Geschäftsverzeichnisnrn. 6590, 6597, 6599 und 6601
Entscheid Nr. 96/2018 vom 19. Juli 2018

E N T S C H E I D

In Sachen: Klagen auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation, erhoben von der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, von der VoG « Académie Fiscale » und Jean Pierre Riquet, von der VoG « Liga voor Mensenrechten » und der VoG « Ligue des Droits de l'Homme » und von Patrick Van Assche und anderen.

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten J. Spreutels und A. Alen, und den Richtern L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, F. Daoût und R. Leysen, unter Assistenz des Kanzlers P.-Y. Dutilleux, 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 10. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 11. Januar 2017 in der Kanzlei eingegangen ist, erhob die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, unterstützt und vertreten durch RA E. Lemmens und RA J.-F. Henrotte, in Lüttich zugelassen, Klage auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation (veröffentlicht im *Belgischen Staatsblatt* vom 18. Juli 2016).

b. Mit einer Klageschrift, die dem Gerichtshof mit am 16. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 17. Januar 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung desselben Gesetzes: die VoG « Académie Fiscale » und Jean Pierre Riquet.

c. Mit einer Klageschrift, die dem Gerichtshof mit am 17. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 18. Januar 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung desselben Gesetzes: die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA J. Vander Velpen, in Antwerpen zugelassen, und die VoG « Ligue des Droits de l'Homme », unterstützt und vertreten durch RA R. Jespers, in Antwerpen zugelassen.

d. Mit einer Klageschrift, die dem Gerichtshof mit am 18. Januar 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 19. Januar 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung desselben Gesetzes: Patrick Van Assche, Christel Van Akeleyen und Karina De Hoog, unterstützt und vertreten durch RA D. Pattyn, in Brügge zugelassen.

Diese unter den Nummern 6590, 6597, 6599 und 6601 ins Geschäftsverzeichnis des Gerichtshofes eingetragenen Rechtssachen wurden verbunden.

Der Ministerrat, unterstützt und vertreten durch RA S. Depré und RA E. de Lophem, in Brüssel zugelassen (in den Rechtssachen Nrn. 6590 und 6597) und unterstützt und vertreten durch RA J. Vanpraet und RA Y. Peeters, in Brügge zugelassen (in den Rechtssachen Nrn. 6599 und 6601), hat Schriftsätze eingereicht, die klagenden Parteien in der Rechtssache Nr. 6597 haben Erwiderungsschriftsätze eingereicht, und der Ministerrat hat auch Gegenerwiderungsschriftsätze eingereicht.

Durch Anordnung vom 1. März 2018 hat der Gerichtshof nach Anhörung der referierenden Richter F. Daoût und T. Merckx-Van Goey beschlossen, dass die Rechtssachen verhandlungsreif sind, dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und dass vorbehaltlich eines solchen Antrags die Verhandlung am 21. März 2018 geschlossen und die Rechtssachen zur Beratung gestellt werden.

Infolge der Anträge mehrerer Parteien auf Anhörung hat der Gerichtshof durch Anordnung vom 21. März 2018 den Sitzungstermin auf den 25. April 2018 anberaumt.

Auf der öffentlichen Sitzung vom 25. April 2018

- erschienen

. RA E. Lemmens, RA J.-F. Henrotte und RÄin P. Limbrée, in Lüttich zugelassen, für die klagende Partei in der Rechtssache Nr. 6590,

. RA J. Vander Velpen und RA R. Jespers, für die klagenden Parteien in der Rechtssache Nr. 6599,

. RA D. Pattyn, für die klagenden Parteien in der Rechtssache Nr. 6601,

. RA E. de Lophem, ebenfalls *loco* RA S. Depré, für den Ministerrat in den Rechtssachen Nrn. 6590 und 6597,

. RA J. Vanpraet, für den Ministerrat in den Rechtssachen Nrn. 6599 und 6601,

. RA J. Van Cauter, in Gent zugelassen, für « Child Focus », intervenierende Partei zur Sitzung,

- haben die referierenden Richter F. Daoût und T. Merckx-Van Goey Bericht erstattet,

- wurden die vorgenannten Rechtsanwälte angehört,

- wurden die Rechtssachen zur Beratung gestellt.

Die Vorschriften des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, die sich auf das Verfahren und den Sprachengebrauch beziehen, wurden zur Anwendung gebracht.

II. *Rechtliche Würdigung*

(...)

In Bezug auf das angefochtene Gesetz und seinen Kontext

B.1.1. Es wurden vier Klagen auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation erhoben.

B.1.2. Dieses bestimmt:

« CHAPITRE 1er. - *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

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

Art. 2. A l'article 2 de la loi 13 juin 2005 relative aux communications électroniques, modifié en dernier lieu par la loi du 18 décembre 2015, et partiellement annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, 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) au lieu du 74°, annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré 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. 3. L'article 125, § 2, de la même loi est abrogé.

Art. 4. Dans la même loi, à la place de l'article 126 annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré un article 126 rédigé comme 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, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, les opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, conservent les données visées au paragraphe 3, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Le présent article ne porte pas sur le contenu des communications.

L'obligation de conserver les données visées au paragraphe 3 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 ou traitées par les opérateurs 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. Seules les autorités suivantes peuvent obtenir, sur simple demande, des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, des données conservées en vertu du présent article, pour les finalités et selon les conditions énumérées ci-dessous :

1° les autorités judiciaires, en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle et dans les conditions fixées par ces articles;

2° les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil de données visées aux articles 16/2, 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans les conditions fixées par cette loi;

3° tout officier de police judiciaire de l'Institut, en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et au présent article;

4° les services d'urgence offrant de l'aide sur place, lorsque, à la suite d'un appel d'urgence, ils n'obtiennent pas du fournisseur ou de l'opérateur concerné les données d'identification de l'appelant à l'aide de la base de données visée à l'article 107, § 2, alinéa 3, ou obtiennent des données incomplètes ou incorrectes. Seules les données d'identification de l'appelant peuvent être demandées et au plus tard dans les 24 heures de l'appel;

5° l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, dans le cadre de sa mission d'assistance à personne en danger, de recherche de personnes dont la disparition est inquiétante et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent. Seules les données visées au paragraphe 3, alinéas 1 et 2, relatives à la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données peuvent être demandées à l'opérateur ou au fournisseur concerné par l'intermédiaire d'un service de police désigné par le Roi;

6° le Service de médiation pour les télécommunications, en vue de l'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, conformément aux conditions visées à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Seules les données d'identification peuvent être demandées.

Les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, font en sorte que les données visées au paragraphe 3, soient accessibles de manière illimitée à partir de la Belgique et que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et aux seules autorités visées au présent paragraphe.

Sans préjudice d'autres dispositions légales, les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, ne peuvent utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités.

§ 3. Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2 et 3, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, sont conservées pendant douze mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant 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 à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre.

§ 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs 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 pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er;

4° conservent les données sur le territoire de l'Union européenne;

5° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

6° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé au paragraphe 3, sans préjudice des articles 122 et 123;

7° assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2.

La traçabilité visée à l'alinéa 1er, 7°, s'effectue à l'aide d'un journal. L'Institut et la Commission pour la protection de la vie privée peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 5. 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 Chambre des représentants.

Ces statistiques comprennent notamment :

1° les cas dans lesquels des données 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, 1°, sont 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 du ministre et sur avis de l'Institut, les statistiques que les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 6. Sans préjudice du rapport visé au paragraphe 5, alinéa 4, 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 3, alinéa 4, sur la mise en œuvre du présent 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. 5. Dans la même loi, un article 126/1 est inséré rédigé comme suit :

' Art. 126/1. § 1er. Au sein de chaque opérateur, et au sein de chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, est constituée une Cellule de coordination, chargée de fournir aux autorités belges légalement habilitées, à leur demande, des données conservées en vertu des articles 122, 123 et 126, les données d'identification de l'appelant en vertu de l'article 107, § 2, alinéa 1er, ou les données qui peuvent être requises en vertu des articles 46*bis*, 88*bis* et 90*ter* du Code d'instruction criminelle et des articles 18/7, 18/8, 18/16 et 18/17 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Le cas échéant, plusieurs opérateurs ou fournisseurs peuvent créer une Cellule de coordination commune. En pareil cas, cette Cellule de coordination doit prévoir le même service pour chaque opérateur ou fournisseur.

Afin de faire partie de la Cellule de coordination, les membres doivent :

1° Avoir fait l'objet d'un avis de sécurité positif et non périmé conformément à l'article 22*quinquies* de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

2° Ne pas avoir fait l'objet d'un refus du ministre de la Justice, ce refus devant être motivé et pouvant intervenir en tout temps.

Un avis est considéré comme étant périmé 5 ans après son octroi.

Les opérateurs et fournisseurs qui ne fournissent aucun des services visés à l'article 126, § 1er, sont dispensés de la condition visée à l'alinéa 3, 1°.

Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l'alinéa 1er. Ils peuvent cependant, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l'opérateur ou du fournisseur.

Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.

