LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

COUR CONSTITUTIONNELLE

[2021/202174]

Extrait de l'arrêt n° 57/2021 du 22 avril 2021

Numéros du rôle : 6590, 6597, 6599 et 6601

En cause : les recours en annulation de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques », introduits par l'Ordre des barreaux francophones et germanophone, par l'ASBL « Académie Fiscale » et Jean Pierre Riquet, par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme » et par Patrick Van Assche et autres.

La Cour constitutionnelle,

composée des présidents F. Daoût et L. Lavrysen, et des juges J.-P. Moerman, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques et Y. Kherbache, assistée du greffier F. Meersschaut, présidée par le président F. Daoût,

après en avoir délibéré, rend l'arrêt suivant :

I. *Objet des recours et procédure*

a. Par requête adressée à la Cour par lettre recommandée à la poste le 10 janvier 2017 et parvenue au greffe le 11 janvier 2017, l'Ordre des barreaux francophones et germanophone, assisté et représenté par Me E. Lemmens et Me J.-F. Henrotte, avocats au barreau de Liège, a introduit un recours en annulation de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » (publiée au *Moniteur belge* du 18 juillet 2016).

b. Par requête adressée à la Cour par lettre recommandée à la poste le 16 janvier 2017 et parvenue au greffe le 17 janvier 2017, un recours en annulation de la même loi a été introduit par l'ASBL « Académie Fiscale » et Jean Pierre Riquet.

c. Par requête adressée à la Cour par lettre recommandée à la poste le 17 janvier 2017 et parvenue au greffe le 18 janvier 2017, un recours en annulation de la même loi a été introduit par l'ASBL « Liga voor Mensenrechten », assistée et représentée par Me J. Vander Velpen, avocat au barreau d'Anvers, et l'ASBL « Ligue des Droits de l'Homme », assistée et représentée par Me R. Jespers, avocat au barreau d'Anvers.

d. Par requête adressée à la Cour par lettre recommandée à la poste le 18 janvier 2017 et parvenue au greffe le 19 janvier 2017, un recours en annulation de la même loi a été introduit par Patrick Van Assche, Christel Van Akeleyen et Karina De Hoog, assistés et représentés par Me D. Pattyn, avocat au barreau de Flandre occidentale.

Ces affaires, inscrites sous les numéros 6590, 6597, 6599 et 6601 du rôle de la Cour, ont été jointes.

Par arrêt interlocutoire n° 96/2018 du 19 juillet 2018, publié au *Moniteur belge* du 27 septembre 2018, la Cour a posé à la Cour de justice de l'Union européenne les questions préjudicielles suivantes :

« 1. L'article 15, paragraphe 1, de la Directive 2002/58/CE, lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, § 1er, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la Directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communication électronique, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe 1, du règlement (UE) 2016/679 et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci ?

2. L'article 15, paragraphe 1, de la Directive 2002/58/CE, combiné avec les articles 4, 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la Directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, si cette réglementation a notamment pour objet de réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et 8 de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques ?

3. Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi ? ».

Par arrêt du 6 octobre 2020 dans les affaires C-511/18, C-512/18 et C-520/18, la Cour de justice de l'Union européenne a répondu aux questions.

(...)

II. *En droit*

(...)

Quant à la loi attaquée et à son contexte

B.1. Les parties requérantes demandent l'annulation de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques », qui dispose :

« 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 nº 84/2015 de la Cour constitutionnelle, les modifications suivantes sont apportées :

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

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

b) au lieu du 74º, annulé par l'arrêt nº 84/2015 de la Cour constitutionnelle, il est inséré un 74º rédigé comme suit :

' 74º " 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 nº 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 :

1º 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

2º 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 :

1º 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;

2º 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;

3º 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;

4º 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;

5º 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;

6º 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, 7º, 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 :

1º 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;

2º 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;

3º 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;

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

5º 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 nº 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 :

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

2º 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. ';

3º 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 :

1º la nature de la méthode spécifique;

2º 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;

3º la menace potentielle qui justifie la méthode spécifique;

4º 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 2º et le 3º;

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

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

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

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

9º 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;

10º 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;

11º la date de la décision;

12º 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. Par la loi attaquée, le législateur a entendu répondre à l'annulation, par l'arrêt de la Cour n° 84/2015 du 11 juin 2015, de l'article 126 de la loi du 13 juin 2005 « relative aux communications électroniques » (ci-après : la loi du 13 juin 2005), tel qu'il avait été modifié par la loi du 30 juillet 2013 « portant modification des articles 2, 126, et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1567/001, p. 4).

B.3. Il ressort des travaux préparatoires de la loi attaquée que le législateur a examiné en profondeur tant l'arrêt précité de la Cour n° 84/2015 du 11 juin 2015 que l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014, dans les affaires jointes *Digital Rights Ireland Ltd* (C-293/12) et *Kärntner Landesregierung e.a.* (C-594/12), par lequel la Cour de justice a invalidé la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 « sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE », et sur lequel l'arrêt n° 84/2015 est basé.

L'objectif que le législateur poursuit par la loi attaquée est non seulement de lutter contre le terrorisme et la pédopornographie mais également de pouvoir utiliser les données conservées dans une grande variété de situations dans lesquelles ces données peuvent être à la fois le point de départ mais également une étape de l'enquête pénale (*Doc. parl.* Chambre, 2015-2016, DOC 54-1567/001, p. 6).

B.4. Il ressort de l'exposé des motifs de la loi attaquée que le législateur a considéré qu'il était impossible, à la lumière de l'objectif poursuivi, de mettre en place une obligation de conservation ciblée et différenciée, et qu'il a choisi d'assortir l'obligation de conservation générale et indifférenciée de garanties strictes, tant sur le plan de la protection de la conservation que sur le plan de l'accès, afin de limiter à un minimum l'ingérence dans le droit au respect de la protection de la vie privée. À cet égard, il a été souligné qu'il est tout simplement impossible d'opérer une différenciation *a priori* en fonction des personnes, des périodes temporelles et des zones géographiques (*ibid.*, pp. 10-18).

Quant au fond

B.5. Le moyen unique dans les affaires nos 6590 et 6597 est pris de la violation, par la loi attaquée, des articles 10 et 11 de la Constitution, lus isolément ou en combinaison avec les articles 6 et 8 de la Convention européenne des droits de l'homme ainsi qu'avec les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne.

B.6.1. L'Ordre des barreaux francophones et germanophone, partie requérante dans l'affaire n° 6590, reproche à la loi attaquée de traiter de manière identique les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, dont notamment les avocats, et les autres utilisateurs de ces services. Cette partie requérante constate que la loi implique encore une obligation généralisée d'enregistrement et de conservation de certaines métadonnées, lesquelles permettent de déterminer si un avocat a été consulté par une personne physique ou morale, d'identifier cet avocat, d'identifier ses interlocuteurs et en particulier ses clients, ainsi que les date et heure de la communication. Cette obligation généralisée s'impose à l'ensemble des fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à internet, de courrier électronique par internet, de téléphonie par internet et de réseaux publics de communications électroniques.

B.6.2. La partie requérante dans l'affaire n° 6590 fait également grief à la loi attaquée de prévoir une obligation généralisée de conservation des données sans opérer de distinction entre les justiciables selon qu'ils font, ou non, l'objet d'une mesure d'enquête ou de poursuite pour des faits susceptibles de donner lieu à des condamnations pénales. Elle soutient encore que les catégories de données visées par la loi sont extrêmement larges et variées, en ce qu'elles concernent celles qui visent à identifier l'utilisateur ou l'abonné et les moyens de communication, 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, ainsi que les données de communication même si leur contenu est en revanche exclu.

B.7.1. Les parties requérantes dans l'affaire nº 6597 reprochent à la loi attaquée de traiter de manière identique les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, dont notamment les professionnels comptables et fiscaux, et les autres utilisateurs de ces services sans tenir compte du statut particulier des professionnels comptables et fiscaux, du caractère fondamental du secret professionnel auquel ils sont soumis et de la nécessaire relation de confiance qui doit les unir à leurs clients.

B.7.2. Elles reprochent également à la loi attaquée de traiter de manière identique les justiciables qui font l'objet de mesures d'enquête ou de poursuite pour des faits susceptibles de s'inscrire dans les finalités de la conservation des données électroniques litigieuses et ceux qui ne font pas l'objet de telles mesures.

B.8.1. Le premier moyen dans l'affaire nº 6599 est pris de la violation des articles 10, 11, 12, 15, 22 et 29 de la Constitution, lus isolément ou en combinaison avec les articles 5, 8, 9, 10, 11, 14, 15, 17 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec le principe général de sécurité juridique, de proportionnalité, de droit à l'autodétermination en matière d'information ainsi qu'avec l'article 5, paragraphe 4, du Traité sur l'Union européenne.

B.8.2. L'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme » (devenue entretemps « Ligue des droits humains »), parties requérantes dans l'affaire nº 6599, reprochent à la loi attaquée de prévoir une obligation générale de conservation des données, ce qui oblige les opérateurs et les fournisseurs de services téléphoniques publics (y compris la téléphonie par internet), d'accès à internet et de courrier électronique par internet ainsi que les fournisseurs de réseaux publics de communications électroniques, à conserver durant douze mois, *de facto* pour tous les Belges, suspects ou non, les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile et la téléphonie par internet, et les données relatives à l'accès à internet, et à les mettre à la disposition de la police et de la justice, des services de renseignement et de sécurité, des services d'urgence, de la Cellule des personnes disparues ainsi que du Service de médiation pour les télécommunications.

B.9.1. Le premier moyen dans l'affaire nº 6601 est pris de la violation, par la loi attaquée, de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8, 11, paragraphe 1, et 52 de la Charte des droits fondamentaux de l'Union européenne, des articles 10, 11, 19 et 22 de la Constitution, de l'article 2, point *a)*, de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », ainsi que des articles 1er, 2, 3, 5, 6, 9 et 15 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) » (ci-après : la Directive 2002/58/CE).

B.9.2. Les parties requérantes dans l'affaire nº 6601 sont des personnes physiques qui habitent en Belgique et utilisent différents services de communications électroniques dans le cadre d'un contrat conclu avec un opérateur. Dans la première branche du premier moyen, elles font grief à la loi attaquée d'imposer une obligation générale et indifférenciée de conservation des données d'identification, de connexion et de localisation ainsi que des données de communication personnelles à charge des fournisseurs de services de téléphonie, en ce compris par internet, d'accès à internet, de courrier électronique par internet, aux opérateurs qui fournissent des réseaux publics de communications électroniques ainsi qu'aux opérateurs qui fournissent un de ces services.

B.10. Compte tenu de leur connexité, les moyens exposés dans les diverses affaires sont examinés ensemble.

B.11.1. Compte tenu, d'une part, des divergences de vues entre les parties requérantes et le Conseil des ministres quant à l'interprétation à donner à plusieurs dispositions, notamment l'article 15, paragraphe 1, de la Directive 2002/58/CE et les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne, que la Cour doit associer à son contrôle de la loi attaquée, et, d'autre part, des explications avancées par le Conseil des ministres pour justifier la compatibilité de la loi attaquée avec les normes de référence invoquées par les parties requérantes, la Cour a, par son arrêt nº 96/2018 du 19 juillet 2018, posé à la Cour de justice de l'Union européenne les trois questions préjudicielles suivantes :

« 1. L'article 15, paragraphe 1, de la Directive 2002/58/CE, lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, § 1er, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la Directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communication électronique, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe 1, du règlement (UE) 2016/679 et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci ?

2. L'article 15, paragraphe 1, de la Directive 2002/58/CE, combiné avec les articles 4, 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la Directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, si cette réglementation a notamment pour objet de réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et 8 de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques ?

3. Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi ? ».

B.11.2. L'article 15, paragraphe 1, de la Directive 2002/58/CE dispose :

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

B.11.3. La Cour a également décidé de suspendre l'examen des affaires jusqu'à ce que la Cour de justice ait statué dans les affaires en cause *Ministerio Fiscal* (C-207/16) et en cause *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e.a.* (C-623/17).

B.12. Par son arrêt du 2 octobre 2018 en cause *Ministerio Fiscal* (C-207/16), la Cour de justice a jugé, en grande chambre, que l'article 15, paragraphe 1, de la Directive 2002/58/CE, lu à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte des droits fondamentaux de l'Union européenne, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave. Cet arrêt repose sur la motivation suivante :

« *Sur le fond*

48. Par ses deux questions, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui présente une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave et, dans l'affirmative, à l'aune de quels critères la gravité de l'infraction en cause doit être appréciée.

49. À cet égard, il ressort de la décision de renvoi que, comme l'a relevé en substance M. l'avocat général au point 38 de ses conclusions, la demande de décision préjudicielle ne vise pas à déterminer si les données à caractère personnel en cause au principal ont été conservées par les fournisseurs de services de communications électroniques dans le respect des conditions visées à l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte. Cette demande porte, ainsi qu'il ressort du point 46 du présent arrêt, uniquement sur la question de savoir si et dans quelle mesure l'objectif poursuivi par la réglementation en cause au principal est susceptible de justifier l'accès d'autorités publiques, telles que la police judiciaire, à de telles données, sans que les autres conditions d'accès résultant de cet article 15, paragraphe 1, fassent l'objet de cette demande.

50. En particulier, cette juridiction s'interroge sur les éléments à prendre en compte afin d'apprécier si les infractions au regard desquelles des autorités policières peuvent être autorisées, à des fins d'enquête, à accéder à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, sont d'une gravité suffisante pour justifier l'ingérence que comporte un tel accès dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, tels qu'interprétés par la Cour dans ses arrêts du 8 avril 2014, *Digital Rights Ireland e.a.* (C-293/12 et C-594/12, EU: C: 2014: 238), et *Tele2 Sverige et Watson e.a*.

51. Quant à l'existence d'une ingérence dans ces droits fondamentaux, il y a lieu de rappeler que, comme l'a relevé M. l'avocat général aux points 76 et 77 de ses conclusions, l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de ' grave ' et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Un tel accès constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, points 124 et 126 ainsi que jurisprudence citée].

52. En ce qui concerne les objectifs susceptibles de justifier une réglementation nationale, telle que celle en cause au principal, régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, il convient de rappeler que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la Directive 2002/58 revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt *Tele2 Sverige et Watson e.a.*, points 90 et 115).

53. Or, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, il y a lieu d'observer que le libellé de l'article 15, paragraphe 1, première phrase, de la Directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les ' infractions pénales ' en général.

54. À cet égard, la Cour a, certes, jugé que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées (voir, en ce sens, arrêt *Tele2 Sverige et Watson e.a.*, point 99).

55. La Cour a toutefois motivé cette interprétation par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne (voir, en ce sens, arrêt *Tele2 Sverige et Watson e.a.*, point 115).

56. En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de ' grave '.

57. En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'' infractions pénales ' en général.

58. Il convient donc, avant tout, de déterminer si, en l'occurrence, en fonction des circonstances de l'espèce, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire aux données en cause au principal comporterait doit être considérée comme étant ' grave '.

59. À cet égard, la demande en cause au principal par laquelle la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. Ainsi qu'il a été relevé au point 40 du présent arrêt, cette demande vise l'accès aux seuls numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne portent pas, comme l'ont confirmé tant le gouvernement espagnol que le ministère public lors de l'audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.

60. Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.

61. Dans ces conditions, l'accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d'ingérence ' grave ' dans les droits fondamentaux des personnes dont les données sont concernées.

62. Ainsi qu'il ressort des points 53 à 57 du présent arrêt, l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'' infractions pénales ' en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la Directive 2002/58, sans qu'il soit nécessaire que ces infractions soient qualifiées de ' graves '.

63. Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave ».

Dans le dispositif de l'arrêt, la Cour de justice a dit pour droit :

« L'article 15, paragraphe 1, de la Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la charte des droits fondamentaux, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave ».

B.13. Par son arrêt du 6 octobre 2020, en cause *Privacy International* (C-623/17), prononcé en grande chambre, la Cour de justice a jugé que l'article 15, paragraphe 1, de la Directive 2002/58/CE, lu à la lumière de l'article 4, paragraphe 2, du Traité sur l'Union européenne ainsi que des articles 7, 8, 11 et l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement. Cet arrêt repose sur la motivation suivante :

« *Sur la seconde question*

50. Par sa seconde question, la juridiction de renvoi cherche, en substance, à savoir si l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

51. À titre liminaire, il convient de rappeler que, selon les indications figurant dans la demande de décision préjudicielle, l'article 94 de la loi de 1984 autorise le ministre à imposer aux fournisseurs de services de communications électroniques, par voie d'instructions, lorsqu'il l'estime nécessaire dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger, de transmettre aux services de sécurité et de renseignement les données relatives aux communications en masse, ces données incluant les données relatives au trafic et les données de localisation ainsi que des informations sur les services utilisés, au sens de l'article 21, paragraphes 4 et 6, de la RIPA. Cette dernière disposition couvre, entre autres, les données nécessaires pour identifier la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, le numéro de téléphone de l'appelant et le numéro appelé, les adresses IP de la source et du destinataire de la communication ainsi que les adresses des sites Internet visités.

52. Une telle communication par transmission des données concerne l'ensemble des utilisateurs des moyens de communications électroniques, sans qu'il soit précisé si cette transmission doit intervenir en temps réel ou de manière différée. Une fois transmises, ces données sont, selon les indications figurant dans la demande de décision préjudicielle, conservées par les services de sécurité et de renseignement et demeurent à la disposition de ces derniers aux fins de leurs activités, à l'instar des autres bases de données que ces services détiennent. En particulier, les données ainsi recueillies, qui sont soumises à des traitements et à des analyses de masse et automatisés, peuvent être recoupées avec d'autres bases de données comportant différentes catégories de données à caractère personnel en masse ou être divulguées hors de ces services et à des États tiers. Enfin, ces opérations ne sont pas subordonnées à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante et ne donnent lieu à aucune information des personnes concernées.

53. La Directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la Directive 2002/58, que le législateur de l'Union a entendu ' faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée '.

54. À cet effet, l'article 5, paragraphe 1, de la Directive 2002/58 dispose que ' les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes '. Cette même disposition souligne également que, ' [e]n particulier, [les États membres] interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1 ', et précise que ' [ce] paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité. '

55. Ainsi, cet article 5, paragraphe 1, consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs, de stocker, sans le consentement de ceux-ci, ces communications et ces données. Eu égard au caractère général de son libellé, cette disposition couvre nécessairement toute opération permettant à des tiers de prendre connaissance des communications et des données y afférentes à des fins autres que l'acheminement d'une communication.

56. L'interdiction d'intercepter les communications et les données y afférentes figurant à l'article 5, paragraphe 1, de la Directive 2002/58 englobe donc toute forme de mise à disposition par les fournisseurs de services de communications électroniques de données relatives au trafic et de données de localisation à des autorités publiques, tels des services de sécurité et de renseignement, ainsi que la conservation desdites données par ces autorités, quelle que soit l'utilisation ultérieure qui est faite de celles-ci.

57. Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement (arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, point 109).

58. Toutefois, l'article 15, paragraphe 1, de la Directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, 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. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par l'un de ces motifs.

59. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la Directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêts du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, points 89 et 104, ainsi que du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, point 111).

60. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la Directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement, à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU: C: 2014: 238, points 25 et 70, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, points 91 et 92 ainsi que jurisprudence citée).

61. Ces mêmes questions se posent également pour d'autres types de traitement de données, tels que leur transmission à des personnes autres que les utilisateurs ou l'accès à ces données en vue de leur utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, points 122 et 123 ainsi que jurisprudence citée].

62. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la Directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, *Connolly/Commission*, C-274/99 P, EU: C: 2001: 127, point 39, et du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 93 et jurisprudence citée).

63. Toutefois, les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18, EU: C: 2020: 559, point 172 ainsi que jurisprudence citée).

64. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

65. Il convient d'ajouter que l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné (arrêt du 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18, EU: C: 2020: 559, point 175 ainsi que jurisprudence citée).

66. En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la Directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est ' nécessaire, appropriée et proportionnée, au sein d'une société démocratique ', au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être ' rigoureusement ' proportionnée au but poursuivi.

67. À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre l'objectif et les intérêts et droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, C-73/07, EU: C: 2008: 727, point 56; du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU: C: 2010: 662, points 76, 77 et 86, ainsi que du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU: C: 2014: 238, point 52; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 140].

68. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights Ireland* e.a., C-293/12 et C-594/12, EU: C: 2014: 238, points 54 et 55, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 117; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 141].

69. S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause au principal, satisfait aux exigences de l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, il convient de relever que la transmission des données relatives au trafic et des données de localisation à des personnes autres que les utilisateurs, telles que des services de sécurité et de renseignement, déroge au principe de confidentialité. Dès lors que cette opération est effectuée, comme en l'occurrence, de manière généralisée et indifférenciée, elle a pour effet de faire de la dérogation à l'obligation de principe de garantir la confidentialité des données la règle, alors que le système mis en place par la Directive 2002/58 exige qu'une telle dérogation demeure l'exception.

70. En outre, conformément à la jurisprudence constante de la Cour, la transmission des données relatives au trafic et des données de localisation à un tiers constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure qui est faite de ces données. À cet égard, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, points 124 et 126 ainsi que jurisprudence citée, et arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, points 115 et 116].

71. L'ingérence que comporte la transmission des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement dans le droit consacré à l'article 7 de la Charte doit être considérée comme étant particulièrement grave, compte tenu notamment du caractère sensible des informations que peuvent fournir ces données et, notamment, de la possibilité d'établir à partir de celles-ci le profil des personnes concernées, une telle information étant tout aussi sensible que le contenu même des communications. En outre, elle est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, arrêts du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU: C: 2014: 238, points 27 et 37, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, points 99 et 100).

72. Il convient de relever encore qu'une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la Directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (*JO* 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights Ireland* e.a., C-293/12 et C-594/12, EU: C: 2014: 238, point 28; du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 101, ainsi que du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, point 118).

