund des in § 7 erwähnten Evaluationsberichts kann der König nach Stellungnahme des Instituts und des Ausschusses für den Schutz des Privatlebens durch einen im Ministerrat beratenen Erlass für bestimmte Kategorien die Datenspeicherungsfrist anpassen, ohne dass diese Frist achtzehn Monate überschreiten darf.

Der König kann unter den in Artikel 4 § 1 erwähnten Umständen nach Stellungnahme des Instituts und des Ausschusses für den Schutz des Privatlebens durch einen im Ministerrat beratenen Erlass für einen begrenzten Zeitraum eine Datenspeicherungsfrist von mehr als zwölf Monaten festlegen.

Wenn der König unter den in Absatz 2 erwähnten Umständen eine Speicherungsfrist von mehr als vierundzwanzig Monaten festlegt, setzt der Minister die Europäische Kommission und die anderen Mitgliedstaaten der Europäischen Union unverzüglich von jeder vorgenommenen Maßnahme und deren Begründung in Kenntnis.

§ 5. Für die Vorratsspeicherung der in § 1 Absatz 1 erwähnten Daten gilt für Anbieter eines elektronischen Kommunikationsnetzes beziehungsweise -dienstes Folgendes:

1. Sie gewährleisten, dass die auf Vorrat gespeicherten Daten von der gleichen Qualität sind und der gleichen Sicherheit und dem gleichen Schutz unterliegen wie die im Netz vorhandenen Daten.

2. Sie sorgen dafür, dass in Bezug auf die auf Vorrat gespeicherten Daten geeignete technische und organisatorische Maßnahmen getroffen werden, um sie vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung, unbefugter oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen.

3. Sie gewährleisten, dass der Zugang zu den auf Vorrat gespeicherten Daten ausschließlich einem oder mehreren Mitgliedern des in Artikel 2 des Königlichen Erlasses vom 9. Januar 2003 zur Festlegung der Modalitäten der gesetzlichen Mitwirkungspflicht bei gerichtlichen Ersuchen in Bezug auf elektronische Kommunikation erwähnten Koordinationsbüros der Justiz sowie dem Personal und den Angestellten dieser Anbieter, denen das vorerwähnte Büro eine spezifische Ermächtigung erteilt hat, vorbehalten ist.

4. Sie sorgen dafür, dass die auf Vorrat gespeicherten Daten nach Ablauf der auf diese Daten anwendbaren Speicherungsfrist vernichtet werden.

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass die technischen und administrativen Maßnahmen fest, die die in § 1 Absatz 1 erwähnten Dienste- und Netzanbieter ergreifen müssen, um den Schutz der auf Vorrat gespeicherten personenbezogenen Daten zu gewährleisten.

Die in § 1 Absatz 1 erwähnten Dienste- und Netzanbieter gelten für diese Daten im Sinne des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten als für die Verarbeitung Verantwortliche.

§ 6. Der Minister und der Minister der Justiz sorgen dafür, dass der Europäischen Kommission und der Abgeordnetenkammer jährlich eine Statistik über die Vorratsspeicherung der Daten übermittelt wird, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste beziehungsweise öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Aus dieser Statistik muss hervorgehen:

1. in welchen Fällen gemäß den anwendbaren gesetzlichen Bestimmungen Daten an die zuständigen Behörden weitergegeben worden sind,

2. wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist,

3. in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

Diese Statistik darf keine personenbezogenen Daten enthalten.

Die Daten, die die Anwendung von § 2 Buchstabe *a)* betreffen, werden ebenfalls dem Bericht beigefügt, den der Minister der Justiz gemäß Artikel 90*decies* dem Parlament erstatten muss.

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers nach Stellungnahme des Instituts die Statistik fest, die die Dienste- beziehungsweise Netzanbieter jährlich dem Institut übermitteln, und die Statistik, die das Institut dem Minister und dem Minister der Justiz übermittelt.