Chaque opérateur et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, veille à la confidentialité des données traitées par la Cellule de coordination et communique sans délai à l'Institut et à la Commission pour la protection de la vie privée les coordonnées de la Cellule de coordination et de ses membres ainsi que toute modification de ces données.

§ 2. Chaque opérateur et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition de l'Institut des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Chaque opérateur et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, est considéré comme responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel pour les données traitées sur base de l'article 126 et du présent article.

Les opérateurs de réseaux publics de communications électroniques et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, respectent l'article 114, § 2, pour l'accès aux données visées au paragraphe 1er et leur transmission aux autorités.

§ 3. Chaque fournisseur et chaque opérateur visés à l'article 126, § 1er, alinéa 1er, désigne un ou plusieurs préposés à la protection des données à caractère personnel, qui doit répondre aux conditions cumulatives énumérées au paragraphe 1er, alinéa 3.

Ce préposé ne peut pas faire partie de la Cellule de coordination.

Plusieurs opérateurs ou fournisseurs peuvent désigner un ou plusieurs préposés communs à la protection des données à caractère personnel. En pareil cas, ces préposés doivent assurer la même mission pour chaque opérateur ou fournisseur individuel.

Dans l'exercice de ses missions, le préposé à la protection des données à caractère personnel agit en toute indépendance, et a accès à toutes les données à caractère personnel transmises aux autorités ainsi qu'à tous les locaux pertinents du fournisseur ou de l'opérateur.

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

Le préposé doit avoir la possibilité de communiquer directement avec la direction de l'opérateur ou du fournisseur.

Le préposé à la protection des données veille à ce que :

1° les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi;

2° le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver;

3° seules les autorités légalement habilitées aient accès aux données conservées;

4° les mesures de sécurité et de protection des données à caractère personnel décrites dans la présente loi et dans la politique de sécurité du fournisseur ou de l'opérateur soient mises en œuvre.

Chaque fournisseur et chaque opérateur visés à l'article 126, § 1er, alinéa 1er, communique sans délai à l'Institut et à la Commission pour la protection de la vie privée les coordonnées des préposés à la protection des données à caractère personnel, ainsi que toute modification de ces données.

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

1° les modalités de la demande et de l'octroi de l'avis de sécurité;

2° les exigences auxquelles la Cellule de coordination doit répondre, en prenant en compte la situation des opérateurs et fournisseurs recevant peu de demandes des autorités judiciaires, n'ayant pas d'établissement en Belgique ou opérant principalement de l'étranger;

3° les informations à fournir à l'Institut et à la Commission pour la protection de la vie privée conformément aux paragraphes 1 et 3 ainsi que les autorités qui ont accès à ces informations;

4° les autres règles régissant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, avec les autorités belges ou avec certaines d'entre elles, pour la fourniture des données visées au paragraphe 1er, en ce compris, si nécessaire et par autorité concernée, la forme et le contenu de la demande. '.

Art. 6. A l'article 127 de la même loi, modifié par les lois des 4 février 2010, 10 juillet 2012 et 27 mars 2014, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, les mots ' , aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, ' sont insérés entre les mots ' aux opérateurs ' et les mots ' ou aux utilisateurs finals ';

b) dans l'alinéa 2, les mots ' et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, ' sont insérées entre les mots ' des opérateurs ' et les mots ' aux opérations ';

2° le paragraphe 6 est abrogé.

Art. 7. A l'article 145 de la même loi, modifié par les lois du 25 avril 2007 et du 27 mars 2014, les modifications suivantes sont apportées :

1° les mots ' 126, 126/1, ' sont insérés entre les mots ' 124, ' et le mot ' 127 ';

2° les mots ' , 126, 126/1 ' sont insérés entre les mots ' 47 ' et ' et 127 ';

3° au lieu du paragraphe 3*ter*, annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, 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, les divulgue ou en fait un usage quelconque. '.

CHAPITRE 3. - *Modifications du Code d'instruction criminelle*

Art. 8. Dans l'article 46*bis*, § 1er, du Code d'instruction criminelle, inséré par la loi du 10 juin 1998 et remplacé par la loi du 23 janvier 2007, les modifications suivantes sont apportées :

a) les mots ' le concours de l'opérateur d'un réseau de communication ' sont remplacés par les mots ' le concours de l'opérateur d'un réseau de communication ';

b) le paragraphe est complété par un alinéa rédigé comme suit :

' Pour des infractions qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi, ou, en cas d'extrême urgence, l'officier de police judiciaire, ne peuvent requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision. '.

Art. 9. Dans l'article 88*bis* du même Code, inséré par la loi du 11 février 1991, remplacé par la loi du 10 juin 1998 et modifié par les lois des 8 juin 2008 et 27 décembre 2012, les modifications suivantes sont apportées :

a) dans le paragraphe 1er, l'alinéa 1er est remplacé par ce qui suit :

' S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut procéder ou faire procéder, en requérant au besoin, directement ou par l'intermédiaire d'un service de police désigné par le Roi, le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques. ';

b) dans le paragraphe 1er, alinéa 2, les mots ' moyen de télécommunication ' sont remplacés par les mots ' moyen de communication électronique ' et les mots ' de la télécommunication ' par les mots ' de la communication électronique ';

c) dans le paragraphe 1er, l'alinéa 3 est remplacé par ce qui suit :

' Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée. ';

d) dans le paragraphe 1er, l'alinéa 4, est remplacé par ce qui suit :

' Il précise également la durée durant laquelle elle pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2. ';

e) le paragraphe 1er est complété par un alinéa rédigé comme suit :

' En cas d'urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 3 et 4. ';

f) le paragraphe 2, dont le texte actuel formera le paragraphe 4, est remplacé par ce qui suit :

' § 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent :

- pour une infraction visée au livre II, titre I*ter*, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;

- pour une autre infraction visée à l'article 90*ter*, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324*bis* du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;

- pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance. ';

g) l'article est complété par un paragraphe 3 rédigé comme suit :

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

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. ';

h) dans le paragraphe 2, qui est renuméroté en paragraphe 4, alinéa 1er, les mots ' Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication ' sont remplacés par les mots ' Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique '.

Art. 10. L'article 90*decies* du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois des 8 avril 2002, 7 juillet 2002, 6 janvier 2003 et par la loi du 30 juillet 2013 annulée par l'arrêt de la Cour constitutionnelle n° 84/2015, est complété par un alinéa rédigé comme suit :

' A ce rapport est également joint le rapport dressé en application de l'article 126, § 5, alinéa 4, de la loi du 13 juin 2005 relative aux communications électroniques. '.

Art. 11. Dans l'article 464/25, § 2, alinéa 1er, du même Code, les mots ' l'article 88*bis*, § 2, alinéas 1er et 3 ' sont remplacés par les mots ' l'article 88*bis*, § 4, alinéas 1er et 3 '.

CHAPITRE 4. - *Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Art. 12. A l'article 13 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, modifié par la loi du 4 février 2010, les modifications suivantes sont apportées :

1° dans le texte néerlandais de l'alinéa 1er, le mot ' inlichtingen ' est remplacé par le mot ' informatie ';

2° l'alinéa 3 est remplacé par ce qui suit :

' Les services de renseignement et de sécurité veillent à la sécurité des données ayant trait à leurs sources et à celles des informations et des données à caractère personnel fournies par ces sources. ';

3° l'article est complété par un alinéa rédigé comme suit :

' Les agents des services de renseignement et de sécurité ont accès aux informations, renseignements et données à caractère personnel recueillis et traités par leur service, pour autant que ceux-ci soient utiles dans l'exercice de leur fonction ou de leur mission. '.

Art. 13. Dans l'article 18/3 de la même loi, inséré par la loi du 4 février 2010, les modifications suivantes sont apportées :

a) dans le paragraphe 1er, l'alinéa 3, actuel formera le paragraphe 5;

b) dans le paragraphe 1er, alinéa 4, qui formera le paragraphe 7, le mot ' mettre ' est remplacé par les mots ' le suivi de la mise ';

c) le paragraphe 2, dont les alinéas 2 à 5 actuels formeront le paragraphe 6, est remplacé par ce qui suit :

' § 2. La décision du dirigeant du service mentionne :

1° la nature de la méthode spécifique;

2° selon le cas, les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode spécifique;

3° la menace potentielle qui justifie la méthode spécifique;

4° les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3°;

5° la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission;

6° le nom du (ou des) officier(s) de renseignement responsable(s) pour le suivi de la mise en œuvre de la méthode spécifique;

7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode spécifique;

8° le cas échéant, le concours avec une information ou une instruction judiciaire;

9° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle;

10° dans le cas où il est fait application de l'article 18/8, la motivation de la durée de la période à laquelle a trait la collecte de données;

11° la date de la décision;

12° la signature du dirigeant du service. ';

d) le paragraphe 3 est remplacé par ce qui suit :

' § 3. Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.