73. Enfin, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

74. S'agissant des objectifs susceptibles de justifier de telles ingérences, plus particulièrement de l'objectif de sauvegarde de la sécurité nationale, en cause au principal, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme (arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, point 135).

75. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la Directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, mêmes graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs (arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, point 136).

76. Toutefois, pour satisfaire à l'exigence de proportionnalité rappelée au point 67 du présent arrêt, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, une réglementation nationale comportant une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte doit respecter les exigences résultant de la jurisprudence citée aux points 65, 67 et 68 du présent arrêt.

77. En particulier, s'agissant de l'accès d'une autorité à des données à caractère personnel, une réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 192 et jurisprudence citée].

78. Ainsi, et dès lors qu'un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, une réglementation nationale régissant l'accès aux données relatives au trafic et aux données de localisation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 119 et jurisprudence citée).

79. Ces exigences s'appliquent, a fortiori, à une mesure législative, telle que celle en cause au principal, sur le fondement de laquelle l'autorité nationale compétente peut imposer aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement. En effet, une telle transmission a pour effet de mettre ces données à la disposition des autorités publiques [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 212].

80. Dès lors que la transmission des données relatives au trafic et des données de localisation a lieu de manière généralisée et indifférenciée, elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement pourrait avoir un lien, même indirect ou lointain, avec l'objectif de sauvegarde de la sécurité nationale et, en particulier, sans que soit établie une relation entre les données dont la transmission est prévue et une menace pour la sécurité nationale (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU: C: 2014: 238, points 57 et 58, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 105). Eu égard au fait que la transmission de telles données aux autorités publiques équivaut, conformément à ce qui a été constaté au point 79 du présent arrêt, à un accès, il convient de considérer qu'une réglementation permettant une transmission généralisée et indifférenciée des données aux autorités publiques, implique un accès général.

81. Il en résulte qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte.

82. Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la seconde question que l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement ».

Dans le dispositif de l'arrêt, la Cour de justice a dit pour droit :

« 2) L'article 15, paragraphe 1, de la Directive 2002/58, telle que modifiée par la Directive 2009/136, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement ».

B.14. Par son arrêt du 6 octobre 2020, *La Quadrature du Net et autres* (C-511/18, C-512/18 et C-520/18), prononcé en grande chambre, la Cour de justice a répondu comme suit aux deux premières questions posées par la Cour par son arrêt nº 96/2018 :

« Sur les premières questions dans les affaires C-511/18 et C-512/18 ainsi que sur les première et deuxième questions dans l'affaire C-520/18

81. Par les premières questions dans les affaires C-511/18 et C-512/18 ainsi que par les première et deuxième questions dans l'affaire C-520/18, qu'il convient d'examiner conjointement, les juridictions de renvoi cherchent, en substance, à savoir si l'article 15, paragraphe 1, de la Directive 2002/58 doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs de services de communications électroniques, à des fins prévues à cet article 15, paragraphe 1, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

[...]

Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58

105. Il convient de rappeler, à titre liminaire, qu'il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (voir, en ce sens, arrêt du 17 avril 2018, *Egenberger*, C-414/16, EU: C: 2018: 257, point 44).

106. La Directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la Directive 2002/58, que le législateur de l'Union a entendu ' faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée '.

107. À cet effet, l'article 5, paragraphe 1, de la Directive 2002/58 consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et ces données.

108. S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, il ressort de l'article 6 ainsi que des considérants 22 et 26 de la Directive 2002/58 qu'un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 86 et jurisprudence citée).

109. Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.

110. Toutefois, l'article 15, paragraphe 1, de la Directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, 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. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par l'un de ces motifs.

111. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la Directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, points 89 et 104).

112. Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la Directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, point 52 et jurisprudence citée).

113. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la Directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, points 25 et 70, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, points 91 et 92 ainsi que jurisprudence citée).

114. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la Directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, *Connolly/Commission*, C-274/99 P, EU: C: 2001: 127, point 39, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 93 et jurisprudence citée).

115. Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la Directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, points 124 et 126 ainsi que jurisprudence citée; voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 30 janvier 2020, *Breyer c. Allemagne*, CE: ECHR: 2020: 0130JUD005000112, § 81].

116. Il est également sans pertinence que les données conservées soient ou non utilisées par la suite (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 16 février 2000, *Amann c. Suisse*, CE: ECHR: 2000: 0216JUD002779895, § 69, ainsi que 13 février 2020, *Trjakovski et Chipovski c. Macédonie du Nord*, CE: ECHR: 2020: 0213JUD005320513, § 51), l'accès à de telles données constituant, quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, points 124 et 126].

117. Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, point 27, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 99).

118. Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, point 28, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU: C: 2016: 970, point 101). Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la Directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (*JO* 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés.

119. D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

120. Cela étant, en ce qu'il permet aux États membres d'introduire les dérogations visées au point 110 du présent arrêt, l'article 15, paragraphe 1, de la Directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18, EU: C: 2020: 559, point 172 ainsi que jurisprudence citée).

121. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

122. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la Directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui.

123. À cet égard, l'article 6 de la Charte, auquel se réfèrent le Conseil d'État et la Cour constitutionnelle, consacre le droit de toute personne non seulement à la liberté mais également à la sûreté et garantit des droits correspondant à ceux qui le sont à l'article 5 de la CEDH (voir, en ce sens, arrêts du 15 février 2016, *N.*, C-601/15 PPU, EU: C: 2016: 84, point 47; du 28 juillet 2016, *JZ*, C-294/16 PPU, EU: C: 2016: 610, point 48, ainsi que du 19 septembre 2019, *Rayonna prokuratura Lom*, C-467/18, EU: C: 2019: 765, point 42 et jurisprudence citée).

124. En outre, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne. Il convient donc de tenir compte des droits correspondants de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimale [voir, en ce sens, arrêts du 12 février 2019, TC, C-492/18 PPU, EU: C: 2019: 108, point 57, ainsi que du 21 mai 2019, *Commission/Hongrie (Usufruits sur terres agricoles)*, C-235/17, EU: C: 2019: 432, point 72 et jurisprudence citée].

125. S'agissant de l'article 5 de la CEDH, qui consacre le ' droit à la liberté ' et le ' droit à la sûreté ', celui-ci vise, selon la jurisprudence de la Cour européenne des droits de l'homme, à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée (voir, en ce sens, Cour EDH, 18 mars 2008, *Ladent c. Pologne*, CE: ECHR: 2008: 0318JUD001103603, § § 45 et 46; 29 mars 2010, *Medvedyev et autres c. France*, CE: ECHR: 2010: 0329JUD000339403, § § 76 et 77, ainsi que 13 décembre 2012, *El-Masri v. ' The former Yugoslav Republic of Macedonia '*, CE: ECHR: 2012: 1213JUD003963009, § 239). Toutefois, dans la mesure où cette disposition vise une privation de liberté commise par une autorité publique, l'article 6 de la Charte ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales.

126. En revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, évoquée par la Cour constitutionnelle, il convient de souligner que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale [voir, en ce sens, arrêt du 18 juin 2020, *Commission/Hongrie (Transparence associative)*, C-78/18, EU: C: 2020: 476, point 123 et jurisprudence citée de la Cour européenne des droits de l'homme]. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants.

127. Or, face à ces différentes obligations positives, il convient de procéder à une conciliation nécessaire des différents intérêts et droits en cause.

128. En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la CEDH, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différentes intérêts et droits à protéger (Cour EDH, 28 octobre 1998, *Osman c. Royaume-Uni*, CE: ECHR: 1998: 1028JUD002345294, § § 115 et 116; 4 mars 2004, *M.C. c. Bulgarie*, CE: ECHR: 2003: 1204JUD003927298, § 151; 24 juin 2004, *Von Hannover c. Allemagne*, CE: ECHR: 2004: 0624JUD005932000, § § 57 et 58, ainsi que 2 décembre 2008, *K.U. c. Finlande*, CE: ECHR: 2008: 1202JUD 000287202, § § 46, 48 et 49).

129. En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la Directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est ' nécessaire, appropriée et proportionnée, au sein d'une société démocratique ', au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être ' rigoureusement ' proportionnée au but poursuivi.

130. À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, C-73/07, EU: C: 2008: 727, point 56; du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU: C: 2010: 662, points 76, 77 et 86, ainsi que du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, point 52; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 140].

131. Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la Directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, point 55 et jurisprudence citée).

132. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, points 54 et 55, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 117; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 141].

133. Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 191 et jurisprudence citée, ainsi que arrêt du 3 octobre 2019, *A e.a.*, C-70/18, EU: C: 2019: 823, point 63].

- Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale

134. Il y a lieu de faire observer que l'objectif de sauvegarde de la sécurité nationale, évoqué par les juridictions de renvoi et les gouvernements ayant présenté des observations, n'a pas encore été spécifiquement examiné par la Cour dans ses arrêts interprétant la Directive 2002/58.

135. À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

136. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la Directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

137. Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport.

138. L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.

139. Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale, telles que celles visées aux points 135 et 136 du présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues.

- Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique

140. Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général [voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU: C: 2016: 970, point 102, ainsi que du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, points 56 et 57; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU: C: 2017: 592, point 149].

141. Une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 107).

142. En effet, compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 118 du présent arrêt, que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit, comme le prévoit le système mis en place par la Directive 2002/58, l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître.

143. En outre, la Cour a souligné qu'une réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi. Une telle réglementation, contrairement à l'exigence rappelée au point 133 du présent arrêt, concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, points 57 et 58, ainsi que du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 105).

144. En particulier, comme l'a déjà jugé la Cour, une telle réglementation n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave (voir, en ce sens, arrêts du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU: C: 2014: 238, point 59, et du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 106).

145. Or, même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé aux points 126 et 128 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi.

146. En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation.

147. Ainsi, comme l'a déjà jugé la Cour, l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 108).

148. S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la Directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 111).

149. À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.

150. La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.

151. Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.

- Sur les mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique

152. Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.

153. Toutefois, les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt.

154. Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause exigée par la jurisprudence citée au point 130 du présent arrêt, il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, comme l'ont indiqué plusieurs gouvernements dans leurs observations soumises à la Cour, s'avérer impossible sans avoir recours à une mesure législative au titre de l'article 15, paragraphe 1, de la Directive 2002/58. Tel peut notamment être le cas, ainsi que l'ont fait valoir ces gouvernements, des infractions particulièrement graves en matière de pédopornographie, telles que l'acquisition, la diffusion, la transmission ou la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous *c)*, de la Directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (*JO* 2011, L 335, p. 1).

155. Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, au sens de la jurisprudence citée au point 133 du présent arrêt, avec les objectifs poursuivis et que les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.

156. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées.

157. En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, points 59 et 60).

158. Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la Directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, point 62).

159. Dans ces conditions, eu égard à la conciliation nécessaire des droits et des intérêts en cause et pour les raisons figurant aux points 131 et 158 du présent arrêt, il y a lieu de considérer que, même en l'absence de lien entre l'ensemble des utilisateurs des moyens de communications électroniques et les objectifs poursuivis, l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à une mesure législative imposant, sans délai particulier, aux fournisseurs de services de communications électroniques la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs des moyens de communications électroniques aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique, sans qu'il soit nécessaire que les infractions pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves.

- Sur les mesures législatives prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave

160. En ce qui concerne les données relatives au trafic et les données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la Directive 2002/58, ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de celle-ci, telles que décrites aux points 134 à 159 du présent arrêt, il y a lieu de relever que ces données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant cette directive, leur traitement et leur stockage.

161. Toutefois, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée.

162. À cet égard, il y a lieu de relever que la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens - n° 185), laquelle a été signée par les 27 États membres et ratifiée par 25 d'entre eux, et dont l'objectif est de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques, prévoit, à son article 14, que les parties contractantes adoptent aux fins d'enquêtes ou de procédures pénales spécifiques certaines mesures quant aux données relatives au trafic déjà stockées, telles que la conservation rapide de ces données. En particulier, l'article 16, paragraphe 1, de cette convention stipule que les parties contractantes adoptent les mesures législatives qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide des données relatives au trafic stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

163. Dans une situation telle que celle visée au point 161 du présent arrêt, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts en cause visée au point 130 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la Directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent.

164. Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

165. À cet égard, il importe de préciser qu'une telle conservation rapide ne doit pas être limitée aux données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale. Tout en respectant le cadre dressé par l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, et compte tenu des considérations figurant au point 133 du présent arrêt, une telle mesure peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. En outre, l'accès des autorités compétentes aux données ainsi conservées doit s'effectuer dans le respect des conditions résultant de la jurisprudence ayant interprété la Directive 2002/58 (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU: C: 2016: 970, points 118 à 121 et jurisprudence citée).

166. Il convient encore d'ajouter que, ainsi qu'il ressort en particulier des points 115 et 133 du présent arrêt, l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la Directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale.

167. À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la Directive 2002/58.

168. Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 que l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives

- permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

- permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

Dans le dispositif de l'arrêt, la Cour de justice a dit pour droit :

« 1) L'article 15, paragraphe 1, de la Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la Directive 2002/58, telle que modifiée par la Directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives

- permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

- permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

[...] ».

B.15. Il ressort de l'arrêt de la Cour de justice du 6 octobre 2020 en cause *La Quadrature du Net et autres*, précité, que l'article 15, paragraphe 1, de la Directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, sauf dans les hypothèses limitées décrites par l'arrêt précité.

En ce qu'elle prévoit, par principe et sans limitation à ces hypothèses, une conservation généralisée et indifférenciée, par les opérateurs et fournisseurs de services de communications électroniques, des données d'identification, des données d'accès et de connexion, ainsi que des données de communication, visées à l'article 126, § 3, de la loi du 13 juin 2005, la loi attaquée viole par conséquent l'article 15, paragraphe 1, de la Directive 2002/58/CE, lu à la lumière des dispositions précitées de la Charte des droits fondamentaux de l'Union européenne, et en combinaison avec les articles 10 et 11 de la Constitution.

B.16.1. Dans le dispositif de l'arrêt du 6 octobre 2020 en cause *La Quadrature du Net et autres*, précité, la Cour de justice précise cependant que l'article 15, paragraphe 1, de la Directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, ne s'oppose pas à divers types de mesures législatives que la Cour énumère. Sont ainsi admissibles, notamment, des mesures législatives « prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire », ou encore des mesures législatives « prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ». Ces mesures législatives doivent assurer, « par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

B.16.2. Sur la base de ces précisions de la Cour de justice, le Conseil des ministres soutient dans ses mémoires complémentaires qu'en tout état de cause, la loi attaquée ne doit pas être annulée en ce qu'elle prévoit l'obligation généralisée et indifférenciée de conservation, par les opérateurs et fournisseurs de services de communications électroniques, des adresses IP attribuées à la source d'une connexion, d'une part, et des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, d'autre part.

Le Conseil des ministres en conclut que seuls doivent être annulés, le cas échéant, les alinéas 2 et 3 de l'article 126, § 3, de la loi du 13 juin 2005, qui visent respectivement les données de connexion et de localisation et les données de communication. Il estime que l'alinéa 1er de l'article 126, § 3, précité, qui vise les données d'identification, ne doit en revanche pas être annulé, pas plus que les autres dispositions de la loi attaquée, dès lors qu'elles contiennent les garanties nécessaires en termes de conservation des données et d'accès à celles-ci.

B.17. En l'espèce, il y a lieu de constater que la loi attaquée repose, dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l'ensemble des données visées à l'article 126, § 3, de la loi du 13 juin 2005, et qu'elle poursuit, d'une manière générale, comme il est dit en B.3 et en B.4, des objectifs plus larges que la lutte contre la criminalité grave ou le risque d'atteinte à la sécurité publique.

La distinction que l'article 126, § 3, de la loi du 13 juin 2005 opère entre trois catégories de données (à savoir : les données d'identification, les données d'accès et de connexion, ainsi que les données de communication) n'a d'incidence que sur le point de départ de la durée de conservation des données, de douze mois en toute hypothèse, et éventuellement sur les possibilités d'accéder à celles-ci, pour les instances habilitées (voy. l'article 46*bis* du Code d'instruction criminelle et l'article 126, § 2, de la loi du 13 juin 2005). Cette catégorisation ne correspond par ailleurs pas aux distinctions qui sont opérées par la Cour de justice dans son arrêt du 6 octobre 2020 en ce qui concerne les différentes catégories de données susceptibles de faire l'objet d'une obligation de conservation généralisée et indifférenciée, moyennant le respect de plusieurs conditions (à savoir, en l'occurrence : les adresses IP attribuées à la source d'une connexion et les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques).

B.18. L'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué : l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours « répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi » (pointss 132 et 133).

B.19. Il appartient au législateur d'élaborer une réglementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatibles avec l'article 15, paragraphe 1, de la Directive 2002/58/CE, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. En particulier, il appartient également au législateur, dans ce contexte, d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire.

B.20. Compte tenu de ce qui précède, il y a lieu d'annuler les articles 2, *b)*, 3 à 11 et 14 de la loi attaquée, qui sont indissociablement liés.

B.21. Les autres moyens dans les affaires nos 6599 et 6601 concernent également la conservation généralisée et indifférenciée des données relatives aux communications électroniques et l'accès à celles-ci. Dès lors qu'ils ne peuvent conduire à une annulation plus étendue, il n'y a pas lieu de les examiner.

Quant au maintien des effets

B.22. Dans ses mémoires en réplique, le Conseil des ministres demande à la Cour, à titre infiniment subsidiaire, de maintenir les effets des dispositions qui seraient le cas échéant annulées, afin de ne pas mettre en péril le travail de recherche et de poursuites des infractions exécuté par les services de police et de renseignement.

B.23.1. L'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle dispose :

« Si la Cour l'estime nécessaire, elle indique, par voie de disposition générale, ceux des effets des dispositions annulées qui doivent être considérés comme définitifs ou maintenus provisoirement pour le délai qu'elle détermine ».

B.23.2. En la matière, la Cour doit tenir compte des limitations qui découlent du droit de l'Union européenne quant au maintien des effets des normes nationales qui doivent être annulées parce qu'elles sont contraires à ce droit (CJUE, grande chambre, 8 septembre 2010, C-409/06, *Winner Wetten*, points 53-69; CJUE, grande chambre, 28 février 2012, C-41/11, *Inter-Environnement Wallonie et Terre wallonne*, points 56-63).

En règle générale, ce maintien des effets ne peut avoir lieu qu'aux conditions qui sont fixées par la Cour de justice en réponse à une question préjudicielle.

B.24.1. En réponse à la troisième question préjudicielle posée par la Cour quant à un éventuel maintien des effets de la loi attaquée, la Cour de justice a jugé :

« Sur la troisième question dans l'affaire C-520/18

213. Par la troisième question dans l'affaire C-520/18, la juridiction de renvoi cherche, en substance, à savoir si une juridiction nationale peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, entre autres, de la poursuite des objectifs de sauvegarde de la sécurité nationale et de lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, résultant de son caractère incompatible avec l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

214. Le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes normes de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces différentes normes sur le territoire desdits États [arrêts du 15 juillet 1964, *Costa*, 6/64, EU: C: 1964: 66, pp. 1159 et 1160, ainsi que du 19 novembre 2019, *A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême)*, C-585/18, C-624/18 et C-625/18, EU: C: 2019: 982, points 157 et 158 et jurisprudence citée].

215. En vertu du principe de primauté, à défaut de pouvoir procéder à une interprétation de la réglementation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel [arrêts du 22 juin 2010, *Melki et Abdeli*, C-188/10 et C-189/10, EU: C: 2010: 363, point 43 et jurisprudence citée; du 24 juin 2019, *Popławski*, C-573/17, EU: C: 2019: 530, point 58, ainsi que du 19 novembre 2019, *A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême)*, C-585/18, C-624/18 et C-625/18, EU: C: 2019: 982, point 160].

216. Seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée [voir, en ce sens, arrêts du 23 octobre 2012, *Nelson e.a.*, C-581/10 et C-629/10, EU: C: 2012: 657, points 89 et 91; du 23 avril 2020, *Herst*, C-401/18, EU: C: 2020: 295, points 56 et 57, ainsi que du 25 juin 2020, *A e.a. (Éoliennes à Aalter et à Nevele)*, C-24/19, EU: C: 2020: 503, point 84 et jurisprudence citée].

217. Il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (voir, en ce sens, arrêt du 29 juillet 2019, *Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU: C: 2019: 622, point 177 ainsi que jurisprudence citée).

218. Toutefois, la Cour a jugé, dans une affaire où était en cause la légalité de mesures adoptées en méconnaissance de l'obligation édictée par le droit de l'Union d'effectuer une évaluation préalable des incidences d'un projet sur l'environnement et sur un site protégé, qu'une juridiction nationale peut, si le droit interne le permet, exceptionnellement maintenir les effets de telles mesures lorsque ce maintien est justifié par des considérations impérieuses liées à la nécessité d'écarter une menace réelle et grave de rupture de l'approvisionnement en électricité de l'État membre concerné, à laquelle il ne pourrait être fait face par d'autres moyens et alternatives, notamment dans le cadre du marché intérieur, ledit maintien ne pouvant couvrir que le laps de temps strictement nécessaire pour remédier à cette illégalité (voir, en ce sens, arrêt du 29 juillet 2019, *Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU: C: 2019: 622, points 175, 176, 179 et 181).

219. Or, contrairement à l'omission d'une obligation procédurale telle que l'évaluation préalable des incidences d'un projet dans le domaine spécifique de la protection de l'environnement, une méconnaissance de l'article 15, paragraphe 1, de la Directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle mentionnée au point précédent. En effet, le maintien des effets d'une législation nationale, telle que celle en cause au principal, signifierait que cette législation continue à imposer aux fournisseurs de services de communications électroniques des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées.