§ 7. Unbeschadet des in § 6 Absatz 3 erwähnten Berichts erstatten der Minister und der Minister der Justiz der Abgeordnetenkammer zwei Jahre nach Inkrafttreten des in § 1 Absatz 3 erwähnten Königlichen Erlasses einen Evaluationsbericht über die Umsetzung dieses Artikels, damit überprüft wird, ob Bestimmungen angepasst werden müssen, insbesondere was die auf Vorrat zu speichernden Daten und die Vorratsspeicherungsfrist betrifft. ’

Art. 6. In Artikel 145 desselben Gesetzes, abgeändert durch das Gesetz vom 25. April 2007, wird ein § 3*ter* mit folgendem Wortlaut eingefügt:

’ § 3*ter*. Mit einer Geldbuße von 50 bis zu 50.000 EUR und einer Gefängnisstrafe von sechs Monaten bis zu drei Jahren oder mit nur einer dieser Strafen wird belegt:

1. wer in anderen als in den durch das Gesetz vorgesehenen Fällen oder unter Nichteinhaltung der durch das Gesetz vorgeschriebenen Formalitäten bei der Ausübung seiner Funktion in betrügerischer Absicht oder mit der Absicht zu schaden die in Artikel 126 erwähnten Daten auf irgendeine Weise übernimmt, in Besitz hält oder von diesen Daten irgendeinen Gebrauch macht,

2. wer Daten, wohl wissend, dass sie durch Begehung der in Nr. 1 erwähnten Straftat erhalten wurden, in Besitz hält, anderen Personen preisgibt oder verbreitet oder von den so erhaltenen Daten irgendeinen Gebrauch macht. ’

KAPITEL 3 - Abänderung von Artikel 90*decies* des Strafprozessgesetzbuches

Art. 7. Artikel 90*decies* des Strafprozessgesetzbuches, eingefügt durch das Gesetz vom 30. Juni 1994 und abgeändert durch die Gesetze vom 8. April 2002, 7. Juli 2002 und 6. Januar 2003, wird durch einen Absatz mit folgendem Wortlaut ergänzt:

’ Diesem Bericht wird der in Anwendung von Artikel 126 § 6 Absatz 3 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erstellte Bericht beigefügt. ’».

B.2.1. Die klagende Partei in der Rechtssache Nr. 5856 leitet einen einzigen Klagegrund ab aus einem Verstoß durch Artikel 5 des angefochtenen Gesetzes gegen die Artikel 10 und 11 der Verfassung, gegebenenfalls in Verbindung mit den Artikeln 6 und 8 der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8 und 47 der Charta der Grundrechte der Europäischen Union.

B.2.2. Sie bemängelt, dass durch den vorerwähnten Artikel 5 die Nutzer von Telekommunikations- oder elektronischen Kommunikationsdiensten, die dem Berufsgeheimnis unterlägen, darunter insbesondere die Rechtsanwälte, auf identische Weise behandelt würden wie die anderen Nutzer dieser Dienste, ohne den besonderen Status der Rechtsanwälte, die grundlegende Beschaffenheit des Berufsgeheimnisses, dem sie unterlägen, und ihr notwendiges Vertrauensverhältnis zu ihren Mandanten zu berücksichtigen.

Durch die angefochtene Bestimmung würden ebenfalls die Rechtsunterworfenen, die Gegenstand von Untersuchungs- oder Verfolgungsmaßnahmen seien wegen Taten, die möglicherweise diesen Zwecken entsprechen könnten, zu Unrecht auf identische Weise behandelt wie diejenigen, die nicht Gegenstand solcher Maßnahmen seien.

B.3.1. Der erste Klagegrund in der Rechtssache Nr. 5859 ist abgeleitet aus einem Verstoß durch Artikel 5 des angefochtenen Gesetzes gegen die Artikel 10, 11, 12, 15, 22 und 29 der Verfassung, gegebenenfalls in Verbindung mit den Artikeln 5, 8, 9, 10, 11, 14, 15, 17 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union und mit Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte, mit den allgemeinen Rechtsgrundsätzen der Rechtssicherheit, der Verhältnismäßigkeit und der «informationellen Selbstbestimmung» sowie mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union (nachstehend: EUV).