Ces listes comprennent les données visées au § 2, 1° à 3°, 5° et 7°. ';

e) l'article est complété par un paragraphe 8 rédigé comme suit :

' § 8. Le dirigeant du service met fin à la méthode spécifique lorsque la menace potentielle qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dans les plus brefs délais la Commission de sa décision. '.

Art. 14. Dans l'article 18/8 de la même loi, inséré par la loi du 4 février 2010, les modifications suivantes sont apportées :

a) dans le paragraphe 1er, l'alinéa 1er est remplacé comme suit :

' Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique, procéder ou faire procéder :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques. ';

b) dans le paragraphe 1er, alinéa 2, les mots ' données d'appel ' sont remplacés par les mots ' données de trafic '.

c) le paragraphe 2, dont le texte actuel formera le paragraphe 4, est remplacé par ce qui suit :

‘ § 2. Pour ce qui concerne l’application de la méthode visée au paragraphe 1er aux données conservées sur la base de l’article 126 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s’appliquent :

1° pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut dans sa décision requérir les données que pour une période de six mois préalable à la décision;

2° pour une menace potentielle autre que celles visées sous le 1° et le 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision;

3° pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l’extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision. ’.

Art. 15. Dans l’article 43/3 de la même loi, inséré par la loi du 4 février 2010, les mots ‘ visées à l’article 18/3, § 2 ’ sont remplacés par les mots ‘ visées à l’article 18/3, § 3 ’.

Art. 16. Dans l’article 43/5, § 1er, alinéa 2, de la même loi, les mots ‘ visées à l’article 18/3, § 2 ’ sont remplacés par les mots ‘ visées à l’article 18/3, § 3 ’. ».

B.2.1. Durch das angefochtene Gesetz wollte der Gesetzgeber der Nichtigerklärung von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation in der durch 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 » (im Folgenden: das Gesetz vom 30. Juli 2013) abgeänderten Fassung durch den Entscheid des Gerichtshofes Nr. 84/2015 vom 11. Juni 2015 Rechnung tragen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1567/001, S. 4).

B.2.2. Das so für nichtig erklärte Gesetz vom 30. Juli 2013 stellte die teilweise 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 (*Amtsblatt*, 13. April 2006, L 105/54) und von Artikel 15 Nr. 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 (*Amtsblatt*, 31. Juli 2002, L 201/37) dar (Artikel 2 des Gesetzes).

B.2.3. Die Nichtigerklärung durch den Gerichtshof beruht auf den folgenden Gründen:

« 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.3. Aus den Vorarbeiten zu dem angefochtenen Gesetz geht hervor, dass der Gesetzgeber sowohl den vorerwähnten Entscheid Nr. 84/2015 des Verfassungsgerichtshofes vom 11. Juni 2015 als auch das Urteil des Gerichtshofes vom 8. April 2014, auf dem er beruht, gründlich geprüft hat.

Das Ziel, das der Gesetzgeber mit dem angefochtenen Gesetz vom 29. Mai 2016 verfolgt, ist nicht nur die Bekämpfung des Terrorismus und der Kinderpornographie, sondern auch die Möglichkeit, die auf Vorrat gespeicherten Daten in einer Vielzahl von Situationen, in denen diese Daten sowohl der Ausgangspunkt als auch eine Phase der strafrechtlichen Ermittlung sein können, zu benutzen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1567/001, S. 6).

B.4.1. Aus der Begründung des angefochtenen Gesetzes geht hervor, dass der Gesetzgeber der Auffassung war, es sei im Lichte der Zielsetzung unmöglich, eine gezielte und differenzierte Vorratsspeicherungspflicht einzuführen, und sich dafür entschieden hat, die allgemeine und unterschiedslose Vorratsspeicherungspflicht mit strikten Garantien zu versehen, sowohl auf der Ebene des Schutzes der Aufbewahrung als auch auf der Ebene des Zugangs, um den Eingriff in das Recht auf Achtung des Schutzes des Privatlebens auf ein Minimum zu begrenzen. In diesem Zusammenhang wurde betont, dass es schlicht unmöglich sei, eine *a priori*-Differenzierung nach Personen, Zeiträumen und geografischen Gebieten vorzunehmen.

B.4.2. Diese Unmöglichkeit ist in den Vorarbeiten detailliert dargelegt:

« 7. La distinction en fonction des personnes, périodes temporelles et zones géographiques

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

Dans l'avis 33-2015 précité, la Commission [de la protection de la vie privée] va dans le même sens puisqu'elle indique que ' certains aspects des arrêts [de la Cour de justice et de la Cour constitutionnelle] lui paraissent difficilement applicables, en particulier la distinction en fonction des personnes, périodes temporelles et/ ou zones géographiques '.

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

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

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

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

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

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

Cette partie de l'arrêt de la Cour de justice a suscité beaucoup d'interrogations quant à sa portée. Le groupe de travail qui a préparé le présent projet de loi s'est lui aussi interrogé sur la

possibilité de limiter l'impact de l'article 126 en travaillant sur les critères soulevés par la Cour de justice, c'est-à-dire une ' période temporelle ', ' une zone géographique déterminée ' ou encore ' un cercle de personnes '.

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

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

Quant à la référence à une ' zone géographique ' ou un ' cercle de personnes ', une activation de l'article 126 LCE sur la base de ce type de critère s'apparenterait à du profilage avec les risques de discrimination qui en découlent.

c) Pas d'exclusion de certaines professions

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

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

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

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

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

Ni l'arrêt de la Cour constitutionnelle ni celui de la Cour de justice de l'Union européenne ne concluent toutefois qu'un seul des quatre éléments suffit à constituer une violation du

principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant l'élément essentiel de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle auraient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments.

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

8. Les catégories de données

La Cour constitutionnelle note que ' [...] 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 '.

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

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

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

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

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

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

9. Le renforcement des garanties au niveau de l'accès des autorités aux données

La directive UE a été considérée comme particulièrement problématique parce qu'elle ne réglait que l'obligation de conservation sans réglementer et donc sans encadrer l'accès des autorités aux données concernées. La Cour constitutionnelle note que ' 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. '

L'article 126 LCE annulé renvoyait pourtant explicitement, pour les deux régimes d'accès principaux, aux règles régissant cet accès, c'est-à-dire les articles 46*bis* et 88*bis* du Code d'instruction criminelle pour le cadre pénal et les articles 18/7 et 18/8 de la loi organique des services de renseignement et de sécurité pour les accès au niveau de l'activité de renseignement.

Le présent projet de loi donne suite à cette partie de l'arrêt de la Cour constitutionnelle en renforçant le lien entre l'article 126 LCE et le régime d'accès défini dans les autres lois précitées. Il clarifie aussi le fait que l'accès aux données conservées n'est possible que pour les finalités explicitement énumérées dans l'article 126 LCE.

Mais le présent projet de loi va plus loin en renforçant les garanties prévues par le Code d'instruction criminelle et la loi organique des services de renseignement et de sécurité. Il encadre aussi mieux l'accès pour les autres finalités. Celles-ci sont précisées et étendues à certaines situations très spécifiques.

a) Renforcement des garanties dans le Code d'instruction criminelle

Le projet de loi modifie en première instance les règles quant à l'accès aux données d'identification qui est réglé par l'article 46*bis* du Code d'instruction criminelle et qui concerne l'accès aux données des deux premières catégories. Cet article 46*bis* a déjà été modifié par les lois du 27 décembre 2004 et du 23 janvier 2007. Il n'est pas possible d'alourdir la procédure pour une mesure aussi fréquente et dont l'impact sur la vie privée reste limité. Les conditions restent bien entendu applicables, notamment l'autorisation préalable et motivée du parquet ou du juge d'instruction.

Le projet introduit néanmoins une différenciation de l'accès aux donnés à l'article 46*bis*, en ajoutant au § 1er que pour des infractions de moindre gravité, qui ne sont pas de nature à entraîner une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, les données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi.

Le Conseil d'Etat fait remarquer dans son avis que ce n'est pas la même différenciation sur la base de la gravité de l'infraction que celle prévue pour l'article 88*bis* C.I.Cr. (voy. *infra*) et que les raisons y afférentes doivent être indiquées plus clairement.

Tout d'abord, il serait déraisonnable de rendre la demande des données visées à l'article 46*bis*, § 1er, 1° et 2° possible seulement pour les infractions graves.

Comme il a déjà été indiqué, les données d'identification visées ne sont pas de nature à ce que leur communication implique une intrusion importante dans la vie privée.

Enfin, le raisonnement du Conseil d'Etat n'est que partiellement valide lorsqu'il indique que les données d'identification de l'article 46*bis* peuvent *de facto* être conservées pour une durée beaucoup plus longue que 12 mois. D'une part, il est vrai que ce délai de conservation ne commence à courir qu'à ' la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé ' (article 126, § 3, premier alinéa LCE) mais, d'autre part, cette règle ne va pas toujours mener dans la pratique à une durée de conservation plus longue que douze mois.

Il faut en particulier prendre en compte la situation des adresses IP dynamiques qui changent fréquemment et pour lesquelles le délai commencera à courir à partir de la fin de la communication concernée. Or, pouvoir identifier qui utilisait une adresse IP précise à un moment X est de plus en plus important pour les enquêtes en raison de l'évolution des communications.