220. Partant, la juridiction de renvoi ne saurait faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, de la législation nationale en cause au principal.

221. Cela étant, dans leurs observations soumises à la Cour, VZ, WY et XX font valoir que la troisième question soulève, implicitement mais nécessairement, le point de savoir si le droit de l'Union s'oppose à une exploitation, dans le cadre d'une procédure pénale, des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec ce droit.

222. À cet égard et afin de donner une réponse utile à la juridiction de renvoi, il y a lieu de rappeler que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, d'informations et d'éléments de preuve qui ont été obtenus par une telle conservation de données contraire au droit de l'Union.

223. En effet, il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (voir, en ce sens, arrêts du 6 octobre 2015, *Târşia*, C-69/14, EU: C: 2015: 662, points 26 et 27; du 24 octobre 2018, *XC e.a.*, C-234/17, EU: C: 2018: 853, points 21 et 22 ainsi que jurisprudence citée, et du 19 décembre 2019, *Deutsche Umwelthilfe*, C-752/18, EU: C: 2019: 1114, point 33).

224. En ce qui concerne le principe d'équivalence, il appartient au juge national saisi d'une procédure pénale fondée sur des informations ou des éléments de preuve obtenus en méconnaissance des exigences résultant de la Directive 2002/58 de vérifier si le droit national régissant cette procédure prévoit des règles moins favorables en ce qui concerne l'admissibilité et l'exploitation de telles informations et de tels éléments de preuve que celles régissant les informations et les éléments de preuve obtenus en violation du droit interne.

225. Quant au principe d'effectivité, il convient de relever que les règles nationales relatives à l'admissibilité et à l'exploitation des informations et des éléments de preuve ont pour objectif, en vertu des choix opérés par le droit national, d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales. Or, cet objectif peut, selon le droit national, être atteint non seulement par une interdiction d'exploiter de telles informations et de tels éléments de preuve, mais également par des règles et des pratiques nationales régissant l'appréciation et la pondération des informations et des éléments de preuve, voire par une prise en considération de leur caractère illégal dans le cadre de la détermination de la peine.

226. Cela étant, il ressort de la jurisprudence de la Cour que la nécessité d'exclure des informations et des éléments de preuve obtenus en méconnaissance des prescriptions du droit de l'Union doit être appréciée au regard, notamment, du risque que l'admissibilité de tels informations et éléments de preuve comporte pour le respect du principe du contradictoire et, partant, du droit à un procès équitable (voir, en ce sens, arrêt du 10 avril 2003, *Steffensen*, C-276/01, EU: C: 2003: 228, points 76 et 77). Or, une juridiction qui considère qu'une partie n'est pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation (voir, en ce sens, arrêt du 10 avril 2003, *Steffensen*, C-276/01, EU: C: 2003: 228, points 78 et 79).

227. Partant, le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

228. Eu égard aux considérations qui précèdent, il y a lieu de répondre à la troisième question dans l'affaire C-520/18 qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits ».

Dans le dispositif de l'arrêt, la Cour de justice a dit pour droit :

« 4) Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la Directive 2002/58, telle que modifiée par la Directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits ».

B.24.2. Il ressort de l'arrêt précité que la Cour n'est pas fondée à maintenir provisoirement les effets des dispositions annulées.

B.24.3. Il appartient au juge pénal compétent de statuer, le cas échéant, sur l'admissibilité des preuves qui ont été recueillies lors de la mise en œuvre des dispositions annulées, conformément à l'article 32 du titre préliminaire du Code de procédure pénale et à la lumière des précisions apportées par la Cour de justice dans l'arrêt du 6 octobre 2020 précité.

Par ces motifs,

la Cour

annule les articles 2, *b)*, 3 à 11 et 14 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » et rejette les recours pour le surplus.

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 22 avril 2021.

Le greffier, Le président,

F. Meersschaut F. Daoût

GRONDWETTELIJK HOF

[2021/202174]

Uittreksel uit arrest nr. 57/2021 van 22 april 2021

Rolnummers 6590, 6597, 6599 en 6601

In zake : de beroepen tot vernietiging van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie », ingesteld door de « Ordre des barreaux francophones et germanophone », door de vzw « Académie Fiscale » en Jean Pierre Riquet, door de vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme » en door Patrick Van Assche en anderen.

Het Grondwettelijk Hof,

samengesteld uit de voorzitters F. Daoût en L. Lavrysen, en de rechters J.-P. Moerman, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques en Y. Kherbache, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter F. Daoût,

wijst na beraad het volgende arrest :

I. *Onderwerp van de beroepen en rechtspleging*

a. Bij verzoekschrift dat aan het Hof is toegezonden bij op 10 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 11 januari 2017, heeft de « Ordre des barreaux francophones et germanophone », bijgestaan en vertegenwoordigd door Mr. E. Lemmens en Mr. J.-F. Henrotte, advocaten bij de balie te Luik, beroep tot vernietiging ingesteld van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » (bekendgemaakt in het *Belgisch Staatsblad* van 18 juli 2016).

b. Bij verzoekschrift dat aan het Hof is toegezonden bij op 16 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 17 januari 2017, is beroep tot vernietiging ingesteld van dezelfde wet door de vzw « Académie Fiscale » en Jean Pierre Riquet.

c. Bij verzoekschrift dat aan het Hof is toegezonden bij op 17 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 18 januari 2017, is beroep tot vernietiging ingesteld van dezelfde wet door de vzw « Liga voor Mensenrechten », bijgestaan en vertegenwoordigd door Mr. J. Vander Velpen, advocaat bij de balie van Antwerpen, en de vzw « Ligue des Droits de l'Homme », bijgestaan en vertegenwoordigd door Mr. R. Jespers, avocaat bij de balie van Antwerpen.

d. Bij verzoekschrift dat aan het Hof is toegezonden bij op 18 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 19 januari 2017, is beroep tot vernietiging ingesteld van dezelfde wet door Patrick Van Assche, Christel Van Akeleyen en Karina De Hoog, bijgestaan en vertegenwoordigd door Mr. D. Pattyn, advocaat bij de balie van West-Vlaanderen.

Die zaken, ingeschreven onder de nummers 6590, 6597, 6599 en 6601 van de rol van het Hof, werden samengevoegd.

Bij tussenarrest nr. 96/2018 van 19 juli 2018, bekendgemaakt in het *Belgisch Staatsblad* van 27 september 2018, heeft het Hof de volgende prejudiciële vragen gesteld aan het Hof van Justitie van de Europese Unie :

« 1. Dient artikel 15, lid 1, van de Richtlijn 2002/58/EG, in samenhang gelezen met het recht op veiligheid, gewaarborgd bij artikel 6 van het Handvest van de grondrechten van de Europese Unie, en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de Richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, nationale regeling die niet alleen ten doel heeft het onderzoeken, opsporen en vervolgen van feiten van zware criminaliteit, maar ook het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit of het voorkomen van een verboden gebruik van de elektronische communicatiesystemen, of de verwezenlijking van een andere doelstelling die is geïdentificeerd bij artikel 23, lid 1, van de Verordening (EU) 2016/679 en die bovendien onderworpen is aan nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe ?

2. Dient artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 4, 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de Richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, indien die regeling mede tot doel heeft om de op de overheid rustende positieve verplichtingen ingevolge de artikelen 4 en 8 van het Handvest te bewerkstelligen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt en het effectief mogelijk maakt om de pleger van het misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronische communicatiemiddelen ?

3. Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden ? ».

Bij arrest van 6 oktober 2020 in de zaken C-511/18, C-512/18 en C-520/18 heeft het Hof van Justitie van de Europese Unie op de vragen geantwoord.

(...)

II. *In rechte*

(...)

Ten aanzien van de bestreden wet en de context ervan

B.1. De verzoekende partijen vorderen de vernietiging van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie », die bepaalt :

« HOOFDSTUK 1. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

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

Art. 2. In artikel 2 van de wet [van] 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van 18 december 2015, en gedeeltelijk vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, worden de volgende wijzigingen aangebracht :

a) de bepaling onder 11° wordt vervangen als volgt :

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

b) in de plaats van de bepaling onder 74°, vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, wordt een als volgt luidende bepaling onder 74° ingevoegd :

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

Art. 3. Artikel 125, § 2, van dezelfde wet wordt opgeheven.

Art. 4. In dezelfde wet wordt in de plaats van artikel 126, vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, het als volgt luidende artikel 126 ingevoegd :

' Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, dienen de aanbieders aan het publiek van telefoniediensten, via internet inbegrepen, van internettoegang, van e-mail via het internet, de operatoren die openbare elektronische-communicatienetwerken aanbieden, alsook de operatoren die een van deze diensten verstrekken, de in paragraaf 3 bedoelde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Dit artikel heeft geen betrekking op de inhoud van de communicatie.

De verplichting om de in paragraaf 3 bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten :

1° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren van openbare elektronische-communicatiediensten of van een openbaar netwerk voor elektronische communicatie, of

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

§ 2. Enkel de volgende overheden mogen op eenvoudig verzoek van de in paragraaf 1, eerste lid, bedoelde aanbieders en operatoren gegevens ontvangen die worden bewaard krachtens dit artikel om de doeleinden en volgens de hieronder opgesomde voorwaarden :

1° de gerechtelijke autoriteiten, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken, voor de uitvoering van de in de artikelen 46*bis* en 88*bis* van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen;

2° de inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren van gegevens zoals bedoeld in de artikelen 16/2, 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten te vervullen en volgens de voorwaarden vastgelegd in die wet;

3° elke officier van gerechtelijke politie van het Instituut, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de artikelen 114, 124 en dit artikel;

4° de hulpdiensten die hulp ter plaatse bieden, wanneer ze naar aanleiding van een noodoproep, van de betrokken aanbieder of operator niet de identificatiegegevens van de oproeper ontvangen met behulp van de databank beoogd in artikel 107, § 2, derde lid, of onvolledige of onjuiste gegevens krijgen. Enkel de identificatiegegevens van de oproeper mogen worden gevraagd en uiterlijk binnen 24 uur na de oproep;

5° de officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood, opsporing van personen van wie de verdwijning onrustwekkend is en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is. Enkel de gegevens die zijn beoogd in paragraaf 3, eerste en tweede lid, met betrekking tot de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan het verzoek om de gegevens te krijgen, mogen worden gevraagd aan de operator of de aanbieder in kwestie via een door de Koning aangewezen politiedienst;

6° de Ombudsdienst voor telecommunicatie, met het oog op de identificatie van de persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, conform de voorwaarden beoogd in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Enkel de identificatiegegevens mogen worden gevraagd.

De aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de in paragraaf 3 bedoelde gegevens onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en uitsluitend aan de in deze paragraaf bedoelde autoriteiten kunnen worden meegedeeld.

Onverminderd andere wettelijke voorschriften mogen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, de krachtens paragraaf 3 bewaarde gegevens niet gebruiken voor andere doeleinden.

§ 3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin het tweede en derde lid specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf maanden bewaard vanaf de datum van de communicatie.

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

§ 4. Wat betreft de bewaring van de gegevens bedoeld in paragraaf 3, dienen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid :

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

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

3° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten bedoeld in paragraaf 2, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 126/1, § 1;

4° de gegevens op het grondgebied van de Europese Unie te bewaren;

5° te zorgen voor maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

6° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt zoals vastgelegd in paragraaf 3, worden verwijderd van elke drager, onverminderd de artikelen 122 en 123;

7° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit bedoeld in paragraaf 2.

De in het eerste lid, 7°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer mogen dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.

§ 5. De minister en de minister van Justitie zorgen ervoor dat statistieken inzake de bewaring van de gegevens die worden gegenereerd of verwerkt in het kader van de verstrekking van openbaar toegankelijke communicatienetwerken en -diensten jaarlijks worden bezorgd aan de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name :

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

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

3° de gevallen waarin verzoeken om gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt, op voorstel van de minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, jaarlijks bezorgen aan het Instituut en die welke het Instituut bezorgt aan de minister en aan de minister van Justitie.

§ 6. Onverminderd het verslag bedoeld in paragraaf 5, vierde lid, brengen de minister en de minister van Justitie, twee jaar na de inwerkingtreding van het in paragraaf 3, vierde lid, bedoelde koninklijk besluit een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de te bewaren gegevens en de bewaringstermijn. '.

Art. 5. In dezelfde wet wordt een artikel 126/1 ingevoegd, luidende :

' Art. 126/1. § 1. Binnen elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde Belgische autoriteiten, op hun verzoek, van de gegevens bewaard krachtens de artikelen 122, 123 en 126, de identificatiegegevens van de oproeper krachtens artikel 107, § 2, eerste lid, of de gegevens die kunnen worden gevorderd krachtens de artikelen 46*bis*, 88*bis* en 90*ter* van het Wetboek van strafvordering en de artikelen 18/7, 18/8, 18/16 en 18/17 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

In voorkomend geval kunnen verscheidene operatoren of aanbieders een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval moet deze Coördinatiecel voorzien in dezelfde dienst voor elke operator of aanbieder.

Om deel uit te maken van de Coördinatiecel dienen de leden :

1° het voorwerp [te] hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies conform artikel 22*quinquies* van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

2° niet het voorwerp [te] hebben uitgemaakt van een weigering door de minister van Justitie, waarbij die weigering met redenen moet worden omkleed en zich te allen tijde kan voordoen.

Een advies wordt als achterhaald beschouwd 5 jaar na zijn verstrekking.

De operatoren en aanbieders die geen van de diensten bedoeld in artikel 126, § 1, verstrekken, zijn vrijgesteld van de in het derde lid, 1°, beoogde voorwaarde.

Enkel de leden van de Coördinatiecel mogen antwoorden op de verzoeken van de autoriteiten met betrekking tot de gegevens bedoeld in het eerste lid. Ze mogen echter, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator of van de aanbieder.

De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.

Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel en deelt onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer de contactgegevens van de Coördinatiecel en van zijn leden mee alsook elke wijziging van die gegevens.

§ 2. Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, stelt een interne procedure op om te antwoorden op de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens betreffende de gebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en hun antwoord.

Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, wordt beschouwd als verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, voor de gegevens behandeld op basis van artikel 126 en dit artikel.

De operatoren van openbare netwerken voor elektronische communicatie en de aanbieders bedoeld in artikel 126, § 1, eerste lid, nemen artikel 114, § 2, in acht voor de toegang tot de gegevens bedoeld in paragraaf 1 en hun overdracht aan de autoriteiten.

§ 3. Elke aanbieder bedoeld in artikel 126, § 1, eerste lid, en elke operator bedoeld in artikel 126, § 1, eerste lid, wijst een of meer aangestelden aan voor de bescherming van persoonsgegevens, die moet beantwoorden aan de cumulatieve voorwaarden opgesomd in paragraaf 1, derde lid.

Deze aangestelde mag geen deel uitmaken van de Coördinatiecel.

Verscheidene operatoren of aanbieders mogen een of meer gemeenschappelijke aangestelden voor de bescherming van de persoonsgegevens aanduiden. In dat geval moeten deze aangestelden dezelfde opdracht uitvoeren voor elke individuele operator of aanbieder.

Bij de uitvoering van zijn opdrachten handelt de aangestelde voor de bescherming van de persoonsgegevens in volledige onafhankelijkheid, en heeft hij toegang tot alle persoonsgegevens die worden bezorgd aan de autoriteiten, alsook tot alle relevante lokalen van de aanbieder of de operator.

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

De aangestelde moet de mogelijkheid hebben om rechtstreeks te communiceren met de directie van de operator of de aanbieder.

De aangestelde voor de gegevensbescherming zorgt ervoor dat :

1° de behandelingen door de Coördinatiecel worden uitgevoerd conform de wet;

2° de aanbieder of de operator enkel die gegevens verzamelt en bewaart die hij wettelijk mag bewaren;

3° enkel de wettelijk bevoegde autoriteiten toegang hebben tot de bewaarde gegevens;

4° de maatregelen voor beveiliging en bescherming van persoonsgegevens beschreven in deze wet en in het veiligheidsbeleid van de aanbieder of de operator ten uitvoer worden gebracht.

Elke aanbieder en elke operator bedoeld in artikel 126, § 1, eerste lid, deelt onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer de contactgegevens van de aangestelden voor de bescherming van persoonsgegevens mee alsook elke wijziging van die gegevens.

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

1° de nadere regels van het verzoek en de verstrekking van het veiligheidsadvies;

2° de vereisten waaraan de Coördinatiecel moet beantwoorden, door rekening te houden met de situatie van de operatoren en aanbieders die weinig verzoeken krijgen van de gerechtelijke overheden, die geen vestiging hebben in België of voornamelijk vanuit het buitenland handelen;

3° de informatie die moet worden verstrekt aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer conform de paragrafen 1 en 3 alsook de autoriteiten die toegang hebben tot die informatie;

4° de overige regels die de samenwerking van de operatoren en van de aanbieders bedoeld in artikel 126, § 1, eerste lid, met de Belgische autoriteiten of met sommige van hen, regelen, voor de verstrekking van de in paragraaf 1 beoogde gegevens, in voorkomend geval en per betrokken overheid met inbegrip van de vorm en de inhoud van het verzoek. '.

Art. 6. In artikel 127 van dezelfde wet, gewijzigd door de wetten van 4 februari 2010, 10 juli 2012 en 27 maart 2014, worden de volgende wijzigingen aangebracht :

1° in paragraaf 1 worden de volgende wijzigingen aangebracht :

a) in het eerste lid worden de woorden ', aan de aanbieders bedoeld in artikel 126, § 1, eerste lid, ' ingevoegd tussen de woorden ' aan de operatoren ' en de woorden ' of aan de eindgebruikers ';

b) in het tweede lid worden de woorden ' en de aanbieders bedoeld in artikel 126, § 1, eerste lid, ' ingevoegd tussen de woorden ' de operatoren ' en de woorden ' aan de in het eerste lid, 2°, bedoelde verrichtingen ';

2° paragraaf 6 wordt opgeheven.

Art. 7. In artikel 145 van dezelfde wet, gewijzigd bij de wetten van 25 april 2007 en 27 maart 2014 worden de volgende wijzigingen aangebracht :

1° de woorden ' 126, 126/1, ' worden ingevoegd tussen de woorden ' 124, ' en ' 127 ';

2° de woorden ', 126, 126/1 ' worden ingevoegd tussen de woorden ' 47 ' en ' en 127 ';

3° in de plaats van paragraaf 3*ter*, vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, wordt een als volgt luidende paragraaf 3*ter* ingevoegd :

' § 3*ter*. Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft :

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

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

HOOFDSTUK 3. — *Wijzigingen van het Wetboek van strafvordering*

Art. 8. In artikel 46*bis*, § 1, van het Wetboek van strafvordering, ingevoegd bij de wet van 10 juni 1998 en vervangen bij de wet van 23 januari 2007, worden de volgende wijzigingen aangebracht :

a) in de Franse tekst worden de woorden ' le concours de l'opérateur d'une réseau de communication ' vervangen door de woorden ' le concours de l'opérateur d'un réseau de communication ';

b) de paragraaf wordt aangevuld met een lid, luidende :

' Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, kunnen de procureur des Konings of, in geval van uiterst dringende noodzakelijkheid, de officier van gerechtelijke politie, de in het eerste lid bedoelde gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan zijn beslissing. '.

Art. 9. In artikel 88*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 1991, vervangen bij de wet van 10 juni 1998 en gewijzigd bij de wetten van 8 juni 2008 en 27 december 2012, worden de volgende wijzigingen aangebracht :

a) in paragraaf 1 wordt het eerste lid vervangen als volgt :

' Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij, zo nodig rechtstreeks of via een door de Koning aangewezen politiedienst de medewerking vorderen van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst, om over te gaan of te doen overgaan tot :

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties. ';

b) in paragraaf 1, tweede lid [,] wordt het woord ' telecommunicatiemiddel ' vervangen door de woorden ' elektronisch communicatiemiddel ' en het woord ' telecommunicatie ' door [de woorden] ' elektronische communicatie';

c) in paragraaf 1 wordt het derde lid vervangen als volgt :

' De onderzoeksrechter doet in een met redenen omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad. ';

d) in paragraaf 1 wordt het vierde lid vervangen als volgt :

' Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 2. ';

e) paragraaf 1 wordt aangevuld met een lid, luidende :

' In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Hij moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde en vierde lid. ';

f) paragraaf 2, waarvan de huidige tekst paragraaf 4 zal vormen, wordt vervangen als volgt :

' § 2. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing :

- voor een strafbaar feit bedoeld in boek II, titel I*ter*, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan zijn bevelschrift;

- voor een ander strafbaar feit bedoeld in artikel 90*ter*, § § 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

- voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift. ';

g) het artikel wordt aangevuld met een paragraaf 3, luidende :

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

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

h) in paragraaf 2, die tot paragraaf 4 vernummerd wordt, worden in het eerste lid de woorden ' Iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst ' vervangen door de woorden ' Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst '.

Art. 10. Artikel 90*decies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 8 april 2002, 7 juli 2002, 6 januari 2003 en bij de wet van 30 juli 2013 vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, wordt aangevuld met een lid, luidende :

' Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 5, vierde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie. '.

Art. 11. In artikel 464/25, § 2, eerste lid, van hetzelfde Wetboek worden de woorden ' artikel 88*bis*, § 2, eerste en derde lid, ' vervangen door de woorden ' artikel 88*bis*, § 4, eerste en derde lid, '.

HOOFDSTUK 4. — *Wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst*

Art. 12. In artikel 13 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, gewijzigd bij de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht :

1° in het eerste lid wordt het woord ' inlichtingen ' vervangen door het woord ' informatie ';

2° het derde lid wordt vervangen als volgt :

' De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die deze bronnen leveren. ';

3° het artikel wordt aangevuld met een lid, luidende :

' De agenten van de inlichtingen- en veiligheidsdiensten hebben toegang tot de door hun dienst ingewonnen en verwerkte informatie, inlichtingen en persoonsgegevens, voor zover deze nuttig zijn voor de uitoefening van hun functie of opdracht. '.