B.3.2. In einem ersten Teil des Klagegrunds verweisen die klagenden Parteien auf die Schlussanträge des Generalanwalts beim Gerichtshof der Europäischen Union vom 12. April 2013 in den verbundenen Rechtssachen C-293/12 und C-594/12. In diesen Schlussanträgen habe der Generalanwalt die gesamte « Vorratsdatenspeicherungsrichtlinie» für unvereinbar mit Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union gehalten, da die Einschränkungen der Grundrechtsausübung, die sie aufgrund der durch sie auferlegten Verpflichtung zur Vorratsdatenspeicherung enthalte, nicht mit unabdingbaren Grundsätzen einhergingen, die für die zur Beschränkung des Zugangs zu den Daten und ihrer Auswertung notwendigen Garantien gelten müssten. Der Generalanwalt vertrat ebenfalls den Standpunkt, dass Artikel 6 der Richtlinie mit den Artikeln 7 und 52 Absatz 1 der Charta unvereinbar sei, soweit er den Mitgliedstaaten vorschreibe, sicherzustellen, dass die in ihrem Artikel 5 genannten Daten für die Dauer von bis zu zwei Jahren auf Vorrat gespeichert würden. Die klagenden Parteien halten außerdem fest, dass die Richtlinie entsprechend diesen Schlussanträgen unverhältnismäßig sei gegenüber der vorgeblichen Notwendigkeit, den Binnenmarkt zu regulieren, und dass sie folglich im Widerspruch zu Artikel 5 Absatz 4 des EUV stehe.

Die klagenden Parteien in der Rechtssache Nr. 5859 leiten daraus ab, dass das angefochtene Gesetz insofern, als mit dessen Artikel 5 die « Vorratsdatenspeicherungsrichtlinie» umgesetzt werde, ebenfalls gegen Artikel 5 Absatz 4 des EUV sowie gegen die Artikel 7 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union verstoße.

B.3.3. In einem zweiten Teil des Klagegrunds führen die klagende Parteien in der Rechtssache Nr. 5859 außerdem acht Beschwerdegründe gegen Artikel 5 des angefochtenen Gesetzes an, der Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation ersetzt. So verstießen die Beschaffenheit und der Umfang der gespeicherten Daten gegen das Recht auf Achtung des Privatlebens. Die klagenden Parteien bemängeln ebenfalls, dass der Gesetzgeber keine getrennten Regeln für die Richtlinie 2002/58/EG und für die Richtlinie 2006/24/EG vorgesehen habe. Sie führen ferner an, dass Artikel 126 § 2 Buchstabe *d)* des Gesetzes vom 13. Juni 2005 zu Situationen führen würde, in denen die Rechtssicherheit und das Verbot von Willkür gefährdet seien und in denen die Einmischung der Behörden in das Privatleben sowie in die Freiheit der Meinungsäußerung, die Pressefreiheit sowie das Versammlungs- und Vereinigungsrecht unverhältnismäßig sei. Die mangelhafte Präzision von Artikel 126 § 2 Buchstabe *a)* hinsichtlich der Bestimmung einer zuständigen Behörde sowie von Buchstabe *d)* derselben Bestimmung hinsichtlich der Ermessensbefugnis der Nachrichtendienste wird ebenfalls angeprangert. In einem Punkt *e)* des zweiten Teils des Klagegrunds wird angeführt, dass im Gesetz keine ausreichende gerichtliche Kontrolle gegen willkürliche Verstöße durch die Behörden vorgesehen sei. In einem Punkt *f)* führen die klagenden Parteien an, der im angefochtenen Gesetz verwendete Begriff der «strafrechtlichen Verstöße» entspreche nicht dem Legalitätsprinzip und sei in jedem Fall unverhältnismäßig. In Punkt *g)* des zweiten Teils desselben Klagegrunds wird das Fehlen einer Definition der je nach Art des Dienstes auf Vorrat zu speichernden Daten sowie das Fehlen von Anforderungen, denen diese Daten entsprechen müssten, angeprangert. Schließlich wird die im angefochtenen Gesetz vorgesehene Dauer der Vorratsspeicherung der Daten in einem Punkt *h)* bemängelt.

B.4. Insofern sie sich beide auf Artikel 5 des angefochtenen Gesetzes beziehen, sind der einzige Klagegrund in der Rechtssache Nr. 5856 und der erste Klagegrund in der Rechtssache Nr. 5859 zusammen zu prüfen.