Le régime applicable pour ce qui concerne le repérage des communications et donc l'accès aux données des deux dernières catégories (données de connexion et de localisation et données personnelles de communication) est également considérablement renforcé sur le plan des garanties. Ce régime est défini à l'article 88*bis* du Code d'instruction criminelle. Le projet de loi apporte trois garanties principales.

Il introduit une exigence de subsidiarité : la mesure ne peut être autorisée que si le résultat ne peut pas être atteint par une autre mesure moins intrusive.

Le projet introduit aussi une différenciation sur la base de la gravité de l'infraction. La mesure ne sera plus disponible dans le cadre de la poursuite d'infractions punies de moins d'un an d'emprisonnement. Pour les infractions punies de un à cinq ans d'emprisonnement, la mesure pourra être autorisée, mais ne pourra porter que sur les données relatives aux six derniers mois. Pour les infractions punies d'au moins cinq ans d'emprisonnement et/ou reprises sur la liste prévue à l'article 90*ter* du Code d'instruction criminelle (c'est-à-dire les infractions pouvant donner lieu à écoute téléphonique), et/ou qui sont commises dans le cadre d'une organisation criminelle, la mesure pourra porter sur une période de neuf mois précédant la demande. Enfin, elle pourra porter sur l'entièreté de la période de conservation pour les enquêtes en matière de terrorisme.

Enfin, une protection explicite est prévue pour les avocats et les médecins.

b) Renforcement des garanties dans la loi organique des services de renseignement et de sécurité

L'accès aux données conservées est réglé par les articles 18/3, 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cet accès est déjà fortement encadré.

L'article 18/3 règle la procédure de mise en œuvre des méthodes spécifiques et leur contrôle par une Commission indépendante, composée de trois magistrats (la Commission BIM). Il prévoit aussi des garanties en vue de préserver le secret professionnel des avocats et médecins et le secret des sources des journalistes.

Conformément à l'art. 18/3, § 1er, de la loi organique, les méthodes spécifiques ne peuvent être mises en œuvre que si :

- les méthodes ordinaires s'avèrent insuffisantes pour récolter les informations nécessaires à une mission de renseignement (subsidiarité);

- il y a une menace potentielle;

- elles sont proportionnelles au degré de gravité de la menace;

- la décision du chef du service est écrite et motivée.

Ces conditions impliquent que les services de renseignement doivent, pour chaque méthode, justifier le lien entre la cible et la menace.

Aucune méthode spécifique ne peut être mise en œuvre avant la notification de la décision du chef du service à la commission. Le contrôle de légalité des méthodes spécifiques par les membres de la commission, en ce compris le respect de la subsidiarité et de la proportionnalité, peut s'effectuer à tout moment. Le Comité R, organe de contrôle parlementaire, remplit un rôle juridictionnel dans le cadre des méthodes BIM.

Il est interdit aux services de renseignement d'obtenir, d'analyser et d'exploiter des données protégées par le secret professionnel et le secret des sources, sauf si le service dispose au préalable d'indices sérieux selon lesquels l'avocat, le médecin ou le journaliste prend personnellement et activement part à une menace.

Dans ce cas, trois garanties sont prévues :

- la méthode ne peut être utilisée qu'après que la commission a émis un avis conforme;

- la méthode ne peut être appliquée sans que, selon le cas, le président de l'OVB, de l'OBFG, du Conseil National de l'Ordre des Médecins ou de l'Association Générale des Journalistes Professionnels en ait été informé au préalable.

- le président de la commission doit vérifier si les données obtenues via cette méthode ont un lien direct avec la menace.

Le renforcement des garanties prévues à l'article 18/3 vise principalement à rendre obligatoire différentes mentions et motivations dans la décision du chef du service, dont la motivation de la période de rétroactivité des données demandées aux opérateurs.

Il est également précisé, pour renforcer les garanties existantes, l'obligation pour le dirigeant du service de mettre fin à la méthode dès qu'il est constaté une illégalité, ou que la menace qui l'a justifiée n'existe plus, ou qu'elle n'est plus utile.

c) Pour les autres accès

Le projet de loi comme la loi annulée concerne principalement la conservation aux fins de l'enquête pénale ainsi que du renseignement, mais d'autres finalités secondaires sont prévues. Le projet de loi ajoute certaines finalités ciblées, mais prévoit des limitations importantes.

Ainsi, la cellule ' personnes disparues ' de la Police aura accès, par l'intermédiaire d'un service de police désigné par le Roi, aux données dans le cadre d'une disparition inquiétante, mais seulement pour une période de 48 heures, étant entendu qu'un accès plus large dans le cadre de l'enquête judiciaire est possible.

Les services d'urgence offrant de l'aide sur place pourront obtenir certaines données conservées dans certaines situations, mais pour autant que la demande envers l'opérateur intervienne au plus tard dans les 24 heures de l'appel.

Quant au Service de médiation pour les télécommunications, pour ce qui concerne une utilisation malveillante d'un réseau ou d'un service de communications électroniques, il pourra obtenir les données d'identification de la personne qui est à l'origine de cette utilisation malveillante.

10. Le renforcement de la sécurisation des données conservées par les opérateurs

Enfin, le projet de loi, faisant suite notamment aux préoccupations émises par la Cour de justice, renforce les mesures à prendre par les opérateurs et fournisseurs de manière à protéger et sécuriser les données et l'accès à celles-ci. Il s'agit notamment de prendre des mesures de protection technologiques à l'égard de ces données, d'assurer la traçabilité des accès, de détruire les données à l'expiration du délai, ou encore de désigner un préposé à la protection des données chargé de veiller au respect des différentes règles en la matière » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1567/001, pp. 10-18).

B.5. Nach der Verabschiedung des angefochtenen Gesetzes hat der Gerichtshof der Europäischen Union zwei Vorabentscheidungsfragen zur Auslegung von Artikel 15 Absatz 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 beantwortet.

B.6.1. Artikel 15 der vorerwähnten Richtlinie bestimmt:

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

[…] ».

B.6.2. Der Gerichtshof der Europäischen Union hat durch ein Urteil der Großen Kammer vom 21. Dezember 2016, also als das angefochtene Gesetz bereits verabschiedet war, geantwortet (EuGH, 21. Dezember 2016, C-203/15, *Tele2 Sverige AB gegen Post-och*

telestyrelsen und C-698/15, *Secretary of State for the Home Departement gegen Tom Watson u. a.*).

B.6.3. Der Gerichtshof ist in Randnummer 78 dieses Urteils zu dem Schluss gelangt: « Daher betrifft eine Rechtsvorschrift, mit der ein Mitgliedstaat den Betreibern elektronischer Kommunikationsdienste auf der Grundlage von Art. 15 Abs. 1 der Richtlinie 2002/58 zu den in dieser Bestimmung genannten Zwecken vorschreibt, den nationalen Behörden unter in der betreffenden Rechtsvorschrift vorgesehenen Voraussetzungen den Zugang zu den von ihnen gespeicherten Daten zu gewähren, die Verarbeitung personenbezogener Daten durch die Betreiber, und eine solche Verarbeitung fällt in den Geltungsbereich dieser Richtlinie ».

B.6.4. Der Gerichtshof erinnert daran, dass Artikel 5 Absatz 1 der Richtlinie vorsieht, dass die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch ihre innerstaatlichen Vorschriften sicherzustellen haben. Der Grundsatz der Vertraulichkeit bedeutet, dass es jeder anderen Person als dem Nutzer untersagt ist, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern (Randnummern 84 und 85).

B.6.5. Der Gerichtshof weist auch darauf hin, dass Artikel 15 Absatz 1 der Richtlinie es den Mitgliedstaaten zwar erlaube, Ausnahmen von der in dem vorerwähnten Artikel 5 Absatz 1 aufgestellten grundsätzlichen Pflicht vorzusehen, gleichwohl seien diese Ausnahmen nach der ständigen Rechtsprechung des Gerichtshofs eng auszulegen. « [Artikel 15] vermag es daher nicht zu rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Verpflichtung und insbesondere von dem in Art. 5 der Richtlinie 2002/58 vorgesehenen Verbot, diese Daten zu speichern, zur Regel wird, soll die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden » (Randnummern 88 und 89).

Es wird insoweit darauf hingewiesen,

« dass Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vorsieht, dass die in dieser Bestimmung genannten Rechtsvorschriften, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweichen, „die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen“ zum Ziel haben

müssen oder einen der anderen Zwecke verfolgen müssen, die in Art. 13 Abs. 1 der Richtlinie 95/46, auf den Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 verweist, genannt sind (vgl. in diesem Sinne Urteil vom 29. Januar 2008, *Promusicae*, C-275/06, EU:C:2008:54, Rn. 53). Hierbei handelt es sich um eine abschließende Aufzählung der Zwecke, wie aus Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58 hervorgeht, wonach die Rechtsvorschriften aus den in Art. 15 Abs. 1 Satz 1 dieser Richtlinie „aufgeführten Gründen“ gerechtfertigt sein müssen. Die Mitgliedstaaten dürfen demnach solche Vorschriften nicht zu anderen als den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 aufgezählten Zwecken erlassen » (Randnummer 90).