Art. 13. In artikel 18/3 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht :

a) in paragraaf 1 zal het huidige derde lid paragraaf 5 vormen;

b) in paragraaf 1, waarvan het vierde lid paragraaf 7 zal vormen, worden de woorden ' om de specifieke methode voor het verzamelen van gegevens aan te wenden ' vervangen door de woorden ' om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen ';

c) paragraaf 2, waarvan het huidige tweede tot vijfde lid paragraaf 6 zullen vormen, wordt vervangen als volgt :

' § 2. De beslissing van het diensthoofd vermeldt :

1° de aard van de specifieke methode;

2° naargelang het geval, de natuurlijke personen of rechtspersonen, verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode;

3° de potentiële dreiging die de specifieke methode rechtvaardigt;

4° de feitelijke omstandigheden die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;

5° de periode waarin de specifieke methode kan worden aangewend, te rekenen vanaf de kennisgeving van de beslissing aan de Commissie;

6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen;

7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de specifieke methode;

8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;

9° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;

10° in geval toepassing wordt gemaakt van artikel 18/8, de motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft;

11° de datum van de beslissing;

12° de handtekening van het diensthoofd. ';

d) paragraaf 3 wordt vervangen als volgt :

' § 3. Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.

Deze lijsten bevatten de gegevens bedoeld in § 2, 1° tot 3°, 5° en 7°. '.

e) het artikel wordt aangevuld met een paragraaf 8, luidende :

' § 8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie. '.

Art. 14. In artikel 18/8 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht :

a) in paragraaf 1 wordt het eerste lid vervangen als volgt :

' De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot :

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties. ';

b) in paragraaf 1, tweede lid, wordt het woord ' oproepgegevens ' vervangen door het woord ' verkeersgegevens'.

c) paragraaf 2, waarvan de huidige tekst paragraaf 4 zal vormen, wordt vervangen als volgt :

' § 2. Wat betreft de toepassing van de methode bedoeld in paragraaf 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing :

1° voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd in zijn beslissing de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing;

2° voor een potentiële dreiging, andere dan deze bedoeld in de bepalingen onder 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing;

3° voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van twaalf maanden voorafgaand aan de beslissing. '.

Art. 15. In artikel 43/3 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010, worden de woorden ' bedoeld in artikel 18/3, § 2 ' vervangen door de woorden ' bedoeld in artikel 18/3, § 3 '.

Art. 16. In artikel 43/5, § 1, tweede lid, van dezelfde wet, worden de woorden ' bedoeld in artikel 18/3, § 2 ' vervangen door de woorden ' bedoeld in artikel 18/3, § 3 ' ».

B.2. Met de bestreden wet is de wetgever willen tegemoetkomen aan de vernietiging, bij het arrest nr. 84/2015 van het Hof van 11 juni 2015, van artikel 126 van de wet van 13 juni 2005 « betreffende de elektronische communicatie » (hierna : de wet van 13 juni 2005), zoals het was gewijzigd bij de wet van 30 juli 2013 « houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1567/001, p. 4).

B.3. Uit de parlementaire voorbereiding van de bestreden wet blijkt dat de wetgever zowel het voormelde arrest van het Hof nr. 84/2015 van 11 juni 2015 als het daaraan ten grondslag liggende arrest van het Hof van Justitie van de Europese Unie van 8 april 2014, in de gevoegde zaken *Digital Rights Ireland Ltd* (C-293/12) en *Kärntner Landesregierung e.a.* (C-594/12), waarbij het Hof van Justitie de Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 « betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG » ongeldig heeft verklaard, grondig heeft onderzocht.

Het doel dat de wetgever met de bestreden wet nastreeft bestaat erin niet alleen terrorisme en kinderpornografie te bestrijden, maar ook de bewaarde gegevens te kunnen gebruiken in zeer veel verschillende situaties waarin die gegevens zowel het vertrekpunt als een fase van het strafonderzoek kunnen zijn (*Parl. St.*, Kamer, 2015-2016, DOC 54-1567/001, p. 6).

B.4. Uit de memorie van toelichting van de bestreden wet blijkt dat de wetgever een gerichte en gedifferentieerde bewaarplicht in het licht van de vooropgestelde doelstelling niet mogelijk heeft geacht en ervoor heeft gekozen om de algemene en ongedifferentieerde bewaarplicht met strikte waarborgen te omringen, zowel op het vlak van de beveiliging van de bewaring, als op het vlak van de toegang, zodat de inmenging in het recht op de bescherming van de persoonlijke levenssfeer tot een minimum zou worden beperkt. In dat verband is erop gewezen dat een a priori differentiatie naar personen, periodes en geografische zones eenvoudigweg niet mogelijk zou zijn (*ibid.*, pp. 10-18).

Ten gronde

B.5. Het enige middel in de zaken nrs. 6590 en 6597 is afgeleid uit de schending, door de bestreden wet, van de artikelen 10 en 11 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 47 van het Handvest van de grondrechten van de Europese Unie.

B.6.1. De « Ordre des barreaux francophones et germanophone », verzoekende partij in de zaak nr. 6590, verwijt de bestreden wet dat zij de gebruikers van telecommunicatie- of elektronische-communicatiediensten die aan het beroepsgeheim zijn onderworpen, onder wie met name de advocaten, en de andere gebruikers van die diensten op identieke wijze behandelt. Die verzoekende partij stelt vast dat de wet eveneens een veralgemeende verplichting tot registratie en bewaring van bepaalde metagegevens inhoudt, die het mogelijk maken te bepalen of een advocaat werd geraadpleegd door een natuurlijke persoon of rechtspersoon, die advocaat te identificeren, zijn gesprekspartners en in het bijzonder zijn cliënten te identificeren, alsook de datum en het uur van de communicatie te bepalen. Die veralgemeende verplichting wordt opgelegd aan alle aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, internettelefoniediensten en openbare elektronische communicatienetwerken.

B.6.2. De verzoekende partij in de zaak nr. 6590 klaagt eveneens aan dat de bestreden wet in een veralgemeende verplichting tot het bewaren van gegevens voorziet zonder een onderscheid tussen de rechtzoekenden te maken naargelang zij al dan niet het voorwerp uitmaken van een onderzoeks- of vervolgingsmaatregel wegens feiten die aanleiding kunnen geven tot strafrechtelijke veroordelingen. Zij voert eveneens aan dat de in de wet bedoelde categorieën van gegevens uitermate ruim en gevarieerd zijn, in zoverre zij betrekking hebben op de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, de gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, alsook de communicatiegegevens, ook al wordt de inhoud ervan daarentegen uitgesloten.

B.7.1. De verzoekende partijen in de zaak nr. 6597 verwijten de bestreden wet dat zij de gebruikers van telecommunicatie- of elektronische communicatiediensten die aan het beroepsgeheim zijn onderworpen, onder wie met name de boekhoudkundige en fiscale professionals, en de andere gebruikers van die diensten op identieke wijze behandelt, zonder rekening te houden met het bijzondere statuut van de boekhoudkundige en fiscale professionals, het fundamentele karakter van het beroepsgeheim waaraan zij onderworpen zijn en de noodzakelijke vertrouwensrelatie tussen hen en hun cliënten.

B.7.2. Zij verwijten de bestreden wet eveneens dat zij de rechtzoekenden die het voorwerp uitmaken van onderzoeks- of vervolgingsmaatregelen wegens feiten die mogelijk beantwoorden aan de doeleinden van de bewaring van de in het geding zijnde elektronische gegevens, en die welke niet het voorwerp van dergelijke maatregelen uitmaken, op identieke wijze behandelt.

B.8.1. Het eerste middel in de zaak nr. 6599 is afgeleid uit de schending van de artikelen 10, 11, 12, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie, met artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, met het algemene beginsel van rechtszekerheid, van evenredigheid, van het recht op informationele zelfbeschikking en met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie.

B.8.2. De vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme » (intussen « Ligue des droits humains » geworden), verzoekende partijen in de zaak nr. 6599, verwijten de bestreden wet dat zij in een algemene verplichting tot het bewaren van gegevens voorziet, hetgeen de operatoren en de aanbieders van openbare telefoniediensten (met inbegrip van internettelefonie), van internettoegang en van e-mail over het internet, alsook de aanbieders van openbare elektronische communicatienetwerken verplicht om de verkeersgegevens betreffende vaste telefonie, mobiele telefonie en internettelefonie en de gegevens betreffende internettoegang *de facto* voor alle - verdachte of niet-verdachte - Belgen gedurende twaalf maanden te bewaren en ter beschikking te stellen van de politie en van het gerecht, van de inlichtingen- en veiligheidsdiensten, van de hulpdiensten, van de Cel Vermiste Personen en van de Ombudsdienst voor telecommunicatie.

B.9.1. Het eerste middel in de zaak nr. 6601 is afgeleid uit de schending, door de bestreden wet, van artikel 8 van het Europees Verdrag voor de rechten van de mens, van de artikelen 7, 8, 11, lid 1, en 52 van het Handvest van de grondrechten van de Europese Unie, van de artikelen 10, 11, 19 en 22 van de Grondwet, van artikel 2, *a)*, van de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens », alsook van de artikelen 1, 2, 3, 5, 6, 9 en 15 van de Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 « betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) » (hierna : de richtlijn 2002/58/EG).

B.9.2. De verzoekende partijen in de zaak nr. 6601 zijn natuurlijke personen die in België wonen en verschillende elektronischecommunicatiediensten gebruiken in het kader van een met een operator gesloten overeenkomst. In het eerste onderdeel van het eerste middel klagen zij aan dat de bestreden wet voorziet in een algemene en ongedifferentieerde verplichting tot het bewaren van identificatie-, verbindings- en lokalisatiegegevens en van persoonlijke communicatiegegevens ten laste van de aanbieders van telefoniediensten, ook via internet, van internettoegang en van e-mail over het internet, ten laste van de operatoren die openbare elektronische communicatienetwerken aanbieden en ten laste van de operatoren die een van die diensten aanbieden.

B.10. Rekening houdend met de onderlinge samenhang ervan, worden de in de diverse zaken aangevoerde middelen samen onderzocht.

B.11.1. Rekening houdend met, enerzijds, de verschillen in zienswijze, tussen de verzoekende partijen en de Ministerraad, over de interpretatie die moet worden gegeven aan meerdere bepalingen die het Hof in zijn toetsing van de bestreden wet dient te betrekken, inzonderheid artikel 15, lid 1, van de Richtlijn 2002/58/EG en de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie, en, anderzijds, de door de Ministerraad gegeven verklaringen om de verenigbaarheid van de bestreden wet met de door de verzoekende partijen aangevoerde referentienormen te verantwoorden, heeft het Hof, bij zijn arrest nr. 96/2018 van 19 juli 2018, aan het Hof van Justitie van de Europese Unie de volgende drie prejudiciële vragen gesteld :

« 1. Dient artikel 15, lid 1, van de Richtlijn 2002/58/EG, in samenhang gelezen met het recht op veiligheid, gewaarborgd bij artikel 6 van het Handvest van de grondrechten van de Europese Unie, en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de Richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, nationale regeling die niet alleen ten doel heeft het onderzoeken, opsporen en vervolgen van feiten van zware criminaliteit, maar ook het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit of het voorkomen van een verboden gebruik van de elektronische communicatiesystemen, of de verwezenlijking van een andere doelstelling die is geïdentificeerd bij artikel 23, lid 1, van de Verordening (EU) 2016/679 en die bovendien onderworpen is aan nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe ?

2. Dient artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 4, 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de Richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, indien die regeling mede tot doel heeft om de op de overheid rustende positieve verplichtingen ingevolge de artikelen 4 en 8 van het Handvest te bewerkstelligen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt en het effectief mogelijk maakt om de pleger van het misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronische communicatiemiddelen ?

3. Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden ? ».

B.11.2. Artikel 15, lid 1, van de Richtlijn 2002/58/EG bepaalt :

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

B.11.3. Het Hof heeft ook beslist het onderzoek van de zaken op te schorten totdat het Hof van Justitie uitspraak zal hebben gedaan in de zaken *Ministerio Fiscal* (C-207/16) en *Privacy International t. Secretary of State for Foreign and Commonwealth Affairs e.a.* (C-623/17).

B.12. Bij zijn arrest van 2 oktober 2018, in zake *Ministerio Fiscal* (C-207/16), heeft het Hof van Justitie in grote kamer geoordeeld dat artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang - op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten - moet worden beperkt tot de bestrijding van zware criminaliteit. Dat arrest steunt op volgende overwegingen :

« *Ten gronde*

48. Met zijn twee vragen, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van Richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - een zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van deze laatsten vormt dat die toegang, wat het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten betreft, zou moeten worden beperkt tot de bestrijding van zware criminaliteit en, zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld.

49. In dit verband blijkt uit de verwijzingsbeslissing dat, zoals de advocaat-generaal in punt 38 van zijn conclusie in wezen heeft opgemerkt, het verzoek om een prejudiciële beslissing er niet toe strekt om uit te maken of de aanbieders van elektronische-communicatiediensten de in het hoofdgeding aan de orde zijnde persoonsgegevens hebben bewaard met inachtneming van de voorwaarden van artikel 15, lid 1, van Richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest. Zoals uit punt 46 van het onderhavige arrest blijkt, betreft het verzoek uitsluitend de vraag of en in welke mate het doel dat met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan rechtvaardigen dat overheidsinstanties zoals de gerechtelijke politie toegang hebben tot dergelijke gegevens, en gaat het verzoek niet over de andere toegangsvoorwaarden die uit voormeld artikel 15, lid 1, voortvloeien.

50. De verwijzende rechter vraagt zich in het bijzonder af welke elementen in aanmerking moeten worden genomen bij de beoordeling of delicten waarvoor politiediensten in het kader van een onderzoek toegang kan worden verleend tot persoonsgegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, voldoende ernstig zijn om de inmenging die een dergelijke toegang betekent in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uitgelegd door het Hof in zijn arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12, EU: C: 2014: 238), en in het arrest *Tele2 Sverige en Watson e.a.*, te rechtvaardigen.

51. Wat betreft de vraag of sprake is van inmenging in die grondrechten, zij eraan herinnerd dat, zoals de advocaat-generaal in de punten 76 en 77 van zijn conclusie heeft aangegeven, de toegang van overheidsinstanties tot dergelijke gegevens inmenging in het in artikel 7 van het Handvest neergelegde grondrecht op eerbiediging van het privéleven vormt, zelfs al kan die inmenging om bepaalde redenen niet als ' ernstig ' worden aangemerkt en zonder dat van belang is of de informatie over het privéleven al dan niet gevoelig is en of de betrokkenen door die inmenging enig nadeel hebben ondervonden. Een dergelijke toegang vormt tevens inmenging in het door artikel 8 van het Handvest gewaarborgde grondrecht op bescherming van persoonsgegevens, aangezien die toegang een verwerking van persoonsgegevens is [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punten 124 en 126 en aldaar aangehaalde rechtspraak].

52. Wat betreft de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling als die in het hoofdgeding, die de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt en die aldus afwijkt van het beginsel van de vertrouwelijkheid van elektronische communicatie, zij eraan herinnerd dat de in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 gegeven opsomming van doelstellingen exhaustief is, zodat die toegang daadwerkelijk en strikt op een van die doelstellingen moet berusten (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punten 90 en 115).

53. Aangaande de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, dient te worden geconstateerd dat het daarbij volgens de bewoordingen van artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 evenwel niet alleen over de bestrijding van ernstige delicten maar over ' strafbare feiten ' in het algemeen gaat

54. Stellig heeft het Hof in dit verband geoordeeld dat ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens waaruit, in hun geheel beschouwd, precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punt 99).

55. Het Hof heeft die uitlegging echter gemotiveerd met de overweging dat de met een toegangsregeling nagestreefde doelstelling in verhouding moet staan tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punt 115).

56. Volgens het evenredigheidsbeginsel kan ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, ernstige inmenging immers slechts worden gerechtvaardigd door de doelstelling om - eveneens 'ernstige' - criminaliteit te bestrijden.

57. Is de inmenging die een dergelijke toegang veroorzaakt daarentegen niet ernstig, dan kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van ' strafbare feiten ' in het algemeen.

58. Allereerst moet dus worden uitgemaakt of *in casu*, gelet op de omstandigheden van de onderhavige zaak, de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die zou voortvloeien uit het feit dat aan de gerechtelijke politie toegang tot de in het hoofdgeding aan de orde zijnde gegevens wordt verleend, als ' ernstig ' moet worden beschouwd.

59. In dit verband heeft het verzoek in het hoofdgeding, waarmee de gerechtelijke politie in een strafrechtelijk onderzoek via rechterlijke toestemming toegang wil verkrijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens, louter tot doel de houders te identificeren van de simkaarten die gedurende een periode van twaalf dagen met het IMEI-nummer van de gestolen mobiele telefoon zijn geactiveerd. Zoals in punt 40 van het onderhavige arrest is uiteengezet, strekt dat verzoek er enkel toe om toegang te verkrijgen tot de telefoonnummers die overeenstemmen met die simkaarten en tot de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. Zoals zowel de Spaanse regering als het openbaar ministerie ter terechtzitting heeft bevestigd, gaat het daarbij echter niet over de communicatie die met de gestolen mobiele telefoon tot stand is gebracht of over de locatie van die telefoon.

60. Met de via het toegangsverzoek in het hoofdgeding beoogde gegevens is het dus blijkbaar alleen mogelijk om, gedurende een bepaalde periode, de met de gestolen mobiele telefoon geactiveerde simkaart(en) in verband te brengen met de civiele identiteit van de houders van die simkaarten. Zonder aanvullende gegevens over de communicatie die met die simkaarten tot stand is gebracht en over de locatie, kan met die gegevens noch de datum, het uur, de duur of de ontvanger van de met de betrokken simkaart(en) verrichte oproepen worden achterhaald, noch waar die communicatie heeft plaatsgevonden of hoe vaak in een gegeven periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken.

61. In die omstandigheden kan de toegang tot de in het verzoek in het hoofdgeding bedoelde gegevens niet worden aangemerkt als een ' ernstige ' inmenging in de grondrechten van de personen waarop de gegevens betrekking hebben.

62. Zoals uit de punten 53 tot en met 57 van dit arrest blijkt, kan de inmenging die een dergelijke gegevenstoegang zou veroorzaken dus worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 vermelde doelstelling om ' strafbare feiten ' in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, zonder dat deze strafbare feiten als ' ernstig ' moeten worden aangemerkt.

63. Gelet op het voorgaande dient op de gestelde vragen te worden geantwoord dat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang - op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten - moet worden beperkt tot de bestrijding van zware criminaliteit ».

In het dictum van het arrest heeft het Hof van Justitie verklaard voor recht :

« Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in samenhang met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang - op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten - moet worden beperkt tot de bestrijding van zware criminaliteit ».

B.13. Bij zijn arrest van 6 oktober 2020, in zake *Privacy International* (C-623/17), uitgesproken in grote kamer, heeft het Hof van Justitie geoordeeld dat artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in het licht van artikel 4, lid 2, van het Verdrag betreffende de Europese Unie en de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische-communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Dat arrest steunt op volgende overwegingen :

« *Tweede vraag*

50. Met zijn tweede vraag wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

51. Om te beginnen zij eraan herinnerd dat section 94 van de wet van 1984 volgens de informatie in het verzoek om een prejudiciële beslissing de Secretary of State de mogelijkheid biedt om aanbieders van elektronischecommunicatiediensten door middel van aanwijzingen de verplichting op te leggen om bulk-communicatiegegevens door te zenden aan de veiligheids- en inlichtingendiensten, indien hij dit noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met een buitenlandse regering. Deze gegevens omvatten verkeers- en locatiegegevens alsmede informatie over de gebruikte diensten, in de zin van section 21, leden 4 en 6, RIPA. Deze laatste bepaling ziet onder meer op de gegevens die nodig zijn om de bron en de bestemming van een communicatie te identificeren, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte materiaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren met name de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, het bron- en het doel-IP-adres en de adressen van de bezochte websites.

52. Een dergelijke verstrekking van gegevens door middel van doorzending betreft alle gebruikers van elektronischecommunicatiemiddelen, zonder dat wordt gespecificeerd of die doorzending wel of niet in real time moet plaatsvinden. De doorgezonden gegevens worden volgens de informatie in het verzoek om een prejudiciële beslissing door de veiligheids- en inlichtingendiensten bewaard en blijven ter beschikking van deze diensten ten behoeve van hun activiteiten, net zoals de andere databases van deze diensten. Met name kunnen de aldus verworven gegevens, waarop automatische bulkverwerking en -analyse worden toegepast, worden onderworpen aan kruiscontroles met andere databases die verschillende categorieën bulkpersoonsgegevens bevatten, of buiten die diensten worden bekendgemaakt, ook aan derde staten. Tot slot is voor die bewerkingen geen voorafgaande toestemming van een rechterlijke instantie of een onafhankelijk bestuursorgaan vereist en geldt er geen verplichting om de betrokkenen te informeren.

53. Zoals met name uit de overwegingen 6 en 7 van Richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van Richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit Richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen ' zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie '.

54. Daartoe bepaalt artikel 5, lid 1, van Richtlijn 2002/58 dat ' [d]e lidstaten [...] via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten [garanderen] '. In diezelfde bepaling wordt benadrukt dat de lidstaten ' met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers [verbieden], indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1 ', en gepreciseerd dat ' [d]it lid [...] de technische opslag die nodig is voor het overbrengen van informatie onverlet [laat], onverminderd het vertrouwelijkheidsbeginsel '.

55. Artikel 5, lid 1, legt aldus het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd. Gelet op haar algemene bewoordingen, bestrijkt die bepaling noodzakelijkerwijs elke voor andere doeleinden dan het overbrengen van informatie uitgevoerde bewerking die derden in staat stelt om kennis te nemen van de communicatie en de daarmee verband houdende gegevens.