B.5.1. Vor seiner Ersetzung durch Artikel 5 des angefochtenen Gesetzes bestimmte Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation (nachstehend: Gesetz vom 13. Juni 2005):

«§ 1. Der König legt auf Vorschlag des Ministers der Justiz und des Ministers und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass die Bedingungen fest, unter denen Betreiber im Hinblick auf Verfolgung und Ahndung strafrechtlicher Verstöße, auf die Ahndung böswilliger Anrufe bei Hilfsdiensten und auf die vom Ombudsdienst für Telekommunikation geführte Ermittlung der Identität von Personen, die elektronische Kommunikationsnetze beziehungsweise -dienste böswillig genutzt haben, sowie im Hinblick auf die Erfüllung der im Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten nachrichtendienstlichen Aufträge Verkehrs- und Identifizierungsdaten von Endnutzern aufzeichnen und aufbewahren.

§ 2. Aufzubewahrende Daten und Dauer dieser Aufbewahrung, die bei öffentlich zugänglichen Telefondiensten zwischen zwölf und sechsunddreißig Monaten liegen muss, werden vom König nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass festgelegt.

Betreiber gewährleisten, dass die in § 1 erwähnten Daten von Belgien aus unbeschränkt zugänglich sind».

B.5.2. Wie es in Artikel 2 des angefochtenen Gesetzes angegeben ist, stellt dieser die teilweise Umsetzung in belgisches Recht der « Vorratsdatenspeicherungsrichtlinie» und von Artikel 15 Absatz 1 der «Datenschutzrichtlinie für elektronische Kommunikation» dar.

In der Begründung des Gesetzes wurde diesbezüglich präzisiert:

«Mit dieser Richtlinie 2006/24/EG sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen elektronischen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.

Die Richtlinie 2006/24/EG hätte im Prinzip bis zum 15. September 2007 umgesetzt werden müssen, mit Ausnahme dessen, was die Speicherung von Kommunikationsdaten in Bezug auf Internetzugang, Internet-Telefonie und Internet-E-Mail betrifft, wofür das Stichdatum der Umsetzung auf den 15. März 2009 festgesetzt worden war, da Belgien die durch die Richtlinie gebotene Möglichkeit, einen Aufschub zu beantragen, genutzt hat.

Ende September 2012 hat die Kommission Belgien gemahnt, die Richtlinie umzusetzen, und Belgien auf die finanziellen Sanktionen hingewiesen, die der Europäische Gerichtshof unserem Land wegen der unvollständigen Umsetzung der Richtlinie auferlegen könnte. Es ist daher ausgeschlossen, noch länger, und ganz gewiss bis zu einer etwaigen Abänderung der Richtlinie zu warten.

Im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG in belgisches Recht ist es unerlässlich, den Wortlaut von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation anzupassen, der in gewissen Punkten Bestimmungen enthält, die nicht mit den europäischen Bestimmungen in Einklang stehen.

Die Umsetzung der Richtlinie 2006/24/EG wird teilweise durch eine Abänderung von Artikel 126 des vorerwähnten Gesetzes vom 13. Juni 2005 vervollständigt und teilweise durch die Annahme eines königlichen Erlasses zur Ausführung dieses neuen Artikels 126, so dass die Liste der auf Vorrat zu speichernden Daten und die Anforderungen, die diese Daten erfüllen müssen, durch den König festgelegt werden» (*Parl. Dok.*, Kammer, 2012-2013, DOC 53-2921/001, SS. 3-4).

B.6. Durch ein Urteil vom 8. April 2014 der Großen Kammer zur Beantwortung von Vorabentscheidungsfragen seitens des irischen « High Court» und des österreichischen Verfassungsgerichtshofes (EuGH, C-293/12, *Digital Rights Ireland Ltd* und C-594/12, *Kärntner Landesregierung u.a.*) hat der Gerichtshof der Europäischen Union die «Vorratsdatenspeicherungsrichtlinie» für ungültig erklärt.