Der Gerichtshof gelangt hinsichtlich der Tragweite von Artikel 15 Absatz 1 der Richtlinie zu dem Schluss,

« dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweicht, sofern dies in Anbetracht der dort genannten Zwecke „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist. Im elften Erwägungsgrund dieser Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss. Was speziell die Vorratsspeicherung von Daten betrifft, verlangt Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58, dass diese nur „während einer begrenzten Zeit“ und „aus den“ in Art. 15 Abs. 1 Satz 1 der Richtlinie aufgeführten Gründen erfolgen darf » (Randnummer 95).

B.6.6. Der Gerichtshof prüft danach, ob eine nationale Regelung wie die in der ersten Rechtssache anwendbare Regelung, die zu den ihm unterbreiteten Vorabentscheidungsfragen geführt hat, den vorstehend beschriebenen Voraussetzungen genügt. Er stellt fest, dass die in Rede stehende nationale Regelung eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht und die Betreiber elektronischer Kommunikationsdienste verpflichtet, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos. Die so auf Vorrat gespeicherten Daten ermöglichen die Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie die Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte (Randnummern 97 und 98).

Nach Auffassung des Gerichtshofs können aus der Gesamtheit dieser Daten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden. Diese Daten ermöglichen so die Erstellung des Profils der betroffenen Personen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.

Der Gerichtshof hat geurteilt:

« 100. Der mit einer solchen Regelung verbundene Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte ist von großem Ausmaß und als besonders schwerwiegend anzusehen. Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 37).

101. Auch wenn eine solche Regelung nicht die Vorratsspeicherung des Inhalts einer Kommunikation erlaubt und folglich nicht den Wesensgehalt der vorgenannten Grundrechte antastet (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 39), könnte die Vorratsspeicherung der Verkehrs- und Standortdaten jedoch Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Nutzer dieser Mittel haben (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 28).

102. n Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, vermag allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 60).

103. Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 51).

104. Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.

105. Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen 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 keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem

Berufsgeheimnis unterliegen (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 57 und 58).

106. Eine solche Regelung verlangt 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 Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59).

107. Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

108. Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

109. Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 54 und die dort angeführte Rechtsprechung).

110. Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

111. Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten

geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

112. In Anbetracht all dessen ist auf die erste Frage in der Rechtssache C-203/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht »

B.6.7. Auf die zweite Vorabentscheidungsfrage in der Rechtssache C-203/15 und auf die erste Vorabentscheidungsfrage in der Rechtssache C-698/15 antwortet der Gerichtshof, dass Artikel 15 Absatz 1 der Richtlinie 2002/58 EG im Licht der Artikel 7, 8 und 11 sowie des Artikel 52 Absatz 1 der Charta dahin auszulegen sei, dass er einer nationalen Regelung entgegenstehe, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand habe, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern seien (Randnummer 125).

B.6.8. Seinerseits hat der Europäische Gerichtshof für Menschenrechte mittlerweile in seinem Urteil *Centrum för Rättvisa* gegen Schweden vom 19. Juni 2018 erkannt, dass die schwedischen Rechtsvorschriften über die Massenüberwachung elektronischer Kommunikationen mit Artikel 8 der Europäischen Menschenrechtskonvention in Übereinstimmung stehen. Um zu der Schlussfolgerung zu gelangen, dass keine Verletzung vorliegt, stützt er sich auf die Kriterien, die er in seiner früheren Rechtsprechung entwickelt hat (siehe insbesondere EuGHMR, Große Kammer, 4. Dezember 2015, *Roman Zakharov* gegen Russland). Er hebt insbesondere Folgendes hervor:

« La Cour a expressément reconnu que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale (*cf. Weber*

et Saravia, précité, § 106). Dans les affaires *Weber et Saravia* et *Liberty e.a.*, la Cour a admis que les règles d'interception de masse n'excédaient pas, en soi, cette marge. Compte tenu du raisonnement de la Cour dans ces arrêts et compte tenu des menaces qui pèsent actuellement sur de nombreux Etats contractants (notamment le terrorisme mondial et d'autres formes graves de criminalité telles que le trafic de drogue, la traite des êtres humains, l'exploitation sexuelle des enfants et la cybercriminalité), des évolutions technologiques qui ont permis aux terroristes et aux criminels d'échapper plus facilement à la détection sur Internet et de l'imprévisibilité des voies par lesquelles les communications électroniques sont transmises, la Cour considère que la décision de recourir à un système d'interception de masse pour identifier des menaces pour la sécurité nationale jusqu'ici inconnues est une décision qui relève toujours de la marge d'appréciation des Etats » (EuGHMR, 19. Juni 2018, *Centrum för Rättvisa* gegen Schweden, § 112).

In Bezug auf den Schriftsatz der « Fondation pour enfants disparus et sexuellement exploités, abgekürzt ' Child Focus ' »

B.7.1. In einem Schriftsatz vom 23. April 2018, der bei der Kanzlei am 25. April 2018 eingegangen ist, teilt Child Focus ihre Bemerkungen zu den Nichtigkeitsklagen mit.

B.7.2. Artikel 87 § 2 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof sieht vor, dass, wenn der Verfassungsgerichtshof über Nichtigkeitsklagen befindet, jede Person, die ein Interesse nachweist, binnen dreißig Tagen ab der in Artikel 74 vorgeschriebenen Veröffentlichung in einem Schriftsatz ihre Bemerkungen an den Verfassungsgerichtshof richten kann. Sie wird dadurch als Partei des Rechtsstreits angesehen.

B.7.3. Die vorerwähnte Veröffentlichung erfolgte im *Belgischen Staatsblatt* vom 15. Februar 2017. Der Schriftsatz ist somit unzulässig.

Zur Hauptsache

B.8. Der einzige Klagegrund in den Rechtssachen Nr. 6590 und 6597 ist aus einer Verletzung der Artikel 10 und 11 der Verfassung, an sich oder in Verbindung mit den Artikeln 6 und 8 der Europäischen Menschenrechtskonvention sowie mit den Artikeln 7, 8 und 47 der Charta der Grundrechte der Europäischen Union durch das angefochtene Gesetz abgeleitet.

B.9.1. Die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, klagende Partei in der Rechtssache Nr. 6590, bemängelt an dem angefochtenen Gesetz, dass es die Nutzer der Telekommunikations- oder elektronischen Kommunikationsdienste, die dem Berufsgeheimnis unterliegen, darunter insbesondere Rechtsanwälte, und die anderen Nutzer dieser Dienste gleich behandele. Diese klagende Partei stellt fest, dass das Gesetz auch eine allgemeine Pflicht zur Aufzeichnung und Vorratsspeicherung von bestimmten Metadaten beinhalte, mit denen festgestellt werden könne, ob ein Rechtsanwalt von einer natürlichen oder juristischen Person um Rat gefragt worden sei, mit denen dieser Rechtsanwalt identifiziert werden könne, mit denen seine Gesprächspartner und insbesondere seine Klienten sowie das Datum und die Uhrzeit der Kommunikation identifiziert werden könnten. Diese allgemeine Pflicht werde sämtlichen öffentlichen Anbietern von Festnetztelefon-, Mobilfunk-, Internetzugangs-, Internet-E-Mail-, Internet-Telefonie-Diensten und von öffentlichen elektronischen Kommunikationsnetzen auferlegt.

B.9.2. Die in der Rechtssache Nr. 6590 klagende Partei kritisiert an dem angefochtenen Gesetz ebenfalls, eine allgemeine Vorratsspeicherungspflicht für Daten vorzusehen, ohne eine Unterscheidung der Rechtsunterworfenen danach vorzunehmen, ob sie Gegenstand einer Ermittlungs- oder Strafverfolgungsmaßnahme wegen Tatbeständen, die zu einer strafrechtlichen Verurteilung führen können, seien oder nicht.

Sie führt weiter aus, dass die im Gesetz erwähnten Datenkategorien äußerst umfassend und vielfältig seien, insofern sie die Daten zur Identifizierung von Nutzern oder Teilnehmern und der Kommunikationsmittel, die Daten in Bezug auf Zugang und Verbindung der Endeinrichtung zu Netzwerk und Dienst und in Bezug auf den Standort dieser Ausrüstung, einschließlich des Netzabschlusspunktes sowie die Kommunikationsdaten betreffen würden, auch wenn ihr Inhalt ausgenommen sei.

B.10.1. Die in der Rechtssache Nr. 6597 klagenden Parteien werfen dem angefochtenen Gesetz vor, die Nutzer der Telekommunikations- oder elektronischen Kommunikationsdienste, die dem Berufsgeheimnis unterliegen, darunter insbesondere Wirtschafts- und Steuerprüfer, und die anderen Nutzer dieser Dienste gleich zu behandeln, ohne den besonderen Status von Wirtschafts- und Steuerprüfern, die grundlegende Bedeutung

des Berufsgeheimnisses, dem sie unterliegen, und das notwendige Vertrauensverhältnis, das sie zu ihren Klienten haben müssten, zu berücksichtigen.