56. Het in artikel 5, lid 1, van Richtlijn 2002/58 neergelegde verbod op het onderscheppen van de communicatie en de daarmee verband houdende verkeersgegevens omvat dus elke vorm van beschikbaarstelling door aanbieders van elektronischecommunicatiediensten van verkeers- en locatiegegevens aan overheidsinstanties, zoals veiligheids- en inlichtingendiensten, alsmede de bewaring van de beschikbaar gestelde gegevens door die instanties, ongeacht het latere gebruik van die gegevens.

57. Met de vaststelling van Richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 109).

58. Artikel 15, lid 1, van Richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

59. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van Richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punten 89 en 104, en 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 111).

60. Bovendien volgt uit artikel 15, lid 1, derde zin, van Richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 25 en 70, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

61. Diezelfde vragen rijzen ook voor andere vormen van gegevensverwerking, zoals de doorzending van gegevens aan anderen dan de gebruikers of de toegang tot die gegevens met het oog op het gebruik ervan [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punten 122 en 123 en aldaar aangehaalde rechtspraak].

62. Bij de uitlegging van artikel 15, lid 1, van Richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, *Connolly/Commissie*, C-274/99 P, EU: C: 2001: 127, punt 39, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 93 en aldaar aangehaalde rechtspraak).

63. De in de artikelen 7, 8 en 11 van het Handvest verankerde rechten hebben echter geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU: C: 2020: 559, punt 172 en aldaar aangehaalde rechtspraak).

64. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

65. Hieraan dient te worden toegevoegd dat het vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU: C: 2020: 559, punt 175 en aldaar aangehaalde rechtspraak).

66. Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel ' in een democratische samenleving noodzakelijk, redelijk en proportioneel is ' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel ' strikt ' evenredig moet zijn aan het nagestreefde doel.

67. In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU: C: 2008: 727, punt 56; 9 november 2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09, EU: C: 2010: 662, punten 76, 77 en 86, en 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 140].

68. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 54 en 55, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 141].

69. Wat de vraag betreft of een nationale regeling als die van het hoofdgeding voldoet aan de vereisten van artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, dient te worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan anderen dan de gebruikers, zoals de veiligheids- en inlichtingendiensten, afwijkt van het vertrouwelijkheidsbeginsel. Wanneer die bewerking, zoals in casu, op algemene en ongedifferentieerde wijze wordt uitgevoerd, heeft zij tot gevolg dat de afwijking van de principeverplichting tot waarborging van de vertrouwelijkheid van de gegevens de regel wordt, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat die afwijking de uitzondering blijft.

70. Voorts vormt de doorzending van verkeers- en locatiegegevens aan een derde volgens vaste rechtspraak van het Hof een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. In dit verband is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punten 124 en 126 en aldaar aangehaalde rechtspraak, en arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punten 115 en 116].

71. De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 27 en 37, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punten 99 en 100).

72. Tevens moet worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan overheidsinstanties voor veiligheidsdoeleinden op zichzelf afbreuk kan doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie, en de gebruikers van elektronischecommunicatiemiddelen kan ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen. Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punt 28; 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 101, en 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 118).

73. Ten slotte is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

74. Wat de doelstellingen betreft die dergelijke inmengingen kunnen rechtvaardigen, meer in het bijzonder de in het hoofdgeding aan de orde zijnde doelstelling van bescherming van de nationale veiligheid, moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 135).

75. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van Richtlijn 2002/58, met name de doelstellingen van bestrijding van - zelfs ernstige - criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich - zelfs ernstige - spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 136).

76. Om te voldoen aan het in punt 67 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, dient een nationale regeling die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, evenwel in overeenstemming te zijn met de eisen die voortvloeien uit de in de punten 65, 67 en 68 van het onderhavige arrest aangehaalde rechtspraak.

77. Wat in het bijzonder de toegang van een autoriteit tot persoonsgegevens betreft, mag een regeling zich niet ertoe beperken te eisen dat de toegang tot deze gegevens wordt verleend voor het met die regeling beoogde doel, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 192 en aldaar aangehaalde rechtspraak].

78. Een nationale regeling die de toegang tot locatie- en verkeersgegevens regelt, moet dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de betrokken gegevens moet worden verleend, aangezien een algemene toegang tot alle bewaarde gegevens, los van enig - zelfs maar indirect - verband met het nagestreefde doel, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 119 en aldaar aangehaalde rechtspraak).

79. Die vereisten zijn *a fortiori* van toepassing op een wettelijke maatregel als aan de orde in het hoofdgeding, op grond waarvan de bevoegde nationale autoriteit aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Een dergelijke doorzending heeft immers tot gevolg dat die gegevens ter beschikking worden gesteld aan overheidsinstanties [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 212].

80. Het feit dat de doorzending van de verkeers- en locatiegegevens geschiedt op algemene en ongedifferentieerde wijze, betekent dat die doorzending algemeen alle personen betreft die gebruikmaken van elektronischecommunicatiediensten, dat wil zeggen zelfs personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - een verband vertoont met de doelstelling van bescherming van de nationale veiligheid. Met name is er geen enkel verband vereist tussen de gegevens die moeten worden doorgezonden en een bedreiging van de nationale veiligheid (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 57 en 58, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 105). Gelet op het feit dat de doorzending van dergelijke gegevens aan overheidsinstanties - overeenkomstig de vaststelling in punt 79 van het onderhavige arrest - gelijkstaat aan het verlenen van toegang tot deze gegevens, moet worden geoordeeld dat een regeling die de algemene en ongedifferentieerde doorzending van gegevens aan overheidsinstanties mogelijk maakt, een algemene toegang tot die gegevens impliceert.

81. Daaruit volgt dat een nationale regeling die aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten oplegt, verder gaat dan strikt noodzakelijk is en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist.

82. Gelet op een en ander moet op de tweede vraag worden geantwoord dat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen ».

In het dictum van het arrest heeft het Hof van Justitie voor recht verklaard :

« 2) Artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen ».

B.14. Bij zijn arrest van 6 oktober 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18), uitgesproken in grote kamer, heeft het Hof van Justitie de eerste twee door het Hof bij zijn arrest nr. 96/2018 gestelde vragen als volgt beantwoord :

« *Eerste vraag in de zaken C-511/18 en C-512/18 en eerste en tweede vraag in zaak C-520/18*

81. Met de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18, die samen moeten worden onderzocht, wensen de verwijzende rechters in wezen te vernemen of artikel 15, lid 1, van Richtlijn 2002/58 aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die voor de in deze bepaling genoemde doeleinden aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt.

[...]

Uitlegging van artikel 15, lid 1, van Richtlijn 2002/58

105. Vooraf zij eraan herinnerd dat volgens vaste rechtspraak bij de uitlegging van een Unierechtelijke bepaling niet alleen rekening moet worden gehouden met de bewoordingen ervan, maar ook met de context van die bepaling, de doelstellingen van de regeling waarvan zij deel uitmaakt en, met name, de ontstaansgeschiedenis van die regeling (zie in die zin arrest van 17 april 2018, *Egenberger*, C-414/16, EU: C: 2018: 257, punt 44).

106. Zoals met name uit de overwegingen 6 en 7 van Richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van Richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit Richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen ' zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie '.

107. Daartoe legt artikel 5, lid 1, van Richtlijn 2002/58 het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert het met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd.

108. Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronischecommunicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van Richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van Richtlijn 2002/58 dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij zijn geanonimiseerd of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 86 en aldaar aangehaalde rechtspraak).

109. Met de vaststelling van Richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd.

110. Artikel 15, lid 1, van Richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

111. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van Richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punten 89 en 104).

112. Met betrekking tot de doelstellingen die een beperking van de met name in de artikelen 5, 6 en 9 van Richtlijn 2002/58 vastgestelde rechten en verplichtingen kunnen rechtvaardigen, heeft het Hof reeds geoordeeld dat de in artikel 15, lid 1, eerste zin, van deze richtlijn gegeven opsomming van doelstellingen exhaustief is, zodat een op grond van die bepaling vastgestelde wettelijke maatregel daadwerkelijk en strikt moet berusten op een van die doelstellingen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, punt 52 en aldaar aangehaalde rechtspraak).

113. Bovendien volgt uit artikel 15, lid 1, derde zin, van Richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 25 en 70, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

114. Bij de uitlegging van artikel 15, lid 1, van Richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie volgens artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, *Connolly/Commissie*, C-274/99 P, EU: C: 2001: 127, punt 39, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 93 en aldaar aangehaalde rechtspraak).

115. In dit verband dient te worden gepreciseerd dat de bewaring van verkeers- en locatiegegevens als zodanig behalve een uitzondering op het in artikel 5, lid 1, van Richtlijn 2002/58 gestelde verbod op de opslag van die gegevens door anderen dan de gebruikers, ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens vormt, waarbij niet van belang is of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punten 124 en 126 en aldaar aangehaalde rechtspraak; zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 30 januari 2020, *Breyer tegen Duitsland*, CE: ECHR: 2020: 0130JUD005000112, § 81].

116. Het is ook irrelevant of de bewaarde gegevens vervolgens al dan niet worden gebruikt (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 16 februari 2000, *Amann t. Zwisterland*, CE: ECHR: 2000: 0216JUD002779895, § 69, en 13 februari 2020, *Trjakovski en Chipovski t. Noord-Macedonië*, CE: ECHR: 2020: 0213JUD005320513, § 51), aangezien de toegang tot die gegevens, ongeacht het latere gebruik ervan, op zichzelf al een inmenging vormt in de in het voorgaande punt genoemde grondrechten [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punten 124 en 126].

117. Deze conclusie is des te meer gerechtvaardigd daar verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. In het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU: C: 2014: 238, punt 27, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 99).

118. De bewaring van verkeers- en locatiegegevens voor politiële doeleinden kan dus om te beginnen op zichzelf afbreuk doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie en de gebruikers van elektronischecommunicatiemiddelen ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU: C: 2014: 238, punt 28, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 101). Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (*PB* 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn.

119. Bovendien is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene en ongedifferentieerde bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

120. Het feit dat het de lidstaten op grond van artikel 15, lid 1, van Richtlijn 2002/58 is toegestaan om te voorzien in de in punt 110 van het onderhavige arrest bedoelde uitzonderingen, heeft ermee te maken dat de in de artikelen 7, 8 en 11 van het Handvest verankerde rechten geen absolute gelding hebben, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU: C: 2020: 559, punt 172 en aldaar aangehaalde rechtspraak).

121. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

122. Bij de uitlegging van artikel 15, lid 1, van Richtlijn 2002/58 in het licht van het Handvest moet derhalve ook rekening worden gehouden met het belang van de door de artikelen 3, 4, 6 en 7 van het Handvest gewaarborgde rechten en met dat van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van ernstige criminaliteit, die bijdragen tot de bescherming van de rechten en vrijheden van anderen.

123. Zo heeft ingevolge artikel 6 van het Handvest, waaraan de Conseil d'État en het Grondwettelijk Hof refereren, eenieder niet alleen recht op vrijheid, maar ook op veiligheid, en waarborgt deze bepaling rechten die overeenstemmen met die welke worden gewaarborgd door artikel 5 EVRM (zie in die zin arresten van 15 februari 2016, *N.*, C-601/15 PPU, EU: C: 2016: 84, punt 47; 28 juli 2016, *JZ*, C-294/16 PPU, EU: C: 2016: 610, punt 48, en 19 september 2019, *Rayonna prokuratura Lom*, C-467/18, EU: C: 2019: 765, punt 42 en aldaar aangehaalde rechtspraak).

124. Voorts zij eraan herinnerd dat artikel 52, lid 3, van het Handvest beoogt te zorgen voor de nodige samenhang tussen de in het Handvest vervatte rechten en de daarmee corresponderende, door het EVRM gewaarborgde rechten, zonder de autonomie van het Unierecht en van het Hof van Justitie van de Europese Unie aan te tasten. Bijgevolg dient bij de uitlegging van het Handvest rekening te worden gehouden met de overeenkomstige rechten van het EVRM, die het minimale beschermingsniveau bepalen [zie in die zin arresten van 12 februari 2019, *TC*, C-492/18 PPU, EU: C: 2019: 108, punt 57, en 21 mei 2019, *Commissie/Hongarije* (*Vruchtgebruik op landbouwgrond*), C-235/17, EU: C: 2019: 432, punt 72 en aldaar aangehaalde rechtspraak].

125. Artikel 5 EVRM, waarin het ' recht op vrijheid ' en het ' recht op veiligheid ' zijn verankerd, beoogt volgens de rechtspraak van het EHRM eenieder te beschermen tegen willekeurige en ongerechtvaardigde vrijheidsontneming (zie in die zin EHRM, 18 maart 2008, *Ladent t. Polen*, CE: ECHR: 2008: 0318JUD001103603, § § 45 en 46; 29 maart 2010, *Medvedyev e.a. t. Frankrijk*, CE: ECHR: 2010: 0329JUD000339403, § § 76 en 77, en 13 december 2012, *El-Masri t. ' The former Yugoslav Republic of Macedonia '*, CE: ECHR: 2012: 1213JUD003963009, § 239). Die bepaling ziet echter op vrijheidsontneming door overheidsinstanties, zodat artikel 6 van het Handvest niet aldus kan worden uitgelegd dat het de overheid een verplichting oplegt om specifieke maatregelen te nemen teneinde bepaalde strafbare handelingen tegen te gaan.

126. Wat daarentegen in het bijzonder de door het Grondwettelijk Hof genoemde effectieve bestrijding betreft van strafbare handelingen waarvan met name minderjarigen en andere kwetsbare personen het slachtoffer zijn, moet worden beklemtoond dat uit artikel 7 van het Handvest positieve verplichtingen voor de overheid kunnen voortvloeien om juridische maatregelen te nemen ter bescherming van het privéleven en het familie- en gezinsleven [zie in die zin arrest van 18 juni 2020, *Commissie/Hongarije* (*Transparantie van verenigingen*), C-78/18, EU: C: 2020: 476, punt 123 en aldaar aangehaalde rechtspraak van het EHRM). Dergelijke verplichtingen kunnen ook uit dat artikel voortvloeien ten aanzien van de bescherming van iemands woning en communicatie, en uit de artikelen 3 en 4 van het Handvest ten aanzien van de bescherming van iemands lichamelijke en geestelijke integriteit en het verbod op folteringen en onmenselijke en vernederende behandelingen.

127. Gelet op die verschillende positieve verplichtingen is het noodzakelijk de diverse op het spel staande belangen en rechten met elkaar te verzoenen.

128. Het EHRM heeft namelijk geoordeeld dat de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten, met name impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging, hetgeen des te belangrijker is wanneer het lichamelijke en geestelijke welzijn van een kind wordt bedreigd. De bevoegde autoriteiten dienen daarbij echter de wettelijk voorgeschreven procedures en de overige waarborgen die de omvang van de strafrechtelijke onderzoeksbevoegdheden beperken, alsmede de overige vrijheden en rechten volledig in acht te nemen. Met name dient er volgens het EHRM een wettelijk kader te worden ingevoerd dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd, met elkaar te verzoenen (EHRM, 28 oktober 1998, *Osman t. Verenigd Koninkrijk*, CE: ECHR: 1998: 1028JUD002345294, § § 115 en 116; 4 maart 2004, *M.C. t. Bulgarij*e, CE: ECHR: 2003: 1204JUD003927298, § 151; 24 juni 2004, *Von Hannover t. Duitsland*, CE: ECHR: 2004: 0624JUD005932000, § § 57 en 58, en 2 december 2008, *K.U. t. Finland*, CE: ECHR: 2008: 1202JUD 000287202, § § 46, 48 en 49).

129. Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel ' in een democratische samenleving noodzakelijk, redelijk en proportioneel is ' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel ' strikt ' evenredig moet zijn aan het nagestreefde doel.

130. In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU: C: 2008: 727, punt 56; 9 november 2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09, EU: C: 2010: 662, punten 76, 77 en 86, en 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 140].

131. Meer bepaald volgt uit de rechtspraak van het Hof dat bij de beoordeling of de lidstaten een beperking van de omvang van de met name in de artikelen 5, 6 en 9 van Richtlijn 2002/58 bedoelde rechten en plichten kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, punt 55 en aldaar aangehaalde rechtspraak).

132. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 54 en 55, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 141].

133. Een regeling die voorziet in de bewaring van persoonsgegevens, moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 191 en aldaar aangehaalde rechtspraak, en arrest van 3 oktober 2019, *A e.a.*, C-70/18, EU: C: 2019: 823, punt 63].

- Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid

134. Het Hof heeft zich in zijn arresten betreffende de uitlegging van Richtlijn 2002/58 nog niet specifiek gebogen over de doelstelling van bescherming van de nationale veiligheid, waaraan is gerefereerd door de verwijzende rechters en de regeringen die opmerkingen hebben ingediend.

135. In dit verband moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten.

136. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van Richtlijn 2002/58, met name de doelstellingen van bestrijding van - zelfs ernstige - criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich - zelfs ernstige - spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.

137. In situaties als die welke in de punten 135 en 136 van het onderhavige arrest zijn beschreven, verzet artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich derhalve in beginsel niet tegen een wettelijke maatregel op grond waarvan de bevoegde autoriteiten aan aanbieders van elektronischecommunicatiediensten een bevel kunnen opleggen om de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen gedurende een beperkte periode te bewaren, wanneer er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid als bedoeld in de punten 135 en 136 van het onderhavige arrest, en die bedreiging werkelijk en actueel of voorzienbaar is. Ook al heeft een dergelijke maatregel zonder onderscheid betrekking op alle gebruikers van elektronischecommunicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont.

138. Het bevel om preventief de gegevens te bewaren van alle gebruikers van elektronischecommunicatiemiddelen, mag echter slechts worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk. Het valt weliswaar niet uit te sluiten dat het aan aanbieders van elektronischecommunicatiemiddelen opgelegde bevel tot bewaring van die gegevens kan worden verlengd wegens het voortduren van een dergelijke bedreiging, maar dit neemt niet weg dat elk bevel slechts mag worden gegeven voor een voorzienbare periode. Een dergelijke gegevensbewaring moet bovendien zijn onderworpen aan beperkingen en zijn omgeven met strikte waarborgen die ervoor zorgen dat de persoonsgegevens van de betrokken personen doeltreffend worden beschermd tegen het risico van misbruik. Die bewaring mag derhalve geen stelselmatig karakter hebben.

139. Gelet op de ernst van de inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten die een dergelijke algemene en ongedifferentieerde bewaring van gegevens met zich brengt, dient te worden gewaarborgd dat de toepassing van die maatregel daadwerkelijk beperkt blijft tot situaties waarin de nationale veiligheid ernstig wordt bedreigd, zoals de in de punten 135 en 136 van het onderhavige arrest bedoelde situaties. Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronischecommunicatiediensten een bevel tot een dergelijke gegevensbewaring wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

- Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

140. Als het gaat om de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, kunnen overeenkomstig het evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, zoals die welke voortvloeien uit de bewaring van verkeers- en locatiegegevens. De doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, kan derhalve enkel niet-ernstige inmengingen in die grondrechten rechtvaardigen [zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 102, en 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, punten 56 en 57; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU: C: 2017: 592, punt 149].

141. Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 107).

142. Gezien het gevoelige karakter van de informatie die verkeers- en locatiegegevens kunnen prijsgeven, is de vertrouwelijkheid van deze gegevens immers essentieel voor het recht op eerbiediging van het privéleven. Mede gelet op het in punt 118 van het onderhavige arrest bedoelde ontmoedigende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de in de artikelen 7 en 11 van het Handvest verankerde grondrechten, en op de ernst van de inmenging die een dergelijke bewaring met zich brengt, is het in een democratische samenleving dan ook van belang dat deze bewaring, zoals het bij Richtlijn 2002/58 ingevoerde stelsel eist, de uitzondering en niet de regel vormt en dat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Deze conclusie geldt zelfs met betrekking tot de doelstellingen van bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen voor de openbare veiligheid en het belang dat aan deze doelstellingen moet worden toegekend.

143. Voorts heeft het Hof benadrukt dat een regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel. Een dergelijke regeling betreft algemeen alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat die personen zich - zelfs maar indirect - in een situatie bevinden die aanleiding kan zijn om strafvervolging in te stellen, wat in strijd is met het in punt 133 van het onderhavige arrest in herinnering gebrachte vereiste. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - verband houdt met die doelstelling van bestrijding van zware misdrijven, en vereist met name niet dat er een verband is tussen de te bewaren gegevens en een bedreiging voor de openbare veiligheid (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU: C: 2014: 238, punten 57 en 58, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 105).

144. Zoals het Hof reeds heeft geoordeeld, beperkt een dergelijke regeling met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU: C: 2014: 238, punt 59, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 106).

145. Zelfs de positieve verplichtingen die, naargelang van het geval, voor de lidstaten kunnen voortvloeien uit de artikelen 3, 4 en 7 van het Handvest en, zoals in de punten 126 en 128 van het onderhavige arrest is opgemerkt, betrekking hebben op de invoering van regels die een effectieve bestrijding van strafbare feiten mogelijk maken, kunnen geen inmengingen rechtvaardigen die zo ernstig zijn als de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van vrijwel de gehele bevolking die een regeling die voorziet in de bewaring van verkeers- en locatiegegevens met zich brengt, zonder dat de gegevens van de betrokken personen, althans indirect, een verband met het nagestreefde doel aan het licht kunnen brengen.

146. Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onderhavige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, *a fortiori*, bescherming van de nationale veiligheid - gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name het Grondwettelijk Hof heeft gerefereerd - de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt.

147. Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 108).

148. De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand van de categorieën betrokken personen, aangezien artikel 15, lid 1, van Richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 111).

149. In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zij die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.

150. Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punt 111). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.

151. Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

- Wettelijke maatregelen die voorzien in de preventieve bewaring van IP-adressen en gegevens inzake de burgerlijke identiteit ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

152. Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.

153. Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben.

154. Om de op het spel staande rechten en belangen met elkaar te verzoenen, zoals de in punt 130 van het onderhavige arrest aangehaalde rechtspraak verlangt, moet echter in aanmerking worden genomen dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten na afloop van de periode waarvoor deze adressen werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat, zoals verschillende regeringen hebben aangevoerd in de door hen bij het Hof ingediende opmerkingen, het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel als bedoeld in artikel 15, lid 1, van Richtlijn 2002/58. Zoals die regeringen hebben betoogd, kan dit met name het geval zijn bij zeer ernstige strafbare feiten op het gebied van kinderpornografie, zoals het online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie in de zin van artikel 2, onder *c)*, van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (*PB* 2011, L 335, blz. 1).

155. In deze omstandigheden moet worden vastgesteld dat, ook al zou een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur die internettoegang mogelijk maakt, personen betreffen bij wie op het eerste gezicht een verband met de nagestreefde doelstellingen in de zin van de in punt 133 van het onderhavige arrest aangehaalde rechtspraak ontbreekt, en ook al moeten internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, een wettelijke maatregel die voorziet in de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen, in beginsel niet in strijd is met artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van die gegevens dienen te regelen.

156. Gelet op het feit dat die bewaring een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, kunnen enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid, die inmenging rechtvaardigen. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk is gelet op het nagestreefde doel. Tot slot moet een dergelijke maatregel voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de online communicatie en de online activiteiten van de betrokken personen.

157. Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als ' ernstig ' worden aangemerkt (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, punten 59 en 60).

158. Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, punt 62).

159. Gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, moet in deze omstandigheden om de in de punten 131 en 158 van het onderhavige arrest uiteengezette redenen worden geoordeeld dat, ook al bestaat er geen verband tussen alle gebruikers van elektronischecommunicatiemiddelen en de nagestreefde doelstellingen, artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 2, van het Handvest, zich niet verzet tegen een wettelijke maatregel op grond waarvan aanbieders van elektronischecommunicatiediensten verplicht zijn om de gegevens inzake de burgerlijke identiteit van alle gebruikers van elektronischecommunicatiemiddelen gedurende een niet nader bepaalde periode te bewaren ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.

- Wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevensten behoeve van de bestrijding van zware criminaliteit

160. Met betrekking tot de verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van Richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen als beschreven in de punten 134 tot en met 159 van het onderhavige arrest, dient te worden opgemerkt dat deze gegevens in beginsel moeten worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen waarbinnen zij overeenkomstig de nationale bepalingen tot omzetting van die Richtlijn moeten worden verwerkt en opgeslagen.

161. Gedurende die verwerking en opslag kunnen zich evenwel situaties voordoen die het noodzakelijk maken om de betrokken gegevens ook na het verstrijken van die termijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

162. In dit verband zij erop gewezen dat het op 23 november 2001 onder auspiciën van de Raad van Europa gesloten Cybercrimeverdrag (Serie Europese Verdragen - nr. 185), dat door alle 27 lidstaten is ondertekend en door 25 lidstaten is geratificeerd, en dat tot doel heeft de bestrijding van door middel van een computersysteem begane strafbare feiten te vergemakkelijken, in artikel 14 bepaalt dat de verdragsluitende partijen ten behoeve van specifieke strafrechtelijke onderzoeken of procedures bepaalde maatregelen moeten nemen met betrekking tot reeds opgeslagen verkeersgegevens, zoals de spoedbewaring van die gegevens. Met name is in artikel 16, lid 1, van dit verdrag bepaald dat de verdragsluitende partijen de wetgevende en andere maatregelen moeten nemen die nodig zijn om hun bevoegde autoriteiten in staat te stellen de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van verkeersgegevens die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat die gegevens vatbaar zijn voor verlies of wijziging.

163. In een situatie als bedoeld in punt 161 van het onderhavige arrest staat het de lidstaten, gelet op de in punt 130 van het onderhavige arrest genoemde noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, vrij om in een op grond van artikel 15, lid 1, van Richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

164. Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen enkel de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

165. In dit verband moet worden gepreciseerd dat een dergelijke spoedbewaring niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht. Mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 133 van het onderhavige arrest, kan een dergelijke maatregel naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd. Bovendien moet aan de bevoegde autoriteiten toegang tot de aldus bewaarde gegevens worden verleend met inachtneming van de voorwaarden die voortvloeien uit de arresten waarin Richtlijn 2002/58 is uitgelegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU: C: 2016: 970, punten 118-121 en aldaar aangehaalde rechtspraak).

166. Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van Richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mist de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167. In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van Richtlijn 2002/58.

168. Gelet op een en ander moet op de eerste vraag in de zaken C-511/18 en C-512/18 en op de eerste en de tweede vraag in zaak C-520/18 worden geantwoord dat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, verzet zich daarentegen niet tegen wettelijke maatregelen

- die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en

- die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik ».

In het dictum van het arrest heeft het Hof van Justitie verklaard voor recht :

« 1) Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, verzet zich daarentegen niet tegen wettelijke maatregelen

- die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en

- die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

[...] ».

B.15. Uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.*, blijkt dat artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, § 1, genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in de in het voormelde arrest beschreven beperkte gevallen.

In zoverre zij principieel en zonder beperking tot die gevallen voorziet in een algemene en ongedifferentieerde bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de identificatiegegevens, de toegangs- en verbindingsgegevens, alsook van de communicatiegegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, schendt de bestreden wet bijgevolg artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest van de grondrechten van de Europese Unie, en in samenhang met de artikelen 10 en 11 van de Grondwet.

B.16.1. In het dictum van het voormelde arrest van 6 oktober 2020, in zake *La Quadrature du Net e.a.*, preciseert het Hof van Justitie echter dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn aldus, met name, wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk », of nog wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen ». Die wettelijke maatregelen moeten, « door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik ».

B.16.2. Op grond van die preciseringen van het Hof van Justitie betoogt de Ministerraad in zijn aanvullende memories dat de bestreden wet in elk geval niet dient te worden vernietigd in zoverre zij voorziet in de algemene en ongedifferentieerde verplichting tot bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de IP-adressen die zijn toegewezen aan de bron van een verbinding, enerzijds, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, anderzijds.

De Ministerraad besluit daaruit dat, in voorkomend geval, enkel het tweede en het derde lid van artikel 126, § 3, van de wet van 13 juni 2005 dienen te worden vernietigd, waarin respectievelijk de verbindings- en locatiegegevens en de communicatiegegevens worden beoogd. Hij is van mening dat het eerste lid van het voormelde artikel 126, § 3, waarin de identificatiegegevens worden beoogd, daarentegen niet dient te worden vernietigd, net zomin als de andere bepalingen van de bestreden wet, aangezien zij de nodige waarborgen bevatten op het vlak van bewaring van en toegang tot de gegevens.

B.17. Te dezen dient te worden vastgesteld dat de bestreden wet, wat het beginsel zelf ervan betreft, berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen, zoals in B.3 en B.4 is vermeld, ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid.

Het onderscheid dat bij artikel 126, § 3, van de wet van 13 juni 2005 wordt gemaakt tussen drie categorieën van gegevens (te weten : identificatiegegevens, toegangs- en verbindingsgegevens, alsook communicatiegegevens) heeft slechts een weerslag op het startpunt van de bewaringstermijn van de gegevens - in elk geval twaalf maanden -, en eventueel op de mogelijkheden voor de gemachtigde instanties om toegang tot die gegevens te hebben (zie artikel 46*bis* van het Wetboek van strafvordering en artikel 126, § 2, van de wet van 13 juni 2005). Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie in zijn arrest van 6 oktober 2020 wordt gemaakt voor wat betreft de verschillende categorieën van gegevens die het voorwerp kunnen uitmaken van een verplichting tot algemene en ongedifferentieerde bewaring, mits verscheidene voorwaarden in acht worden genomen (te weten, te dezen : de IP-adressen die zijn toegewezen aan de bron van een verbinding en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen).

B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt : de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds « beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel » (punten 132 en 133).

B.19. Het staat aan de wetgever een regeling tot stand te brengen waarbij de beginselen in acht worden genomen die van toepassing zijn inzake bescherming van persoonsgegevens, in het licht van de rechtspraak van het Hof van Justitie, en, in voorkomend geval, rekening te houden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die verenigbaar worden geacht met artikel 15, lid 1, van de Richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. In het bijzonder staat het, in die context, ook aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

B.20. Rekening houdend met hetgeen voorafgaat, dienen de artikelen 2, *b)*, 3 tot 11 en 14 van de bestreden wet, die onlosmakelijk met elkaar verbonden zijn, te worden vernietigd.

B.21. De andere middelen in de zaken nrs. 6599 en 6601 betreffen ook de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie en de toegang tot die gegevens. Aangezien zij niet tot een ruimere vernietiging kunnen leiden, dienen zij niet te worden onderzocht.

Ten aanzien van de handhaving van de gevolgen

B.22. In zijn memories van wederantwoord verzoekt de Ministerraad het Hof in uiterst ondergeschikte orde de gevolgen te handhaven van de bepalingen die in voorkomend geval zouden worden vernietigd, teneinde het door de politie- en inlichtingendiensten verrichte werk inzake opsporing en vervolging van misdrijven niet in gevaar te brengen.

B.23.1. Artikel 8, derde lid, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof bepaalt :

« Zo het Hof dit nodig oordeelt, wijst het, bij wege van algemene beschikking, die gevolgen van de vernietigde bepalingen aan welke als gehandhaafd moeten worden beschouwd of voorlopig gehandhaafd worden voor de termijn die het vaststelt ».

B.23.2. Het Hof dient ter zake rekening te houden met de beperkingen die uit het recht van de Europese Unie voortvloeien inzake de handhaving van de gevolgen van nationale normen die dienen te worden vernietigd omdat zij in strijd zijn met dat recht (HvJ, grote kamer, 8 september 2010, C-409/06, *Winner Wetten*, punten 53-69; HvJ, grote kamer, 28 februari 2012, C-41/11, *Inter-Environnement Wallonie en Terre wallonne*, punten 56-63).

In de regel kan dit enkel onder de voorwaarden die door het Hof van Justitie in antwoord op een prejudiciële vraag worden vastgesteld.

B.24.1. In antwoord op de door het Hof gestelde derde prejudiciële vraag over een eventuele handhaving van de gevolgen van de bestreden wet, heeft het Hof van Justitie geoordeeld :

« *Derde vraag in zaak C-520/18*

213. Met de derde vraag in zaak C-520/18 wenst de verwijzende rechter in wezen te vernemen of een nationale rechterlijke instantie een bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd van een onwettigverklaring te beperken wanneer hij op grond van dit recht een nationale wettelijke regeling die ten behoeve van onder meer de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt, onwettig dient te verklaren omdat zij onverenigbaar is met artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

214. Het beginsel van het primaat van het Unierecht houdt in dat dit recht voorrang heeft op het recht van de lidstaten. Dit beginsel verplicht dus alle instanties van de lidstaten om volle werking te verlenen aan de verschillende normen van de Unie, aangezien het recht van de lidstaten niet kan afdoen aan de werking die op het grondgebied van die staten aan deze verschillende normen is verleend [arrest van 15 juli 1964, *Costa*, 6/64, EU: C: 1964: 66, blz. 1219 en 1220, en 19 november 2019, *A. K. e.a.* (*Onafhankelijkheid van de tuchtkamer van de Sąd Najwyszy*), C-585/18, C-624/18 en C-625/18, EU: C: 2019: 982, punten 157 en 158 en aldaar aangehaalde rechtspraak].

215. Het voorrangsbeginsel brengt mee dat, indien de nationale regelgeving niet in overeenstemming met de vereisten van het Unierecht kan worden uitgelegd, de nationale rechter die in het kader van zijn bevoegdheid is belast met de toepassing van de bepalingen van het Unierecht, verplicht is de volle werking van deze bepalingen te verzekeren en daarbij zo nodig, op eigen gezag, elke, zelfs latere, strijdige bepaling van de nationale wettelijke regeling buiten toepassing te laten, zonder dat hij de voorafgaande opheffing hiervan via de wetgeving of enige andere constitutionele procedure hoeft te vragen of af te wachten [arresten van 22 juni 2010, *Melki en Abdeli*, C-188/10 en C-189/10, EU: C: 2010: 363, punt 43 en aldaar aangehaalde rechtspraak; 24 juni 2019, *Popławski*, C-573/17, EU: C: 2019: 530, punt 58, en 19 november 2019, *A. K. e.a.* (*Onafhankelijkheid van de tuchtkamer van de Sąd Najwyszy*), C-585/18, C-624/18 en C-625/18, EU: C: 2019: 982, punt 160].

216. Enkel het Hof kan, bij wijze van uitzondering en om dwingende redenen van rechtszekerheid, een voorlopige opschorting toestaan van het effect dat een regel van het Unierecht op het daarmee strijdige nationale recht heeft, namelijk de terzijdestelling daarvan. Een dergelijke beperking in de tijd van de werking van de door het Hof aan het Unierecht gegeven uitlegging kan slechts worden vastgesteld in het arrest waarin de gevraagde uitlegging wordt gegeven [zie in die zin arresten van 23 oktober 2012, *Nelson e.a.*, C-581/10 en C-629/10, EU: C: 2012: 657, punten 89 en 91; 23 april 2020, *Herst*, C-401/18, EU: C: 2020: 295, punten 56 en 57, en 25 juni 2020, *A e.a.* (*Windturbines in Aalter en Nevele*), C-24/19, EU: C: 2020: 503, punt 84 en aldaar aangehaalde rechtspraak].

217. Aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn (zie in die zin arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU: C: 2019: 622, punt 177 en aldaar aangehaalde rechtspraak).

218. Het Hof heeft evenwel in een zaak waarin het draaide om de rechtmatigheid van maatregelen die waren vastgesteld in strijd met de Unierechtelijke verplichting om een voorafgaande beoordeling te verrichten van de gevolgen van een project voor het milieu of voor een beschermd gebied, geoordeeld dat een nationale rechterlijke instantie, indien het nationale recht dat toestaat, bij wijze van uitzondering de gevolgen van dergelijke maatregelen kan handhaven indien deze handhaving wordt gerechtvaardigd door dwingende redenen die verband houden met de noodzaak om het reële en ernstige risico af te wenden dat de elektriciteitsbevoorrading van de betrokken lidstaat wordt onderbroken, en aan dit risico niet het hoofd zou kunnen worden geboden met andere middelen en alternatieven, met name in het kader van de interne markt, met dien verstande dat die handhaving niet langer kan duren dan strikt noodzakelijk is om een einde te maken aan die onrechtmatigheid (zie in die zin arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU: C: 2019: 622, punten 175, 176, 179 en 181).

219. Anders dan de niet-nakoming van een procedurele verplichting als de voorafgaande beoordeling van de gevolgen van een project op het specifieke terrein van de milieubescherming, kan een schending van artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, niet worden geregulariseerd via een procedure die vergelijkbaar is met die waaraan in het voorgaande punt wordt gerefereerd. Handhaving van de gevolgen van een nationale wettelijke regeling als in het hoofdgeding aan de orde is, zou immers betekenen dat die regeling aan aanbieders van elektronischecommunicatiediensten verplichtingen blijft opleggen die in strijd zijn met het Unierecht en leiden tot een ernstige inmenging in de grondrechten van de personen van wie de gegevens zijn bewaard.

220. Hieruit volgt dat de verwijzende rechter geen bepaling van zijn nationale recht mag toepassen die hem machtigt om de werking in de tijd te beperken van een door hem op grond van dit recht uit te spreken onwettigverklaring van de in het hoofdgeding aan de orde zijnde nationale wettelijke regeling.

221. VZ, WY en XX stellen in hun bij het Hof ingediende schriftelijke opmerkingen dat de derde vraag impliciet maar noodzakelijkerwijs de vraag opwerpt of het Unierecht zich ertegen verzet dat in het kader van een strafrechtelijke procedure wordt gebruikgemaakt van informatie en bewijzen die zijn verkregen door middel van een met dit recht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.

222. Om de verwijzende rechter een nuttig antwoord te verstrekken, zij er in dit verband aan herinnerd dat het bij de huidige stand van het Unierecht uitsluitend een zaak van het nationale recht is om de regels vast te stellen met betrekking tot de aanvaarding en de beoordeling van door middel van een dergelijke met het Unierecht strijdige gegevensbewaring verkregen informatie en bewijzen in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van ernstige strafbare feiten.

223. Het is immers vaste rechtspraak dat het bij gebreke van Unieregelgeving ter zake krachtens het beginsel van procedurele autonomie een aangelegenheid van de interne rechtsorde van elke lidstaat is om de procedureregels vast te stellen voor rechtsvorderingen die ertoe strekken de rechten die de justitiabelen aan het Unierecht ontlenen, te beschermen, op voorwaarde evenwel dat die regels niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) (zie in die zin arresten van 6 oktober 2015, *Târşia*, C-69/14, EU: C: 2015: 662, punten 26 en 27; 24 oktober 2018, *XC e.a.*, C-234/17, EU: C: 2018: 853, punten 21 en 22 en aldaar aangehaalde rechtspraak, en 19 december 2019, *Deutsche Umwelthilfe*, C-752/18, EU: C: 2019: 1114, punt 33).

224. Wat het gelijkwaardigheidsbeginsel betreft, staat het aan de nationale rechter bij wie een strafrechtelijke procedure is aangebracht die gebaseerd is op informatie of bewijzen die in strijd met de uit Richtlijn 2002/58 voortvloeiende vereisten zijn verkregen, om na te gaan of het op die procedure van toepassing zijnde nationale recht minder gunstige regels bevat voor de aanvaarding en het gebruik van dergelijke informatie en bewijzen dan voor de aanvaarding en het gebruik van informatie en bewijzen die zijn verkregen in strijd met het interne recht.

225. Met betrekking tot het doeltreffendheidsbeginsel moet worden opgemerkt dat nationale regels inzake de aanvaarding en het gebruik van informatie en bewijzen tot doel hebben om in overeenstemming met de in het nationale recht gemaakte keuzen te voorkomen dat onrechtmatig verkregen informatie en bewijzen ongerechtvaardigd nadeel toebrengen aan een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd. Dat doel kan naar nationaal recht niet alleen worden bereikt door middel van een verbod op het gebruik van dergelijke informatie en bewijzen, maar ook door middel van nationale regels en praktijken met betrekking tot de beoordeling en de weging van de informatie en de bewijzen, of door de inaanmerkingneming van het onrechtmatige karakter ervan bij de straftoemeting.

226. Uit de rechtspraak van het Hof volgt dat bij de beoordeling of informatie en bewijzen die in strijd met de voorschriften van het Unierecht zijn verkregen, moeten worden uitgesloten, met name moet worden nagegaan of de aanvaarding van dergelijke informatie en bewijzen schending van het beginsel van hoor en wederhoor en dus ook van het recht op een eerlijk proces tot gevolg kan hebben (zie in die zin arrest van 10 april 2003, *Steffensen*, C-276/01, EU: C: 2003: 228, punten 76 en 77). Een rechterlijke instantie die van oordeel is dat een partij niet in de gelegenheid is om doeltreffend commentaar te leveren op een bewijsmiddel dat betrekking heeft op een gebied waarvan de rechters geen kennis hebben en dat een doorslaggevende invloed kan hebben op de beoordeling van de feiten, moet vaststellen dat het recht op een eerlijk proces hierdoor wordt geschonden, en dat bewijsmiddel uitsluiten om die schending te voorkomen (zie in die zin arrest van 10 april 2003, *Steffensen*, C-276/01, EU: C: 2003: 228, punten 78 en 79).

227. Bijgevolg brengt het doeltreffendheidsbeginsel voor de nationale strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

228. Gelet op een en ander moet op de derde vraag in zaak C-520/18 worden geantwoord dat een nationale rechterlijke instantie geen bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten ».

In het dictum van het arrest heeft het Hof van Justitie voor recht verklaard :

« 4) Een nationale rechterlijke instantie mag geen bepaling van haar nationale recht toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten ».

B.24.2. Uit het voormelde arrest blijkt dat het Hof geen gegronde redenen heeft om de gevolgen van de vernietigde bepalingen voorlopig te handhaven.

B.24.3. Het staat aan de bevoegde strafrechter, in voorkomend geval, uitspraak te doen over de toelaatbaarheid van de bewijzen die werden verzameld bij de tenuitvoerlegging van de vernietigde bepalingen, overeenkomstig artikel 32 van de voorafgaande titel van het Wetboek van stafvordering en in het licht van de door het Hof van Justitie in het voormelde arrest van 6 oktober 2020 aangebrachte preciseringen.

Om die redenen,

het Hof

vernietigt de artikelen 2, *b)*, 3 tot 11 en 14 van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » en verwerpt de beroepen voor het overige.

Aldus gewezen in het Frans, het Nederlands en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 22 april 2021.

De griffier, De voorzitter,
F. Meersschaut F. Daoût

VERFASSUNGSGERICHTSHOF

[2021/202174]

Auszug aus dem Entscheid Nr. 57/2021 vom 22. April 2021

Geschäftsverzeichnisnummern 6590, 6597, 6599 und 6601

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 F. Daoût und L. Lavrysen, und den Richtern J.-P. Moerman, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques und Y. Kherbache, unter Assistenz des Kanzlers F. Meersschaut, unter dem Vorsitz des Präsidenten F. Daoût,

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 Westflandern zugelassen.

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

In seinem Zwischenentscheid Nr. 96/2018 vom 19. Juli 2018, veröffentlicht im *Belgischen Staatsblatt* vom 27. Dezember 2018, hat der Verfassungsgerichtshof dem Gerichtshof der Europäischen Union folgende Vorabentscheidungsfragen gestellt:

« 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? ».