B.7. In seinem Schriftsatz stellt der Ministerrat fest, dass aufgrund der materiellen Rechtskraft der Urteile des Gerichtshofes der Europäischen Union jeder Richter nunmehr verpflichtet sei, die Richtlinie 2006/24/EG als ungültig zu betrachten. Er führt jedoch an, dass das vorerwähnte Urteil des Europäischen Gerichtshofes nur Auswirkungen auf die Artikel 2 und 3 des angefochtenen Gesetzes habe, in denen ausgedrückt sei, dass mit dem Gesetz die Richtlinie teilweise in belgisches Recht umgesetzt werde. In Bezug auf Artikel 5 des angefochtenen Gesetzes sei hingegen festzustellen, dass dieser nicht durch das Urteil des Europäischen Gerichtshofes betroffen sei und dass die Mitgliedstaaten befugt seien, die Angelegenheit der Vorratsspeicherung von Daten zu regeln, da diesbezüglich keine Harmonisierungsmaßnahmen bestünden.

B.8. Die Unternehmen, die zur Vorratsspeicherung der Daten verpflichtet sind, sowie die Liste der zu speichernden Daten sind in Artikel 126 § 1 des Gesetzes vom 13. Juni 2005 in der durch Artikel 5 des angefochtenen Gesetzes abgeänderten Fassung aufgeführt.

Die Unternehmen, die zur Vorratsdatenspeicherung verpflichtet sind, sind die öffentlichen Anbieter von Festnetztelefon-, Mobilfunk-, Internetzugangs-, Internet-E-Mail- und Internet-Telefonie-Diensten sowie die Anbieter der zugrunde liegenden öffentlichen elektronischen Kommunikationsnetze.

Aus den Vorarbeiten zu dem angefochtenen Gesetz geht hervor, dass der Gesetzgeber die verwendete Terminologie anpassen wollte, um sie mit der Richtlinie 2006/24/EG in Einklang zu bringen, wobei die im Gesetz erwähnten Kategorien von Anbietern denjenigen entsprechen, die in der genannten Richtlinie aufgelistet sind (*Parl. Dok.*, Kammer, 2012-2013, DOC 53-2921/001, S. 12).

Die auf Vorrat zu speichernden Daten wurden ebenfalls in mehrere Kategorien eingeteilt, ebenso wie die in der Richtlinie festgelegte Liste der auf Vorrat zu speichernden Daten (ebenda, S. 13). Gemäß Artikel 126 § 1 des Gesetzes vom 13. Juni 2005 in der durch den angefochtenen Artikel 5 abgeänderten Fassung handelt es sich um Verkehrsdaten, Standortdaten, Identifizierungsdaten von Endnutzern, Identifizierungsdaten des genutzten elektronischen Kommunikationsdienstes und Identifizierungsdaten der vermutlich genutzten Endeinrichtung, die bei der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden.

Die Ziele, zu denen diese Daten gespeichert werden, sind in Paragraph 2 des abgeänderten Artikels 126 beschrieben. Es geht um die Ermittlung, Untersuchung und Verfolgung der in den Artikeln 46*bis* und 88*bis* des Strafprozessgesetzbuches erwähnten strafrechtlichen Verstöße oder um die Ahndung böswilliger Anrufe bei Hilfsdiensten. Es gilt ebenfalls, die Ermittlung durch den Ombudsdienst für Telekommunikation der Identität von Personen, die böswillig ein elektronisches Kommunikationsnetz beziehungsweise einen elektronischen Kommunikationsdienst genutzt haben, oder die Erfüllung von nachrichtendienstlichen Aufträgen in Anwendung der Artikel 18/7 und 18/8 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste zu ermöglichen.

Eine Mindestfrist von zwölf Monaten für die Speicherung der Daten wird festgelegt in dem abgeänderten Artikel 126 § 3 des Gesetzes vom 13. Juni 2005, wobei diese Frist aufgrund von Paragraph 4 derselben Bestimmung auf achtzehn Monate oder sogar auf mehr als vierundzwanzig Monate verlängert werden kann unter den in Artikel 4 § 1 in Verbindung mit Artikel 4 § 4 Absätze 2 und 3 des Gesetzes vom 13. Juni 2005 vorgesehenen Bedingungen.