B.10.2. Sie bemängeln an dem angefochtenen Gesetz außerdem, dass es die Rechtsunterworfenen, die Gegenstand von Ermittlungs- oder Strafverfolgungsmaßnahmen wegen Tatbeständen sind, die unter die Zwecke der Vorratsspeicherung der strittigen elektronischen Daten fallen könnten, und die Rechtsunterworfenen, die nicht Gegenstand solcher Maßnahmen seien, gleich behandelt.

B.11.1. Ein erster Klagegrund in der Rechtssache Nr. 6599 ist aus einer Verletzung der Artikel 10, 11, 12, 15, 22 und 29 der Verfassung, an sich oder 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, mit Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte, mit dem allgemeinen Grundsatz der Rechtssicherheit, der Verhältnismäßigkeit, des Rechts auf informationelle Selbstbestimmung sowie mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union abgeleitet.

B.11.2. Die VoG « Liga voor Mensenrechten » und die VoG « Ligue des Droits de l'Homme », klagende Parteien in der Rechtssache Nr. 6599, werfen dem angefochtenen Gesetz vor, eine allgemeine Vorratsspeicherungspflicht für Daten vorzusehen, was die Betreiber und Anbieter von öffentlichen Telefondiensten (einschließlich der Internet-Telefonie), Internetzugangs- und Internet-E-Mail-Diensten sowie die Betreiber öffentlicher Kommunikationsnetze dazu verpflichte, *de facto* für alle Belgier, ob verdächtig oder nicht, die Verkehrsdaten in Bezug auf die Festnetztelefonie, die Mobilfunktelefonie und die Internet-Telefonie und die Daten in Bezug auf den Internetzugang zwölf Monate auf Vorrat zu speichern und sie der Polizei und der Justiz, den Nachrichten- und Sicherheitsdiensten, den Hilfsdiensten, der Vermisstenzelle sowie dem Ombudsdienst für Telekommunikation zur Verfügung zu stellen.

B.12.1. Ein erster Klagegrund in der Rechtssache Nr. 6601 ist aus einer Verletzung von Artikel 8 der Europäischen Menschenrechtskonvention, der Artikel 7, 8, 11 Nr. 4 und 52 der Charta der Grundrechte der Europäischen Union, der Artikel 10, 11, 19 und 22 der Verfassung, von Artikel 2 Bst. a der Richtlinie 95/46/EG des Europäischen Parlaments und

des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie der Artikel 1, 2, 3, 5, 6, 9 und 15 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 abgeleitet.

B.12.2. Die in der Rechtssache Nr. 6601 klagenden Parteien sind natürliche Personen, die in Belgien wohnen und verschiedene elektronische Kommunikationsdienste im Rahmen eines mit einem Betreiber abgeschlossenen Vertrags nutzen. Im ersten Teil des ersten Klagegrunds bemängeln sie an dem angefochtenen Gesetz, dass es eine allgemeine und unterschiedslose Pflicht zur Aufbewahrung von Identifizierungs-, Verbindungs- und Standortdaten sowie persönliche Kommunikationsdaten zu Lasten der Anbieter von Telefoniediensten, auch über das Internet, von Internetzugangs-, Internet-E-Maildiensten, der Betreiber, die öffentliche Kommunikationsnetze bereitstellen, sowie der Betreiber, die einen dieser Dienste anbieten, vorsehe.

B.13. In Anbetracht ihres Zusammenhangs sind die in den verschiedenen Rechtssachen dargelegten Klagegründe zusammen zu prüfen.

B.14.1. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist ».

B.14.2. Die Artikel 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union bestimmen:

« Artikel 7

Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht ».

« Artikel 11

Freiheit der Meinungsäußerung und Informationsfreiheit

(1) ede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.

(2) Die Freiheit der Medien und ihre Pluralität werden geachtet ».

« Artikel 52

Tragweite und Auslegung der Rechte und Grundsätze

(1) Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

(2) Die Ausübung der durch diese Charta anerkannten Rechte, die in den Verträgen geregelt sind, erfolgt im Rahmen der in den Verträgen festgelegten Bedingungen und Grenzen.

(3) Soweit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.

(4) Soweit in dieser Charta Grundrechte anerkannt werden, wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, werden sie im Einklang mit diesen Überlieferungen ausgelegt.

(5) Die Bestimmungen dieser Charta, in denen Grundsätze festgelegt sind, können durch Akte der Gesetzgebung und der Ausführung der Organe, Einrichtungen und sonstigen Stellen der Union sowie durch Akte der Mitgliedstaaten zur Durchführung des Rechts der Union in Ausübung ihrer jeweiligen Zuständigkeiten umgesetzt werden. Sie können vor Gericht nur bei der Auslegung dieser Akte und bei Entscheidungen über deren Rechtmäßigkeit herangezogen werden.

(6) Den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten ist, wie es in dieser Charta bestimmt ist, in vollem Umfang Rechnung zu tragen.

(7) Die Erläuterungen, die als Anleitung für die Auslegung dieser Charta verfasst wurden, sind von den Gerichten der Union und der Mitgliedstaaten gebührend zu berücksichtigen ».

B.15. Wie aus dem Text des angefochtenen Gesetzes und den in B.4.2 erwähnten Vorarbeiten hervorgeht, wollte der Gesetzgeber drei Kategorien von auf Vorrat zu speichernden Metadaten einführen – die Identifizierungsdaten, die Zugangs- und Verbindungsdaten sowie die Kommunikationsdaten –, die Bedingungen für den Zugang zu den Daten durch die zuständigen Behörden verschärfen und die Sicherung der von den Betreibern auf Vorrat gespeicherten Daten verstärken, und zwar aufgrund der Auslegung des Urteils des Gerichtshofes der Europäischen Union und des Entscheids des Gerichtshofes, nach denen eine allgemeine Vorratsspeicherungspflicht der Daten zulässig sein könnte, wenn diese Pflicht von solchen Garantien begleitet wird.

B.16. Artikel 95 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) », die am 25. Mai 2018 in Kraft getreten ist, bestimmt, dass diese Verordnung natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union

keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Der in B.6.1 zitierte Artikel 15 Absatz 1 der Richtlinie 2002/58/EG bestimmt, dass die Mitgliedstaaten insbesondere Rechtsvorschriften erlassen können, um Daten für einen beschränkten Zeitraum aus den in diesem Absatz genannten Gründen, unter anderem der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit oder der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen, unter den in dieser Bestimmung im Einzelnen festgelegten Bedingungen auf Vorrat zu speichern.

B.17.1. Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, der durch Artikel 4 des angefochtenen Gesetzes eingefügt wurde, legt in seinem Paragraphen 2 Nr. 2 die Bedingungen fest, unter denen Nachrichten- und Sicherheitsdienste von den in Paragraph 1 Absatz 1 erwähnten Anbietern und Betreibern Daten erhalten können.

In diesem Zusammenhang ist festzustellen, dass das *Investigatory Powers Tribunal – London* dem Gerichtshof der Europäischen Union am 31. Oktober 2017 die folgenden Vorabentscheidungsfragen gestellt hat (Rechtssache C-623/17 *Privacy International / Secretary of State for Foreign and Commonwealth Affairs u. a.*):

« Wenn

a. die Fähigkeiten der Sicherheits- und Nachrichtendienste, ihnen zur Verfügung gestellte Massen-Telekommunikationsdaten zu nutzen, für den Schutz der nationalen Sicherheit des Vereinigten Königreichs, u. a. auf dem Gebiet der Terrorismusbekämpfung, der Spionagebekämpfung und der Bekämpfung der nuklearen Proliferation, wesentlich sind;

b. ein wesentliches Merkmal der Nutzung von Massen-Telekommunikationsdaten durch die Sicherheits- und Nachrichtendienste darin besteht, zuvor unbekannte Bedrohungen der nationalen Sicherheit mittels nicht-zielgerichteter Massen-Techniken zu entdecken, die sich auf das Sammeln von Massen-Telekommunikationsdaten an einem Ort stützen; ihr Hauptnutzen liegt in der schnellen Zielidentifizierung und Entwicklung und in der Bereitstellung einer Grundlage für das Tätigwerden im Fall einer unmittelbaren Bedrohung;

c. der Betreiber eines elektronischen Kommunikationsnetzwerks danach nicht verpflichtet ist, Massen-Telekommunikationsdaten, die nur vom Staat (den Sicherheits- und Nachrichtendiensten) gespeichert werden, (über die gewöhnlichen geschäftlichen Verpflichtungen hinaus) zu speichern;

d. das nationale Gericht (vorbehaltlich bestimmter ausgelassener Fragestellungen) festgestellt hat, dass die Schutzmaßnahmen hinsichtlich der Nutzung von Massen-Telekommunikationsdaten durch die Sicherheits- und Nachrichtendienste mit den Anforderungen der EMRK in Einklang stehen, und

e. das nationale Gericht festgestellt hat, dass das Vorschreiben der Anforderungen, die in den Rn. 119 bis 125 des Urteils vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), spezifiziert werden – wenn sie anwendbar sein sollten –, die Maßnahmen, die für die Gewährleistung der nationalen Sicherheit von den Sicherheits- und Nachrichtendiensten ergriffen werden, durchkreuzen und dadurch die nationale Sicherheit des Vereinigten Königreichs gefährden würden:

1. Fällt in Anbetracht von Art. 4 EUV und Art. 1 Abs. 3 der Richtlinie 2002/58/EG[2] über die Privatsphäre und elektronische Kommunikation (im Folgenden: e-Datenschutzrichtlinie) eine Verpflichtung in einer Anweisung eines Secretary of State (Minister) an einen Betreiber eines elektronischen Kommunikationsnetzwerks, Massen-Telekommunikationsdaten an die Sicherheits- und Nachrichtendienste eines Mitgliedstaats zur Verfügung zu stellen, in den Anwendungsbereich des Unionsrechts und der e-Datenschutzrichtlinie?