In seinem Urteil vom 6. Oktober 2020 in den Rechtssachen C-511/18, C-512/18 und C-520/18 hat der Gerichtshof der Europäischen Union auf die Fragen geantwortet.

(...)

II. *Rechtliche Würdigung*

(...)

In Bezug auf das angefochtene Gesetz und seinen Kontext

B.1. Die klagenden Parteien beantragen die Nichtigerklärung des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation », das bestimmt:

« KAPITEL 1 — *Allgemeine Bestimmung*

Art. 1 - Vorliegendes Gesetz regelt eine in Artikel 74 der Verfassung erwähnte Angelegenheit.

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

Art. 2 - Artikel 2 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation, zuletzt abgeändert durch das Gesetz vom 18. Dezember 2015 und teilweise für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird wie folgt abgeändert:

a) Nummer 11 wird wie folgt ersetzt:

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

b) Anstelle von Nr. 74, für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird eine Nr. 74 mit folgendem Wortlaut eingefügt:

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

Art. 3 - Artikel 125 § 2 desselben Gesetzes wird aufgehoben.

Art. 4 - In dasselbe Gesetz wird anstelle von Artikel 126, für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, ein Artikel 126 mit folgendem Wortlaut eingefügt:

' Art. 126 - § 1 - Unbeschadet des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten speichern öffentliche Anbieter von Telefon-, Internetzugangs-, Internet-E-Mail- und Internet-Telefonie-Diensten, Betreiber öffentlicher elektronischer Kommunikationsnetze und Betreiber einer der beiden Dienste auf Vorrat in § 3 erwähnte Daten, die bei der Bereitstellung der betreffenden Kommunikationsdienste von ihnen erzeugt oder verarbeitet werden.

Vorliegender Artikel bezieht sich nicht auf den Inhalt der Kommunikationen.

Die Verpflichtung zur Vorratsspeicherung der in § 3 erwähnten Daten gilt ebenfalls für erfolglose Anrufversuche, sofern diese Daten bei der Bereitstellung der betreffenden Kommunikationsdienste:

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

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

§ 2 - Nur folgende Behörden dürfen auf einfaches Verlangen von den in § 1 Absatz 1 erwähnten Anbietern und Betreibern Daten erhalten, die aufgrund des vorliegenden Artikels für folgende Zwecke und gemäß den nachstehend aufgezählten Bedingungen auf Vorrat gespeichert werden:

1. Gerichtsbehörden im Hinblick auf Ermittlung, Untersuchung und Verfolgung von Verstößen, zur Ausführung von Maßnahmen, die in den Artikeln 46*bis* und 88*bis* des Strafprozessgesetzbuches erwähnt sind, und unter den durch diese Artikel festgelegten Bedingungen,

2. Nachrichten- und Sicherheitsdienste zur Erfüllung von nachrichtendienstlichen Aufträgen unter Einsatz der in den Artikeln 16/2, 18/7 und 18/8 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste erwähnten Methoden zur Datensammlung und gemäß den in vorliegendem Gesetz festgelegten Bedingungen,

3. Gerichtspolizeioffiziere des Instituts im Hinblick auf Ermittlung, Untersuchung und Verfolgung von Verstößen gegen die Artikel 114, 124 und vorliegenden Artikel,

4. Hilfsdienste, die Hilfe vor Ort anbieten, wenn sie nach einem Notruf vom betreffenden Anbieter oder Betreiber mit Hilfe der in Artikel 107 § 2 Absatz 3 erwähnten Datenbank nicht die Identifizierungsdaten des Anrufers oder unvollständige oder fehlerhafte Daten erhalten. Nur die Identifizierungsdaten des Anrufers dürfen binnen einer Frist von maximal 24 Stunden nach dem Anruf beantragt werden,

5. Gerichtspolizeioffiziere der Vermisstenzelle der Föderalen Polizei im Rahmen ihres Auftrags zur Hilfeleistung für Personen in Gefahr, Suche nach vermissten Personen, deren Verschwinden als Besorgnis erregend angesehen wird, und wenn es schwerwiegende Vermutungen oder Indizien dafür gibt, dass die körperliche Unversehrtheit der vermissten Person unmittelbar in Gefahr ist. Nur die in § 3 Absatz 1 und 2 erwähnten Daten über die vermisste Person, die während 48 Stunden vor dem Antrag auf Erhalt der Daten auf Vorrat gespeichert wurden, dürfen beim betreffenden Betreiber oder Anbieter über einen vom König bestimmten Polizeidienst beantragt werden,

6. der Ombudsdienst für Telekommunikation im Hinblick auf die Identifizierung von Personen, die gemäß den Bedingungen wie in Artikel 43*bis* § 3 Nr. 7 des Gesetzes vom 21. März 1991 zur Umstrukturierung bestimmter öffentlicher Wirtschaftsunternehmen erwähnt böswillig ein elektronisches Kommunikationsnetz beziehungsweise einen elektronischen Kommunikationsdienst genutzt haben. Nur die Identifizierungsdaten dürfen beantragt werden.

Die in § 1 Absatz 1 erwähnten Anbieter und Betreiber sorgen dafür, dass in § 3 erwähnte Daten von Belgien aus unbeschränkt zugänglich sind und dass diese Daten und alle anderen notwendigen Informationen zu diesen Daten unverzüglich und nur den in vorliegendem Paragraphen erwähnten Behörden übermittelt werden können.

Unbeschadet anderer Gesetzesbestimmungen dürfen in § 1 Absatz 1 erwähnte Anbieter und Betreiber die aufgrund von § 3 auf Vorrat gespeicherten Daten nicht für andere Zwecke nutzen.

§ 3 - Daten zur Identifizierung von Nutzer oder Teilnehmer und Kommunikationsmittel, in den Absätzen 2 und 3 spezifisch vorgesehene Daten ausgenommen, werden zwölf Monate ab dem Datum, an dem eine Kommunikation über den benutzten Dienst zum letzten Mal möglich ist, auf Vorrat gespeichert.

Daten in Bezug auf Zugang und Verbindung der Endeinrichtung zu Netzwerk und Dienst und in Bezug auf den Standort dieser Ausrüstung, einschließlich des Netzabschlusspunktes, werden zwölf Monate ab dem Datum der Kommunikation auf Vorrat gespeichert.

Kommunikationsdaten mit Ausnahme des Inhalts, einschließlich ihres Ursprungs und ihrer Bestimmung, werden zwölf Monate ab dem Datum der Kommunikation auf Vorrat gespeichert.

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers und nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass die nach Art der in Absatz 1 bis 3 erwähnten Kategorien auf Vorrat zu speichernden Daten und die Anforderungen, die diese Daten erfüllen müssen, fest.

§ 4 - Für die Vorratsspeicherung der in § 3 erwähnten Daten gilt für in § 1 Absatz 1 erwähnte Anbieter und Betreiber Folgendes:

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

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

3. Sie gewährleisten, dass der Zugang zu den auf Vorrat gespeicherten Daten ausschließlich einem oder mehreren Mitgliedern des in Artikel 126/1 § 1 erwähnten Koordinationsbüros vorbehalten ist.

4. Sie speichern die Daten auf Vorrat auf dem Gebiet der Europäischen Union.

5. Sie treffen Maßnahmen zum technologischen Schutz, die die auf Vorrat gespeicherten Daten ab ihrer Registrierung für Personen, die nicht zu ihrem Zugang befugt sind, unlesbar und unbrauchbar machen.

6. Sie sorgen dafür, dass unbeschadet der Artikel 122 und 123 nach Ablauf der in § 3 erwähnten auf diese Daten anwendbaren Vorratsspeicherungsfrist die auf Vorrat gespeicherten Daten von den Trägern entfernt werden.

7. Sie sorgen dafür, dass bei Anträgen auf Erhalt auf Vorrat gespeicherter Daten seitens einer in § 2 erwähnten Behörde die Nutzung dieser Daten rückverfolgt werden kann.

Die in Absatz 1 Nr. 7 erwähnte Rückverfolgbarkeit wird mit Hilfe eines Tagebuchs durchgeführt. Das Institut und der Ausschuss für den Schutz des Privatlebens dürfen dieses Tagebuch einsehen oder eine Kopie des gesamten oder eines Teils dieses Tagebuchs verlangen. Das Institut und der Ausschuss für den Schutz des Privatlebens schließen ein Zusammenarbeitsprotokoll über Kenntnisnahme und Kontrolle des Inhalts des Tagebuchs.

§ 5 - Der Minister und der Minister der Justiz sorgen dafür, dass der Abgeordnetenkammer jährlich eine Statistik über die Vorratsspeicherung der Daten übermittelt wird, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste beziehungsweise öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden.

Aus dieser Statistik muss hervorgehen:

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

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

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

Diese Statistik darf keine personenbezogenen Daten enthalten.

Die Daten, die die Anwendung von § 2 Nr. 1 betreffen, werden ebenfalls dem Bericht beigefügt, den der Minister der Justiz gemäß Artikel 90*decies* des Strafprozessgesetzbuches dem Parlament erstatten muss.

Der König legt auf Vorschlag des Ministers der Justiz und des Ministers nach Stellungnahme des Instituts die Statistik fest, die in § 1 Absatz 1 erwähnte Anbieter und Betreiber jährlich dem Institut übermitteln, und die Statistik, die das Institut dem Minister und dem Minister der Justiz übermittelt.

§ 6 - Unbeschadet des in § 5 Absatz 4 erwähnten Berichts erstatten der Minister und der Minister der Justiz der Abgeordnetenkammer zwei Jahre nach Inkrafttreten des in § 3 Absatz 4 erwähnten Königlichen Erlasses einen Evaluationsbericht über die Umsetzung des vorliegenden Artikels, damit überprüft wird, ob Bestimmungen angepasst werden müssen, insbesondere was die auf Vorrat zu speichernden Daten und die Vorratsspeicherungsfrist betrifft. ’

Art. 5 - In dasselbe Gesetz wird ein Artikel 126/1 mit folgendem Wortlaut eingefügt:

”Art. 126/1 - § 1 - Bei jedem in Artikel 126 § 1 Absatz 1 erwähnten Betreiber und Anbieter wird ein Koordinationsbüro eingerichtet, das beauftragt ist, den gesetzlich befugten belgischen Behörden auf deren Antrag hin aufgrund von Artikel 122, 123 und 126 auf Vorrat gespeicherte Daten, Identifizierungsdaten des Anrufers aufgrund von Artikel 107 § 2 Absatz 1 oder Daten, die aufgrund der Artikel 46*bis*, 88*bis* und 90*ter* des Strafprozessgesetzbuches und der Artikel 18/7, 18/8, 18/16 und 18/17 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten und Sicherheitsdienste angefordert werden können, zu übermitteln.

Gegebenenfalls können mehrere Betreiber oder Anbieter ein gemeinsames Koordinationsbüro schaffen. In diesem Fall muss das Koordinationsbüro denselben Dienst für jeden Betreiber oder Anbieter vorsehen.

Um dem Koordinationsbüro anzugehören müssen die Mitglieder:

1. Inhaber einer positiven und nicht abgelaufenen Sicherheitsstellungnahme gemäß Artikel 22*quinquies* des Gesetzes vom 11. Dezember 1998 über die Klassifizierung und die Sicherheitsermächtigungen, -bescheinigungen und -stellungnahmen sein,

2. nicht von einer Verweigerung durch den Justizminister betroffen sein; eine solche Verweigerung muss mit Gründen versehen sein und kann jederzeit eintreten.

Eine Stellungnahme wird fünf Jahre nach ihrer Abgabe als abgelaufen betrachtet.

Betreiber und Anbieter, die keinen der in Artikel 126 § 1 erwähnten Dienste anbieten, werden von der in Absatz 3 Nr. 1 erwähnten Bedingung befreit.

Nur die Mitglieder des Koordinationsbüros dürfen Anträge der Behörden in Bezug auf die in Absatz 1 erwähnten Daten beantworten. Sie dürfen jedoch unter ihrer Aufsicht und auf das Notwendigste beschränkt von Angestellten von Betreiber oder Anbieter technische Hilfe bekommen.

Mitglieder des Koordinationsbüros und Angestellte, die technische Hilfe leisten, unterliegen dem Berufsgeheimnis.

In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter achten auf die Vertraulichkeit der vom Koordinationsbüro verarbeiteten Daten und teilen dem Institut und Ausschuss für den Schutz des Privatlebens die Kontaktdaten des Koordinationsbüros und seiner Mitglieder und jede Änderung dieser Daten unverzüglich mit.

§ 2 - In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter richten interne Verfahren zur Beantwortung von Anfragen über den Zugang der Behörden zu den personenbezogenen Daten der Nutzer ein. Sie stellen dem Institut auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihre Antworten zur Verfügung.

In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter gelten für die aufgrund von Artikel 126 und des vorliegenden Artikels verarbeiteten Daten als für die Verarbeitung Verantwortliche im Sinne des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten.

Betreiber öffentlicher elektronischer Kommunikationsnetze und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt halten für den Zugang zu den in § 1 erwähnten Daten und ihre Übermittlung an die Behörden Artikel 114 § 2 ein.

§ 3 - In Artikel 126 § 1 Absatz 1 erwähnte Betreiber und Anbieter bestimmen einen oder mehrere Beauftragte für den Schutz personenbezogener Daten, der beziehungsweise die die in § 1 Absatz 3 erwähnten kumulativen Bedingungen erfüllen muss.

Dieser Beauftragte darf nicht dem Koordinationsbüro angehören.

Verschiedene Betreiber oder Anbieter dürfen einen oder mehrere gemeinsame Beauftragte für den Schutz personenbezogener Daten bestimmen. In diesem Fall dürfen diese Beauftragte denselben Auftrag für jeden individuellen Betreiber oder Anbieter ausführen.

Bei der Ausführung seiner Aufträge handelt der Beauftragte für den Schutz personenbezogener Daten vollkommen unabhängig und hat Zugang zu allen personenbezogenen Daten, die den Behörden übermittelt werden, und zu allen relevanten Räumlichkeiten von Anbieter und Betreiber.

Die Ausführung seiner Aufträge darf für den Beauftragten keine Nachteile mit sich bringen. Er darf insbesondere als Beauftragter aufgrund der Ausführung der Aufgaben, die ihm anvertraut sind, nicht ohne eingehende Begründung entlassen oder ersetzt werden.

Der Beauftragte muss die Möglichkeit haben, direkt mit dem Betreiber oder Anbieter zu kommunizieren.

Der Beauftragte für den Schutz personenbezogener Daten sorgt dafür, dass:

1. vom Koordinationsbüro durchgeführte Verarbeitungen gemäß dem Gesetz ausgeführt werden,

2. Anbieter oder Betreiber nur Daten sammelt und speichert, die er auch gesetzlich aufbewahren darf,

3. nur gesetzlich befugte Behörden Zugang zu den gespeicherten Daten haben,

4. Sicherheitsmaßnahmen und Maßnahmen zum Schutz von personenbezogenen Daten, die in vorliegendem Gesetz und in der Sicherheitspolitik von Anbieter und Betreiber beschrieben sind, durchgeführt werden.

In Artikel 126 § 1 Absatz 1 erwähnte Anbieter und Betreiber teilen dem Institut und dem Ausschuss für den Schutz des Privatlebens die Kontaktdaten der Beauftragten für den Schutz personenbezogener Daten und jede Änderung dieser Daten unverzüglich mit.

§ 4 - Der König bestimmt durch einen im Ministerrat beratenen Erlass nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts:

1. Modalitäten für Beantragung und Abgabe der Sicherheitsstellungnahme,

2. Anforderungen, die das Koordinationsbüro erfüllen muss, unter Berücksichtigung der Situation von Betreiber und Anbieter, die wenige Anträge von Gerichtsbehörden erhalten, die keine Niederlassung in Belgien haben oder hauptsächlich im Ausland tätig sind,

3. Informationen, die dem Institut und Ausschuss für den Schutz des Privatlebens gemäß den Paragraphen 1 und 3 zu übermitteln sind, und Behörden, die Zugang zu diesen Informationen haben,

4. andere Regeln für die Zusammenarbeit der in Artikel 126 § 1 Absatz 1 erwähnten Betreiber und Anbieter mit den belgischen Behörden oder bestimmten unter ihnen für die Übermittlung der in § 1 erwähnten Daten, gegebenenfalls einschließlich Form und Inhalt des Antrags pro betroffene Behörde. ’

Art. 6 - Artikel 127 desselben Gesetzes, abgeändert durch die Gesetze vom 4. Februar 2010, 10. Juli 2012 und 27. März 2014, wird wie folgt abgeändert:

1. Paragraph 1 wird wie folgt abgeändert:

a) In Absatz 1 werden zwischen dem Wort ’ Betreibern ’ und den Wörtern ’ und Endnutzern ’ die Wörter ’ Anbietern wie in Artikel 126 § 1 Absatz 1 erwähnt ’ eingefügt.

b) In Absatz 2 werden zwischen dem Wort ' Betreiber ' und den Wörtern ' an den in Absatz 1 Nr. 2 erwähnten Handlungen ' die Wörter ' und Anbieter wie in Artikel 126 § 1 Absatz 1 erwähnt ' eingefügt.

2. Paragraph 6 wird aufgehoben.

Art. 7 - Artikel 145 desselben Gesetzes, abgeändert durch die Gesetze vom 25. April 2007 und 27. März 2014, wird wie folgt abgeändert:

1. Zwischen dem Wort ' 124, ' und dem Wort ' 127 ' werden die Wörter ' 126, 126/1, ' eingefügt.

2. Zwischen dem Wort ' 47 ' und den Wörtern ' und 127 ' werden die Wörter ', 126, 126/1 ' eingefügt.

3. Anstelle von § 3*ter*, für nichtig erklärt durch Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird ein § 3*ter* mit folgendem Wortlaut eingefügt:

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

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

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

KAPITEL 3 — *Abänderungen des Strafprozessgesetzbuches*

Art. 8 - Artikel 46*bis* § 1 des Strafprozessgesetzbuches, eingefügt durch das Gesetz vom 10. Juni 1998 und ersetzt durch das Gesetz vom 23. Januar 2007, wird wie folgt abgeändert:

a) [Abänderung des französischen Textes]

b) Der Paragraph wird durch einen Absatz mit folgendem Wortlaut ergänzt:

' Für Straftaten, die keine Hauptkorrektionalgefängnisstrafe von einem Jahr oder keine schwerere Strafe zur Folge haben können, kann der Prokurator des Königs oder, in Fällen äußerster Dringlichkeit, der Gerichtspolizeioffizier die in Absatz 1 erwähnten Daten nur für einen Zeitraum von sechs Monaten vor seiner Entscheidung anfordern. '

Art. 9 - Artikel 88*bis* desselben Gesetzbuches, eingefügt durch das Gesetz vom 11. Februar 1991, ersetzt durch das Gesetz vom 10. Juni 1998 und abgeändert durch die Gesetze vom 8. Juni 2008 und 27. Dezember 2012, wird wie folgt abgeändert:

a) Paragraph 1 Absatz 1 wird wie folgt ersetzt:

' Wenn es schwerwiegende Indizien dafür gibt, dass die Straftaten eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können, und wenn der Untersuchungsrichter der Meinung ist, dass es Umstände gibt, die die Erfassung von elektronischen Nachrichten oder die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten notwendig machen, um die Wahrheit herauszufinden, kann er, nötigenfalls indem er dazu direkt oder über einen vom König bestimmten Polizeidienst die technische Mitwirkung des Betreibers eines elektronischen Kommunikationsnetzes oder des Anbieters eines elektronischen Kommunikationsdienstes anfordert, Folgendes vornehmen oder vornehmen lassen:

1. die Erfassung der Verkehrsdaten von elektronischen Kommunikationsmitteln, von denen elektronische Nachrichten ausgehen oder ausgingen beziehungsweise an die elektronische Nachrichten gerichtet sind oder waren,

2. die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten. '

b) In § 1 Absatz 2 wird das Wort ' Telekommunikationsmittel ' durch die Wörter ' elektronische Kommunikationsmittel ' ersetzt und werden die Wörter ' der Fernmeldeverbindung ' jeweils durch die Wörter ' der elektronischen Nachricht ' ersetzt.

c) Paragraph 1 Absatz 3 wird wie folgt ersetzt:

' Der Untersuchungsrichter gibt die tatsächlichen Umstände der Sache, die die Maßnahme rechtfertigen, deren Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und deren Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe in einem mit Gründen versehenen Beschluss an. '

d) Paragraph 1 Absatz 4 wird wie folgt ersetzt:

' Er gibt auch die Dauer der Maßnahme für die Zukunft an, die nicht länger als zwei Monate ab dem Beschluss betragen darf, unbeschadet einer Erneuerung, und gegebenenfalls den Zeitraum in der Vergangenheit, über den der Beschluss sich gemäß § 2 erstreckt. '

e) Paragraph 1 wird durch einen Absatz mit folgendem Wortlaut ergänzt:

' Im Dringlichkeitsfall kann die Maßnahme mündlich angeordnet werden. Sie muss so schnell wie möglich in der in den Absätzen 3 und 4 vorgesehenen Form bestätigt werden. '

f) Paragraph 2, dessen heutiger Text § 4 wird, wird wie folgt ersetzt:

' § 2 - In Bezug auf die Anwendung der in § 1 Absatz 1 erwähnten Maßnahme auf die Verkehrs- oder Standortdaten, die aufgrund von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation gespeichert werden, gelten folgende Bestimmungen:

- Für eine in Buch II Titel I*ter* des Strafgesetzbuches erwähnte Straftat kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von zwölf Monaten vor dem Beschluss anfordern.

- Für eine andere in Artikel 90*ter* § § 2 bis 4 erwähnte Straftat, die nicht im ersten Gedankenstrich erwähnt ist, oder für eine Straftat, die im Rahmen einer in Artikel 324*bis* des Strafgesetzbuches erwähnten kriminellen Organisation begangen worden ist, oder für eine Straftat, die eine Hauptkorrektionalgefängnisstrafe von fünf Jahren oder eine schwerere Strafe zur Folge haben kann, kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von neun Monaten vor dem Beschluss anfordern.