Durch Artikel 126 § 5 des Gesetzes vom 13. Juni 2005 in der durch Artikel 5 des angefochtenen Gesetzes abgeänderten Fassung werden die Anbieter von elektronischen Kommunikationsnetzen oder -diensten beauftragt, die Qualität der gespeicherten Daten sowie ihre Sicherheit und ihren Schutz zu gewährleisten. Die Anbieter müssen ebenfalls Maßnahmen treffen, um sie vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung, unbefugter oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen.

Die Anbieter müssen sodann gewährleisten, dass der Zugang zu den auf Vorrat gespeicherten Daten ausschließlich einem oder mehreren Mitgliedern des in Artikel 2 des königlichen Erlasses vom 9. Januar 2003 «zur Festlegung der Modalitäten der gesetzlichen Mitwirkungspflicht bei gerichtlichen Ersuchen in Bezug auf elektronische Kommunikation» erwähnten Koordinationsbüros der Justiz sowie dem Personal und den Angestellten dieser Anbieter, denen das vorerwähnte Büro eine Ermächtigung erteilt hat, vorbehalten ist.

Schließlich müssen die Anbieter ebenfalls dafür sorgen, dass die auf Vorrat gespeicherten Daten vernichtet werden.

B.9. Wie der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil vom 8. April 2014 (Randnr. 34) erkannt hat, stellt die durch die Artikel 3 und 6 der Richtlinie 2006/24/EG den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auferlegte Pflicht, die in Artikel 5 dieser Richtlinie aufgeführten Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, als solche einen Eingriff in die durch Artikel 7 der Charta garantierten Rechte dar.

Der Europäische Gerichtshof hat in Randnummer 35 des Urteils ebenfalls erkannt, dass «der Zugang der zuständigen nationalen Behörden zu den Daten einen zusätzlichen Eingriff in dieses Grundrecht [darstellt] (vgl., zu Art. 8 EMRK, Urteile des EGMR *Leander*/Schweden vom 26. März 1987, Serie A, Nr. 116, § 48, *Rotaru*/Rumänien [GK], Nr. 28341/95, § 46, Rep. 2000-V, sowie *Weber und Saravia*/Deutschland (Entsch.), Nr. 54934/00, § 79, Rep. 2006-XI). Auch die Art. 4 und 8 der Richtlinie 2006/24, die Regeln für den Zugang der zuständigen nationalen Behörden zu den Daten aufstellen, greifen daher in die durch Art. 7 der Charta garantierten Rechte ein».

Dieser Eingriff durch die Richtlinie wurde als besonders schwerwiegend eingestuft (Randnr. 37), obwohl die Richtlinie die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet (Randnr. 39). Bei der Prüfung der Verhältnismäßigkeit des festgestellten Eingriffs hat der Europäische Gerichtshof geschlussfolgert:

«48. Im vorliegenden Fall ist angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens und des Ausmaßes und der Schwere des mit der Richtlinie 2006/24 verbundenen Eingriffs in dieses Recht der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt, so dass die Richtlinie einer strikten Kontrolle unterliegt.

49. Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.

50. Diese Beurteilung kann nicht durch den - insbesondere von Herrn Tschohl und Herrn Seitlinger sowie der portugiesischen Regierung in ihren beim Gerichtshof eingereichten schriftlichen Erklärungen angeführten - Umstand in Frage gestellt werden, dass es mehrere elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie 2006/24 fielen oder die eine anonyme Kommunikation ermöglichten. Dieser Umstand vermag zwar die Eignung der in der Vorratsspeicherung der Daten bestehenden Maßnahme zur Erreichung des verfolgten Ziels zu begrenzen, führt aber, wie der Generalanwalt in Nr. 137 seiner Schlussanträge ausgeführt hat, nicht zur Ungeeignetheit dieser Maßnahme.

51. Zur Erforderlichkeit der durch die Richtlinie 2006/24 vorgeschriebenen Vorratsspeicherung der Daten ist festzustellen, dass zwar die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme - wie sie die Richtlinie 2006/24 vorsieht - für die Kriminalitätsbekämpfung nicht rechtfertigen.

52. Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt nach ständiger Rechtsprechung des Gerichtshofs jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen (Urteil *IPI*, C-473/12, EU: C: 2013: 715, Rn. 39 und die dort angeführte Rechtsprechung).