2. Wenn die erste Frage bejaht wird: Ist eine der im Urteil Watson aufgestellten Anforderungen oder irgendeine andere Anforderung zusätzlich zu den in der EMRK aufgestellten auf eine solche Anweisung eines Secretary of State anwendbar? Und, wenn ja, wie und inwieweit sind solche Anforderungen anwendbar unter Berücksichtigung des wesentlichen Bedürfnisses der Sicherheits- und Nachrichtendienste, den Erwerb großer Datenmengen und Techniken automatisierter Datenverarbeitung zu nutzen, um die nationale Sicherheit zu schützen, und unter Berücksichtigung dessen, in welchem Maß solche Fähigkeiten, die im Übrigen mit der EMRK in Einklang stehen, durch das Vorschreiben solcher Anforderungen bedenklich behindert werden können? »

Der Gerichtshof muss die Antwort auf diese Vorabentscheidungsfragen in seine Prüfung einbeziehen. Aus diesem Grund muss die Prüfung des angefochtenen Gesetzes in Bezug auf diesen Punkt ausgesetzt werden, bis der Gerichtshof in der vorerwähnten Rechtssache ein Urteil erlassen hat.

B.17.2. Artikel 126 § 2 Nr. 1 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, der durch Artikel 4 des angefochtenen Gesetzes eingefügt wurde, legt die Bedingungen fest, unter denen die Gerichtsbehörden im Hinblick auf Ermittlung, Untersuchung und Verfolgung von Verstößen Daten erhalten können. Folglich ist ebenfalls auf die Antwort des Gerichtshofes der Europäischen Union auf die folgende Vorabentscheidungsfrage zu warten, die von der *Audiencia provincial de Tarragona, Sección cuarta* am 14. April 2016 gestellt wurde (Rechtssache C-207/16, *Ministerio Fiscal*):

« Kann die hinreichende Schwere der Straftaten als Kriterium, das einen Eingriff in die Grundrechte rechtfertigt, die in den Art. 7 und 8 der Charta anerkannt werden, allein anhand der Strafe ermittelt werden, die wegen der untersuchten Straftat verhängt werden kann, oder müssen daneben bei dem deliktischen Verhalten bestimmte Grade der Schädlichkeit für Individual- und/oder Kollektivrechtsgüter festgestellt werden?

Falls die Ermittlung der Schwere der Straftat allein anhand der in Betracht kommenden Strafe mit den Verfassungsgrundsätzen der Union, die der Gerichtshof in seinem Urteil vom 8. April 2014 als Standards für die strikte Kontrolle der Richtlinie[2] herangezogen hat, vereinbar ist, wie hoch muss dann die Mindeststrafe sein? Wäre eine allgemeine Grenze von drei Jahren Freiheitsentzug zulässig? ».

Aus den Schlussanträgen des Generalanwalts Henrik Saugmandsgaard Øe vom 3. Mai 2018 in dieser Rechtssache geht hervor, dass die einschlägigen Bestimmungen mehrere Auslegungen zulassen.

B.18. Im Übrigen gehen die Meinungen der Parteien vor dem Gerichtshof darüber auseinander, wie verschiedene Bestimmungen auszulegen sind, insbesondere Artikel 15 Absatz 1 der vorerwähnten Richtlinie 2002/58/EG und die Artikel 7, 8, 11 und 52 der Charta der Grundrechte der Europäischen Union, die der Gerichtshof in seine Kontrolle des angefochtenen Gesetzes einbeziehen muss.

B.19.1. Wie die klagenden Parteien darlegen, habe der Gerichtshof jedoch in seinem Urteil vom 21. Dezember 2016 (C-203/15 und C-698/15 *Tele2 Sverige AB*) entschieden, dass Artikel 5 Absatz 1 der Richtlinie 2002/58/EG eine grundsätzliche Verpflichtung festlege, die Vertraulichkeit der Nachrichten und der damit verbundenen Verkehrsdaten sicherzustellen, und dass Artikel 15 Absatz 1 derselben Richtlinie, der Ausnahmen von diesem Grundsatz enthält, eng auszulegen sei, um zu vermeiden, dass die Ausnahme von dieser grundsätzlichen Verpflichtung, die in Artikel 5 der Richtlinie vorgesehen ist, zur Regel werde, solle die letztgenannte Vorschrift nicht weitgehend ausgehöhlt werden.

Der Gerichtshof habe ebenfalls betont, dass allein die Zwecke, die in Artikel 15 aufgezählt seien, eine Maßnahme rechtfertigen könnten, mit der vom Grundsatz der Vertraulichkeit der Nachrichten und der damit verbundenen Verkehrsdaten abgewichen wird, da Artikel 15 in dieser Hinsicht fordere, dass die Daten nur während einer begrenzten Zeit und aus einem der dort aufgeführten Gründe aufbewahrt werden.

B.19.2. Da – wie die klagenden Parteien ausführen – nach Auffassung des Gerichtshofes eine nationale Regelung, die eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht, ohne dass die Nutzer darüber informiert werden, einen besonders schwerwiegenden Eingriff in die in den Artikeln 7 und 8 der Charta verankerten Grundrechte darstellt, vermag allein die Bekämpfung schwerer Kriminalität eine solche Maßnahme zu rechtfertigen. Der Gerichtshof füge hinzu, dass dieser Zweck zwar dem Gemeinwohl diene, aber für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsehe, für die Kriminalitätsbekämpfung nicht rechtfertigen könne.

Der Gerichtshof schließe daraus, dass eine nationale Regelung, die keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vorsehe und die pauschal sämtliche Personen betreffe, die elektronische Kommunikationsdienste nutzen, ohne geografische oder zeitliche Unterscheidung, ohne dass man den Umstand berücksichtige, ob sich diese Personen auch nur mittelbar in einer Lage befänden, die Anlass zur Strafverfolgung geben könnte, oder dass die Übermittlung von Daten Personen betreffe, deren Kommunikationsvorgänge dem Berufsgeheimnis unterliegen würden, oder ohne einen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen sei, und einer Bedrohung der öffentlichen Sicherheit zu verlangen, die Grenzen des absolut Notwendigen überschreite und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden könne, wie es Artikel 15 der Richtlinie im Licht der Artikel 7, 8 und 11 sowie des Artikels 52 Absatz 1 der Charta verlange.

B.19.3. Nach Ansicht der klagenden Parteien, erklärt der Gerichtshof zwar, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG eine nationalen Regelung nicht untersage, die zur Bekämpfung schwerer Straftaten die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt sei. Dies bedeute aber, dass die nationale Regelung klare und präzise Regeln vorsehen müsse und dass die von der Vorratsdatenspeicherung betroffenen Personen über ausreichende Garantien verfügten, die einen wirksamen Schutz ihrer personenbezogenen

Daten vor Missbrauchsrisiken ermöglichten. Der Gerichtshof füge hinzu, dass die nationale Regelung insbesondere angeben müsse, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden dürfe. Eine solche Regelung müsse sich auf objektive Anknüpfungspunkte stützen, die es ermöglichten, Personenkreise zu erfassen, deren Daten geeignet seien, einen Zusammenhang mit schweren Straftaten sichtbar zu machen oder die eine schwerwiegende Gefahr für die öffentliche Sicherheit darstellten, wobei sich diese Begrenzung durch ein geografisches Kriterium gewährleisten lasse, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen würden, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen würden.

B.19.4. Wie aus B.3 und B.4 hervorgeht, verfolgt der Gesetzgeber mit der Verabschiedung des angefochtenen Gesetzes umfassendere Ziele als die Bekämpfung von schweren Straftaten oder der Gefahr einer schwerwiegenden Beeinträchtigung der öffentlichen Sicherheit.

Der Gesetzgeber hat ebenfalls in den in B.4.2 erwähnten Vorarbeiten mehrmals angegeben, dass von der grundsätzlichen Vorratsspeicherungspflicht von Daten an sich alle Personen betroffen sind, auch wenn sie noch nicht Gegenstand einer Ermittlung sind; er hat außerdem keine Unterscheidung nach Zeitraum, geografischem Gebiet oder Personenkreis vorgenommen und er hat auch keine Ausnahme für Personen, deren Kommunikationsvorgänge dem Berufsgeheimnis unterliegen, vorgesehen.

B.19.5. Nach Auffassung der klagenden Parteien genügt die in dem angefochtenen Gesetz vorgesehene allgemeine Vorratsspeicherungspflicht für Daten nach der vom Gerichtshof mit seinem Urteil vom 21. Dezember 2016 vorgenommenen Auslegung, auch wenn die Bedingungen für den Zugang zu den auf Vorrat gespeicherten Daten in dem angefochtenen Gesetz erheblich verschärft worden seien, nicht den Anforderungen, die in Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union vorgeschrieben seien. Eine solche Pflicht überschreite nämlich die Grenzen des absolut Notwendigen und könne nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es die vorerwähnten europäischen Bestimmungen verlangen.

B.20.1. Der Ministerrat unterstreicht seinerseits, dass durch die angefochtene Rechtsvorschrift mehrere Ziele verfolgt werden. Der Gesetzgeber möchte zunächst die seit langem bestehende Situation, in der der Zugang zu Daten im Telekommunikationssektor im Rahmen von strafrechtlichen Ermittlungen gewährt wird, verbessern, indem er einen gesetzlichen Rahmen schaffe, der die notwendigen Garantien hinsichtlich des Schutzes des Privatlebens biete. Die Vorratsspeicherungspflicht werde auch im Hinblick auf die Suche nach der Wahrheit bei zahlreichen Formen der Kriminalität eingeführt und solle so die Integrität des Strafrechtssystems sicherstellen. Diese Suche nach der Wahrheit sei im Interesse sowohl des Opfers und des Angeklagten (der zum Beispiel beweisen könne, dass er sich zum Zeitpunkt der Tat anderswo befand) als auch aller anderen betroffenen Personen. Mit der Vorratsspeicherungspflicht würden ebenfalls Zwecke verfolgt, die in einer Intervention, um einen Anruf bei den Notdiensten zu verfolgen, oder in der Suche nach einer verschwundenen Person, deren körperliche Unversehrtheit unmittelbar gefährdet sei, bestünden. Dieses Element stelle einen wichtigen Unterschied zu den Situationen dar, die in den vorerwähnten Urteilen des Gerichtshofes angesprochen worden seien. Es bestehe folglich ein Zusammenhang der Verhältnismäßigkeit zwischen der allgemeinen Vorratsspeicherungspflicht und dem Ziel, das sich der Gesetzgeber gesetzt habe.

B.20.2. Der Ministerrat führt außerdem noch aus, dass der Gesetzgeber nicht der Auffassung gewesen sei, dass es im Lichte der Zielsetzung möglich sei, eine gezielte und differenzierte Vorratsspeicherungspflicht einzuführen, und sich dafür entschieden habe, die allgemeine und unterschiedslose Vorratsspeicherungspflicht mit strikten Garantien zu versehen, sowohl auf der Ebene des Schutzes der Vorratsspeicherung als auch auf der Ebene des Zugangs, um den Eingriff in das Recht auf Schutz des Privatlebens auf ein Minimum zu begrenzen. In diesem Zusammenhang betont der Ministerrat, dass es schlicht unmöglich sei, eine *a priori*-Differenzierung nach Personen, Zeiträumen und geografischen Gebieten vorzunehmen. Er verweist in diesem Zusammenhang ebenfalls auf die Schlussanträge des Generalanwalts Henrik Saugmandsgaard Øe in den verbundenen Rechtssachen C-203/15 und C-698/15.

Aus den Anhaltspunkten, über die der Gerichtshof verfügt, geht hervor, dass die Mehrheit der Mitgliedstaaten große Schwierigkeiten hat, ihre Rechtsvorschriften auf dem Gebiet der Vorratsdatenspeicherung mit den Anforderungen des Gerichtshofes in seiner Rechtsprechung in Einklang zu bringen (siehe: *Data retention across the EU*,

http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention; Schreiben des Ministers für Justiz und Sicherheit der Niederlande vom 26. März 2018 an den Präsidenten der « Tweede Kamer der Staten-Generaal », zweite Kammer, Sitzungsjahr 2017-2018, 34 537, Nr. 7).

B.21. Dementsprechend ist dem Gerichtshof der Europäischen Union die vom Ministerrat hilfsweise vorgeschlagene Vorabentscheidungsfrage in der durch den Gerichtshof abgeänderten Form zu stellen.

B.22. Das angefochtene Gesetz soll außerdem eine effektive strafrechtliche Untersuchung und eine wirksame Bestrafung des sexuellen Missbrauchs von Minderjährigen ermöglichen und die wirkliche Identifizierung des Täters einer solchen Straftat ermöglichen, auch wenn von elektronischen Kommunikationsmitteln Gebrauch gemacht wird. Bei der Sitzung wurde in diesem Zusammenhang auf die positiven Verpflichtungen hingewiesen, die sich aus den Artikeln 3 und 8 der Europäischen Menschenrechtskonvention hinsichtlich des Schutzes der körperlichen und seelischen Unversehrtheit von Minderjährigen und anderen schutzbedürftigen Personen ergeben, wie sie vom Europäischen Gerichtshof für Menschenrechte ausgelegt werden (EuGHMR, 2. Dezember 2008, *K.U.* gegen Finnland, §§ 46-49). Diese Verpflichtungen könnten sich ebenfalls aus den entsprechenden Bestimmungen der Charta der Grundrechte der Europäischen Union ergeben, was Folgen für die Auslegung von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG haben könnte.

B.23. Es ist somit die zweite Vorabentscheidungsfrage zu stellen, die im Tenor angegeben ist.

B.24. Schließlich ist die dritte Vorabentscheidungsfrage zu stellen, die im Tenor aufgeführt ist.

Aus diesen Gründen:

Der Gerichtshof

a) stellt vor der Urteilsfällung zur Sache dem Gerichtshof der Europäischen Union folgende Vorabscheidungsfragen:

1. Ist Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit dem Recht auf Sicherheit, das durch Artikel 6 der Charta der Grundrechte der Europäischen Union garantiert wird, und dem Recht auf Schutz der personenbezogenen Daten, wie es durch die Artikel 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union garantiert wird, dahin auszulegen, dass er einer nationalen Regelung wie der des Ausgangsverfahrens entgegensteht, die eine allgemeine Verpflichtung für Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsieht, die Verkehrs- und Standortdaten im Sinne der Richtlinie 2002/58/EG auf Vorrat zu speichern, die von ihnen im Rahmen der Bereitstellung dieser Dienste erzeugt oder verarbeitet werden, wenn diese nationale Regelung nicht nur das Ziel der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, sondern auch die Sicherstellung der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit, die Ermittlung, Feststellung und Verfolgung von anderen Taten als denen der schweren Kriminalität oder die Verhütung eines untersagten Gebrauchs von elektronischen Kommunikationssystemen oder die Erreichung eines sonstigen Ziels verfolgt, das in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführt ist und das zudem den in diesen Rechtsvorschriften für die Vorratsspeicherung von Daten und den Zugang zu diesen genau festgelegten Garantien unterliegt?

2. Ist Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit den Artikeln 4, 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er einer nationalen Regelung wie der des Ausgangsverfahrens entgegensteht, die eine allgemeine Verpflichtung für Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsieht, die Verkehrs- und Standortdaten im Sinne der Richtlinie 2002/58/EG auf Vorrat zu speichern, die von ihnen im Rahmen der Bereitstellung dieser Dienste erzeugt oder verarbeitet werden, wenn diese nationale Regelung insbesondere den Zweck hat, positive Verpflichtungen zu erfüllen, die der Behörde aufgrund von Artikel 4 und 8 der Charta obliegen, und die darin besteht, einen gesetzlichen Rahmen vorzusehen, der eine wirksame strafrechtliche Ermittlung und eine wirksame Ahndung des sexuellen Missbrauchs von Minderjährigen ermöglicht und der eine wirkliche Identifizierung des Täters der Straftat ermöglicht, auch wenn von elektronischen Kommunikationsmitteln Gebrauch gemacht wird?

3. Falls der Verfassungsgerichtshof auf der Grundlage der Antworten auf die erste oder zweite Vorabentscheidungsfrage zu dem Schluss gelangen sollte, dass das angefochtene Gesetz gegen eine oder mehrere der Verpflichtungen verstößt, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, könnte er die Folgen des Gesetzes vom 29. Mai 2016 über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das Gesetz angestrebten Ziele benutzt werden können?

b) setzt im Übrigen die Prüfung der Rechtssachen aus, bis der Gerichtshof der Europäischen Union ein Urteil gefällt hat in den Rechtssachen C-207/16 *Ministerio Fiscal* und C-623/17 *Privacy International / Secretary of State for Foreign and Commonwealth Affairs u. a.*

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 19. Juli 2018.

Der Kanzler, Der Präsident,

P.-Y. Dutilleux J. Spreutels