53. Insoweit ist darauf hinzuweisen, dass der Schutz personenbezogener Daten, zu dem Art. 8 Abs. 1 der Charta ausdrücklich verpflichtet, für das in ihrem Art. 7 verankerte Recht auf Achtung des Privatlebens von besonderer Bedeutung ist.

54. Daher muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen (vgl. entsprechend, zu Art. 8 EMRK, Urteile des EGMR *Liberty u.a.*/Vereinigtes Königreich vom 1. Juli 2008, Nr. 58243/00, § § 62 und 63, *Rotaru*/Rumänien, § § 57 bis 59, sowie *S und Marper*/Vereinigtes Königreich, § 99).

55. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten, wie in der Richtlinie 2006/24 vorgesehen, automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht (vgl. entsprechend, zu Art. 8 EMRK, Urteil des EGMR *S und Marper*/Vereinigtes Königreich, § 103, sowie *M. K.*/Frankreich vom 18. April 2013, Nr. 19522/09, § 35).

56. Zu der Frage, ob der mit der Richtlinie 2006/24 verbundene Eingriff auf das absolut Notwendige beschränkt ist, ist festzustellen, dass nach Art. 3 dieser Richtlinie in Verbindung mit ihrem Art. 5 Abs. 1 alle Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie auf Vorrat zu speichern sind. Sie gilt somit für alle elektronischen Kommunikationsmittel, deren Nutzung stark verbreitet und im täglichen Leben jedes Einzelnen von wachsender Bedeutung ist. Außerdem erfasst die Richtlinie nach ihrem Art. 3 alle Teilnehmer und registrierten Benutzer. Sie führt daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung.

57. Hierzu ist erstens festzustellen, dass sich die Richtlinie 2006/24 generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

58. Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

59. Zum anderen soll die Richtlinie zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.

60. Zweitens kommt zu diesem generellen Fehlen von Einschränkungen hinzu, dass die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.

61. Überdies enthält die Richtlinie 2006/24 keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Art. 4 der Richtlinie, der den Zugang dieser Behörden zu den auf Vorrat gespeicherten Daten regelt, bestimmt nicht ausdrücklich, dass der Zugang zu diesen Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind, sondern sieht lediglich vor, dass jeder Mitgliedstaat das Verfahren und die Bedingungen festlegt, die für den Zugang zu den auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

62. Insbesondere sieht die Richtlinie 2006/24 kein objektives Kriterium vor, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Beschränkungen zu schaffen.

63. Drittens schreibt die Richtlinie 2006/24 hinsichtlich der Dauer der Vorratsspeicherung in ihrem Art. 6 vor, dass die Daten für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern sind, ohne dass eine Unterscheidung zwischen den in Art. 5 der Richtlinie genannten Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird.

64. Die Speicherungsfrist liegt zudem zwischen mindestens sechs Monaten und höchstens 24 Monaten, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.

65. Aus dem Vorstehenden folgt, dass die Richtlinie 2006/24 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte vorsieht. Somit ist festzustellen, dass die Richtlinie einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.

66. Darüber hinaus ist in Bezug auf die Regeln zur Sicherheit und zum Schutz der von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes auf Vorrat gespeicherten Daten festzustellen, dass die Richtlinie 2006/24 keine hinreichenden, den Anforderungen von Art. 8 der Charta entsprechenden Garantien dafür bietet, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind. Erstens sieht Art. 7 der Richtlinie 2006/24 keine speziellen Regeln vor, die der großen nach der Richtlinie auf Vorrat zu speichernden Datenmenge, dem sensiblen Charakter dieser Daten und der Gefahr eines unberechtigten Zugangs zu ihnen angepasst sind. Derartige Regeln müssten namentlich klare und strikte Vorkehrungen für den Schutz und die Sicherheit der fraglichen Daten treffen, damit deren Unversehrtheit und Vertraulichkeit in vollem Umfang gewährleistet sind. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Regeln zu schaffen».

B.10.1. Wie der Europäische Gerichtshof in den Randnummern 56 und 57 seines Urteils hervorgehoben hat, schreibt die Richtlinie die Vorratsspeicherung aller Verkehrsdaten betreffend auf Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie vor, weshalb sie sich generell auf alle Personen und alle elektronischen Kommunikationsmittel erstreckt, ohne irgendeine Differenzierung anhand des Ziels der Bekämpfung schwerer Straftaten, das der Gesetzgeber der Union zu verfolgen beabsichtigte.

Das angefochtene Gesetz unterscheidet sich in diesem Punkt keineswegs von der Richtlinie. Wie in B.8 angeführt wurde, sind die Kategorien der Daten, die auf Vorrat gespeichert werden müssen, nämlich identisch mit denjenigen, die in der Richtlinie aufgelistet sind, während keinerlei Unterschied vorgenommen wird in Bezug auf die betreffenden Personen oder die besonderen Regeln, die entsprechend dem Ziel der Bekämpfung der in dem durch das angefochtene Gesetz ersetzten Artikel 126 § 2 des Gesetzes vom 13. Juni 2005 beschriebenen Straftaten vorzusehen sind. So wie der Europäische Gerichtshof in Bezug auf die Richtlinie festgestellt hat (Randnr. 58), gilt das Gesetz also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit den in dem angefochtenen Gesetz aufgelisteten Verstößen stehen könnte. Ebenso gilt das Gesetz ausnahmslos auch für Personen, deren Kommunikationen dem Berufsgeheimnis unterliegen.

B.10.2. Ebenso wenig wie für die Richtlinie verlangt der angefochtene Artikel 5 einen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Er begrenzt ebenfalls nicht die Vorratsspeicherung der betreffenden Daten auf einen bestimmten Zeitraum oder geografischen Bereich oder auf einen Personenkreis, der in eine Straftat im Sinne des Gesetzes verwickelt sein könnte, oder durch die Vorratsdatenspeicherung zur Verhütung, Feststellung oder Verfolgung dieser Straftaten beitragen könnte.

B.10.3. Die Behörden, die befugt sind, Zugang zu den auf Vorrat gespeicherten Daten zu haben, sind zwar in Artikel 126 § 5 Nr. 3 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 5 des angefochtenen Gesetzes, aufgelistet, doch im Gesetz ist keine materielle oder verfahrensmäßige Bedingung für diesen Zugang festgelegt.

B.10.4. Schließlich wird im Gesetz hinsichtlich der Dauer der Vorratsdatenspeicherung nicht zwischen Kategorien von Daten entsprechend ihrer etwaigen Sachdienlichkeit für die angestrebte Zielsetzung oder nach den betroffenen Personen unterschieden.

B.11. Aus den gleichen Gründen wie denjenigen, die den Gerichtshof der Europäischen Union veranlasst haben, die « Vorratsdatenspeicherungsrichtlinie» für ungültig zu erklären, ist festzustellen, dass der Gesetzgeber durch die Annahme von Artikel 5 des angefochtenen Gesetzes die Grenzen überschritten hat, die durch die Einhaltung des Grundsatzes der Verhältnismäßigkeit im Lichte der Artikel 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union geboten sind.

Folglich verstößt der vorerwähnte Artikel 5 gegen die Artikel 10 und 11 der Verfassung in Verbindung mit diesen Bestimmungen. Der einzige Klagegrund in der Rechtssache Nr. 5856 und der erste Klagegrund in der Rechtssache Nr. 5859 sind begründet.

B.12. Da sie untrennbar mit Artikel 5 verbunden sind, sind ebenfalls die Artikel 1 bis 4, 6 und 7 des angefochtenen Gesetzes vom 30. Juli 2013 und somit das gesamte besagte Gesetz für nichtig zu erklären.

B.13. Da die anderen Klagegründe in der Rechtssache Nr. 5859 nicht zu einer weitergehenden Nichtigerklärung führen könnten, brauchen sie nicht geprüft zu werden.

Aus diesen Gründen:

Der Gerichtshof

erklärt das Gesetz vom 30. Juli 2013 «zur Abänderung der Artikel 2, 126 und 145 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und des Artikels 90*decies* des Strafprozessgesetzbuches» für nichtig.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 11. Juni 2015.

Der Kanzler, Der Präsident,

F. Meersschaut J. Spreutels