- Für andere Straftaten kann der Untersuchungsrichter die Daten nur für einen Zeitraum von sechs Monaten vor dem Beschluss anfordern. '

g) Der Artikel wird durch einen Paragraphen 3 mit folgendem Wortlaut ergänzt:

' § 3 - Die Maßnahme darf sich nur dann auf elektronische Kommunikationsmittel eines Rechtsanwalts oder Arztes beziehen, wenn dieser selber verdächtigt wird, eine in § 1 erwähnte Straftat begangen zu haben oder daran beteiligt gewesen zu sein, oder wenn genaue Tatsachen vermuten lassen, dass Dritte, die verdächtigt werden, eine in § 1 erwähnte Straftat begangen zu haben, seine elektronischen Kommunikationsmittel benutzen.

Die Maßnahme darf nicht durchgeführt werden, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter der provinzialen Ärztekammer davon in Kenntnis gesetzt worden ist. Dieselben Personen werden vom Untersuchungsrichter darüber in Kenntnis gesetzt, welche Elemente seiner Meinung nach unter das Berufsgeheimnis fallen. Diese Elemente werden nicht im Protokoll festgehalten. '

h) In § 2, der zu § 4 umnummeriert wird, werden in Absatz 1 die Wörter ' Jeder Betreiber eines Telekommunikationsnetzes und jeder Anbieter einer Telekommunikationsdienstleistung ' durch die Wörter ' Jeder Betreiber eines elektronischen Kommunikationsnetzes und jeder Anbieter eines elektronischen Kommunikationsdienstes ' ersetzt.

Art. 10 - Artikel 90*decies* desselben Gesetzbuches, eingefügt durch das Gesetz vom 30. Juni 1994 und abgeändert durch die Gesetze vom 8. April 2002, 7. Juli 2002, 6. Januar 2003 und durch das Gesetz vom 30. Juli 2013, für nichtig erklärt durch den Entscheid Nr. 84/2015 des Verfassungsgerichtshofes, wird durch einen Absatz mit folgendem Wortlaut ergänzt:

' Diesem Bericht wird ebenfalls der in Anwendung von Artikel 126 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erstellte Bericht beigefügt. '

Art. 11 - In Artikel 464/25 § 2 Absatz 1 desselben Gesetzbuches werden die Wörter ' Artikel 88*bis* § 2 Absatz 1 und 3 ' durch die Wörter ' Artikel 88*bis* § 4 Absatz 1 und 3 ' ersetzt.

KAPITEL 4 — *Abänderungen des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste*

Art. 12 - Artikel 13 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste, abgeändert durch das Gesetz vom 4. Februar 2010, wird wie folgt abgeändert:

1. *[Abänderung des niederländischen Textes]*

2. Absatz 3 wird wie folgt ersetzt:

' Die Nachrichten- und Sicherheitsdienste sorgen für die Sicherheit der Angaben, die sich auf ihre Quellen beziehen, und der von diesen Quellen gelieferten Informationen und personenbezogenen Daten. '

3. Der Artikel wird durch einen Absatz mit folgendem Wortlaut ergänzt:

' Die Bediensteten der Nachrichten- und Sicherheitsdienste haben Zugang zu den von ihrem Dienst gesammelten und verarbeiteten Informationen, Auskünfte und personenbezogenen Daten, sofern diese bei der Ausübung ihrer Funktion oder ihres Auftrags nützlich sind. '

Art. 13 - Artikel 18/3 desselben Gesetzes, eingefügt durch das Gesetz vom 4. Februar 2010, wird wie folgt abgeändert:

a) Der heutige Paragraph 1 Absatz 3 wird Paragraph 5.

b) In § 1 Absatz 4, der § 7 wird, werden die Wörter ' um die spezifische Methode zum Sammeln von Daten anzuwenden ' durch die Wörter ' um die Anwendung der spezifischen Methode zum Sammeln von Daten zu überwachen ' ersetzt.

c) Paragraph 2, dessen heutige Absätze 2 bis 5 § 6 werden, wird wie folgt ersetzt:

' § 2 - Die Entscheidung des Dienstleiters enthält Folgendes:

1. die Art der spezifischen Methode,

2. je nach Fall, die natürlichen oder juristischen Personen, Vereinigungen oder Gruppierungen, Gegenstände, Orte, Ereignisse oder Informationen, die Gegenstand der spezifischen Methode sind,

3. die potentielle Gefahr, die die spezifische Methode rechtfertigt,

4. die tatsächlichen Umstände, die die spezifische Methode rechtfertigen, die Begründung in Sachen Subsidiarität und Verhältnismäßigkeit, einschließlich der Verbindung zwischen Nr. 2 und 3,

5. den Zeitraum ab der Notifizierung der Entscheidung an den Ausschuss, in dem die spezifische Methode angewandt werden kann,

6. den Namen des Nachrichtenoffiziers (der Nachrichtenoffiziere), der (die) für die Überwachung der Anwendung der spezifischen Methode verantwortlich ist (sind),

7. gegebenenfalls, das technische Mittel, das bei der Anwendung der spezifischen Methode benutzt wird,

8. gegebenenfalls, das Zusammentreffen mit einem Ermittlungsverfahren oder einer gerichtlichen Untersuchung,

9. gegebenenfalls, die ernstzunehmenden Indizien dafür, dass der Rechtsanwalt, der Arzt oder der Journalist persönlich und aktiv an der Entstehung oder der Entwicklung der potentiellen Gefahr mitwirkt oder mitgewirkt hat,

10. in dem Fall, in dem Artikel 18/8 Anwendung findet, die Begründung der Dauer des Zeitraums, auf den die Sammlung der Daten bezogen ist,

11. das Datum der Entscheidung,

12. die Unterschrift des Dienstleiters. '

d) Paragraph 3 wird wie folgt ersetzt:

' § 3 - Für jede spezifische Methode wird dem Ausschuss am Ende jedes Monats eine Liste der ausgeführten Maßnahmen übermittelt.

Diese Listen umfassen die in § 2 Nr. 1 bis 3, 5 und 7 aufgeführten Daten. '

e) Der Artikel wird durch einen Paragraphen 8 mit folgendem Wortlaut ergänzt:

' § 8 - Der Dienstleiter beendet die spezifische Methode, wenn die potentielle Gefahr, die die Methode gerechtfertigt hat, nicht mehr besteht, wenn die Methode für den Zweck, für den sie angewandt worden ist, nicht mehr nützlich ist oder wenn er eine Rechtsverletzung festgestellt hat. Er setzt den Ausschuss schnellstmöglich von seiner Entscheidung in Kenntnis. '

Art. 14 - Artikel 18/8 desselben Gesetzes, eingefügt durch das Gesetz vom 4. Februar 2010, wird wie folgt abgeändert:

a) Paragraph 1 Absatz 3 wird wie folgt ersetzt:

' Die Nachrichten- und Sicherheitsdienste können im Interesse der Erfüllung ihrer Aufträge, notfalls indem sie dazu die technische Mitwirkung des Betreibers eines elektronischen Kommunikationsnetzes oder des Anbieters eines elektronischen Kommunikationsdienstes anfordern, Folgendes vornehmen oder vornehmen lassen:

1. die Erfassung der Verkehrsdaten von elektronischen Kommunikationsmitteln, von denen elektronische Nachrichten ausgehen oder ausgingen beziehungsweise an die elektronische Nachrichten gerichtet sind oder waren,

2. die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten. ’

b) In § 1 Absatz 2 wird das Wort ’ Verbindungsdaten ’ durch das Wort ’ Verkehrsdaten ’ ersetzt.

c) Paragraph 2, dessen heutiger Text § 4 wird, wird wie folgt ersetzt:

’ § 2 - In Bezug auf die Anwendung der in § 1 erwähnten Methode auf die Daten, die aufgrund von Artikel 126 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation gespeichert werden, gelten folgende Bestimmungen:

1. Für eine potentielle Gefahr, die sich auf eine Aktivität mit möglichem Bezug zu kriminellen Organisationen oder schädlichen sektiererischen Organisationen bezieht, kann der Dienstleiter in seiner Entscheidung die Daten nur für einen Zeitraum von sechs Monaten vor der Entscheidung anfordern.

2. Für eine potentielle Gefahr, die nicht in Nr. 1 und Nr. 3 erwähnt ist, kann der Dienstleiter in seiner Entscheidung die Daten für einen Zeitraum von neun Monaten vor der Entscheidung anfordern.

3. Für eine potentielle Gefahr, die sich auf eine Aktivität mit möglichem Bezug zu Terrorismus oder Extremismus bezieht, kann der Dienstleiter in seiner Entscheidung die Daten für einen Zeitraum von zwölf Monaten vor der Entscheidung anfordern. ’

Art. 15 - In Artikel 43/3 desselben Gesetzes, eingefügt durch das Gesetz vom 4. Februar 2010, werden die Wörter ’ Artikel 18/3 § 2 ’ durch die Wörter ’ Artikel 18/3 § 3 ’ ersetzt.

Art. 16 - In Artikel 43/5 § 1 Absatz 2 desselben Gesetzes werden die Wörter ’ Artikel 18/3 § 2 ’ durch die Wörter ’ Artikel 18/3 § 3 ’ ersetzt ».

B.2. Durch das angefochtene Gesetz wollte der Gesetzgeber der Nichtigerklärung von Artikel 126 des Gesetzes vom 13. Juni 2005 « über die elektronische Kommunikation » (nachstehend: Gesetz vom 13. Juni 2005), abgeändert 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 », durch den Entscheid Nr. 84/2015 des Gerichtshofes vom 11. Juni 2015 Rechnung tragen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1567/001, S. 4).

B.3. Aus den Vorarbeiten zu dem angefochtenen Gesetz geht hervor, dass der Gesetzgeber sowohl den vorerwähnten Entscheid Nr. 84/2015 des Gerichtshofes vom 11. Juni 2015 als auch das Urteil des Gerichtshofes der Europäischen Union vom 8. April 2014 in den verbundenen Rechtssachen *Digital Rights Ireland Ltd* (C-293/12) und *Kärntner Landesregierung u.a.* (C-594/12), mit dem der Gerichtshof die 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 » für ungültig erklärt hat und auf dem der Entscheid Nr. 84/2015 beruht, gründlich geprüft hat.

Das Ziel, das der Gesetzgeber mit dem angefochtenen Gesetz 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. 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 (ebenda, SS. 10-18).

Zur Hauptsache

B.5. Der einzige Klagegrund in den Rechtssachen Nrn. 6590 und 6597 ist aus einem Verstoß durch das angefochtene Gesetz gegen die 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 abgeleitet.

B.6.1. 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.6.2. Die klagende Partei in der Rechtssache Nr. 6590 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.7.1. Die klagenden Parteien in der Rechtssache Nr. 6597 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.7.2. 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.8.1. Der erste Klagegrund in der Rechtssache Nr. 6599 ist aus einem Verstoß gegen die 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.8.2. Die VoG « Liga voor Mensenrechten » und die VoG « Ligue des Droits de l'Homme » (nunmehr « Ligue des droits humains »), 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.9.1. Der erste Klagegrund in der Rechtssache Nr. 6601 ist aus einem Verstoß durch das angefochtene Gesetz gegen Artikel 8 der Europäischen Menschenrechtskonvention, die Artikel 7, 8, 11 Absatz 1 und 52 der Charta der Grundrechte der Europäischen Union, die Artikel 10, 11, 19 und 22 der Verfassung, Artikel 2 Buchstabe 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 die 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 (Datenschutzrichtlinie für elektronische Kommunikation » (nachstehend: Richtlinie 2002/58/EG) abgeleitet.

B.9.2. Die klagenden Parteien in der Rechtssache Nr. 6601 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.10. In Anbetracht ihres Zusammenhangs werden die in den verschiedenen Rechtssachen dargelegten Klagegründe zusammen geprüft.

B.11.1. Unter Berücksichtigung einerseits der unterschiedlichen Meinungen der klagenden Parteien und des Ministerrats darüber, wie verschiedene Bestimmungen auszulegen sind, insbesondere Artikel 15 Absatz 1 der 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, und andererseits der vom Ministerrat angeführten Erklärungen, um die Vereinbarkeit des angefochtenen Gesetzes mit den von den klagenden Parteien geltend gemachten Referenznormen zu rechtfertigen, hat der Gerichtshof mit seinem Entscheid Nr. 96/2018 vom 19. Juli 2018 dem Gerichtshof der Europäischen Union die folgenden drei Vorabentscheidungsfragen gestellt:

« 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.11.2. Artikel 15 Absatz 1 der Richtlinie 2002/58/EG bestimmt:

« Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für 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 in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen ».

B.11.3. Der Gerichtshof hat ebenfalls entschieden, die Prüfung der Rechtssachen auszusetzen, bis der Gerichtshof der Europäischen Union ein Urteil in den Rechtssachen *Ministerio Fiscal* (C-207/16) und *Privacy International gegen Secretary of State for Foreign and Commonwealth Affairs u.a.* (C-623/17) gefällt hat.

B.12. Mit ihrem Urteil vom 2. Oktober 2018 in der Rechtssache *Ministerio Fiscal* (C-207/16) hat die Große Kammer des Gerichtshofes entschieden, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta der Grundrechte der Europäischen Union verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste. Dieses Urteil beruht auf der folgenden Begründung:

« *Zur Beantwortung der Fragen*

48. Mit seinen beiden Fragen, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundreche darstellt, der so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste, und nach welchen Kriterien bejahendenfalls die Schwere der in Rede stehenden Straftat zu beurteilen ist.

49. Insoweit geht, wie der Generalanwalt in Nr. 38 seiner Schlussanträge ausgeführt hat, aus dem Vorabentscheidungsersuchen hervor, dass mit diesem nicht geklärt werden soll, ob die im Ausgangsverfahren in Rede stehenden personenbezogenen Daten von den Betreibern elektronischer Kommunikationsdienste unter Beachtung der in Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta vorgesehenen Voraussetzungen gespeichert wurden. Das Ersuchen bezieht sich, wie sich aus Rn. 46 des vorliegenden Urteils ergibt, nur auf die Frage, ob und inwieweit der Zweck der im Ausgangsverfahren in Rede stehenden Regelung geeignet ist, den Zugang öffentlicher Stellen wie der Kriminalpolizei zu solchen Daten zu rechtfertigen, ohne dass die übrigen Zugangsvoraussetzungen nach diesem Art. 15 Abs. 1 Gegenstand dieses Ersuchens wären.

50. Das vorlegende Gericht möchte insbesondere wissen, nach welchen Gesichtspunkten zu beurteilen ist, ob die Straftaten, bezüglich deren den Polizeibehörden zu Ermittlungszwecken der Zugang zu personenbezogenen Daten erlaubt wird, die die Betreiber elektronischer Kommunikationsdienste gespeichert haben, hinreichend schwer sind, um den mit einem solchen Zugang verbundenen Eingriff in die in den Art. 7 und 8 der Charta gewährleisteten Grundrechte, wie sie vom Gerichtshof in seinen Urteilen vom 8. April 2014, *Digital Rights Ireland u. a.* (C-293/12 und C-594/12, EU: C: 2014: 238), und *Tele2 Sverige und Watson u. a.*, ausgelegt worden sind, zu rechtfertigen.

51. Was das Vorliegen eines Eingriffs in diese Grundrechte betrifft, stellt, wie der Generalanwalt in den Nrn. 76 und 77 seiner Schlussanträge ausgeführt hat, der Zugang der öffentlichen Stellen zu solchen Daten einen Eingriff in das in Art. 7 der Charta verankerte Grundrecht auf Achtung des Privatlebens dar, auch wenn keine Umstände vorliegen, aufgrund deren dieser Eingriff als ' schwer ' eingestuft werden kann, und ohne dass es darauf ankommt, ob die betroffenen Informationen über das Privatleben als sensibel anzusehen sind oder die Betroffenen durch diesen Eingriff irgendwelche Nachteile erlitten haben. Zudem stellt ein solcher Zugang einen Eingriff in das in Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar, da es sich dabei um eine Verarbeitung personenbezogener Daten handelt (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung).

52. Hinsichtlich der Zwecke, die eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende - die den Zugang öffentlicher Stellen zu von Betreibern elektronischer Kommunikationsdienste gespeicherten Daten betrifft und damit vom Grundsatz der Vertraulichkeit elektronischer Kommunikationen abweicht - rechtfertigen können, ist darauf hinzuweisen, dass die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zwecke abschließend ist, so dass dieser Zugang tatsächlich strikt einem dieser Zwecke dienen muss (vgl. in diesem Sinne Urteil *Tele2 Sverige und Watson u. a.*, Rn. 90 und 115).

53. Was den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, ist aber festzustellen, dass dieser nach dem Wortlaut von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 nicht auf die Bekämpfung schwerer Straftaten beschränkt ist, sondern ' Straftaten ' im Allgemeinen betrifft.

54. Insoweit hat der Gerichtshof zwar entschieden, dass im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung der schweren Kriminalität einen Zugang öffentlicher Stellen zu von den Betreibern von Kommunikationsdiensten gespeicherten personenbezogenen Daten rechtfertigen kann, aus deren Gesamtheit genaue Schlüsse auf das Privatleben der von diesen Daten betroffenen Personen gezogen werden können (vgl. in diesem Sinne Urteil *Tele2 Sverige und Watson u. a.*, Rn. 99).

55. Der Gerichtshof hat diese Auslegung jedoch damit begründet, dass der mit einer solchen Zugangsregelung verfolgte Zweck im Verhältnis zur Schwere des damit einhergehenden Eingriffs in die betreffenden Grundrechte stehen muss (vgl. in diesem Sinne Urteil *Tele2 Sverige und Watson u. a.*, Rn. 115).

56. Nach dem Grundsatz der Verhältnismäßigkeit kann ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nämlich nur durch einen Zweck der Bekämpfung einer ebenfalls als ' schwer ' einzustufenden Kriminalität gerechtfertigt sein.

57. Ist dagegen der mit einem solchen Zugang verbundene Eingriff nicht schwer, kann dieser Zugang durch einen Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von ' Straftaten ' im Allgemeinen gerechtfertigt sein.

58. Es ist daher zunächst zu prüfen, ob nach den Umständen des vorliegenden Falles der Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte, der mit einem Zugang der Kriminalpolizei zu den im Ausgangsverfahren in Rede stehenden Daten einhergeht, als ' schwer ' anzusehen ist.

59. Insoweit ist festzustellen, dass der im Ausgangsverfahren in Rede stehende Antrag, mit dem die Kriminalpolizei für die Zwecke strafrechtlicher Ermittlungen um gerichtliche Erlaubnis zum Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten ersucht, ausschließlich darauf abzielt, die Identität der Inhaber von SIM-Karten festzustellen, die in einem Zeitraum von zwölf Tagen mit der IMEI des gestohlenen Mobiltelefons aktiviert wurden. Wie in Rn. 40 des vorliegenden Urteils ausgeführt, bezieht sich dieser Antrag nur auf den Zugang zu den diesen SIM-Karten entsprechenden Telefonnummern sowie zu den Daten bezüglich der Identität der Karteninhaber wie deren Name, Vorname und gegebenenfalls Adresse. Dagegen beziehen sich diese Daten, wie sowohl die spanische Regierung als auch die Staatsanwaltschaft in der mündlichen Verhandlung bestätigt haben, weder auf die mittels des gestohlenen Mobiltelefons erfolgte Kommunikation noch auf dessen Ortung.

60. Daher kann mit den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Zugangsantrag bezieht, offenbar nur eine Verbindung zwischen der SIM-Karte oder den SIM-Karten, die mit dem gestohlenen Mobiltelefon aktiviert wurden, und der Identität der Inhaber dieser SIM-Karten während eines bestimmten Zeitraums hergestellt werden. Ohne einen Abgleich mit den Daten bezüglich der mittels dieser SIM-Karten erfolgten Kommunikation und den Standortdaten lassen sich diesen Daten weder das Datum, die Uhrzeit, die Dauer und die Adressaten der mittels der betreffenden SIM-Karte bzw. der betreffenden SIM-Karten erfolgten Kommunikation entnehmen noch die Orte, an denen diese Kommunikation erfolgte, oder die Häufigkeit dieser Kommunikation mit bestimmten Personen während eines bestimmten Zeitraums. Aus diesen Daten lassen sich daher keine genauen Schlüsse auf das Privatleben der Personen ziehen, deren Daten betroffen sind.

61. Unter diesen Umständen kann der Zugang nur zu den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Antrag bezieht, nicht als ' schwerer ' Eingriff in die Grundrechte der Personen eingestuft werden, deren Daten betroffen sind.

62. Wie sich aus den Rn. 53 bis 57 des vorliegenden Urteils ergibt, kann der Eingriff, den ein Zugang zu solchen Daten mit sich bringen würde, somit durch den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von ' Straftaten ' im Allgemeinen gerechtfertigt sein, ohne dass es erforderlich wäre, dass diese Straftaten als ' schwer ' einzustufen sind.

63. Nach alledem ist auf die Vorlagefragen zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass der Zugang öffentlicher Stellen zu Daten, anhand deren die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt werden soll, wie Name, Vorname und gegebenenfalls Adresse dieser Karteninhaber, einen Eingriff in deren in diesen Artikeln der Charta der Grundrechte verankerte Grundreche darstellt, der nicht so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste ».

B.13. Mit ihrem Urteil vom 6. Oktober 2020 in der Rechtssache *Privacy International* (C-623/17) hat die Große Kammer des Gerichtshofes entschieden, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht von Artikel 4 Absatz 2 des Vertrags über die Europäische Union sowie der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln. Dieses Urteil beruht auf der folgenden Begründung:

« *Zur zweiten Frage*

50. Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln.

51. Zunächst ist darauf hinzuweisen, dass Section 94 des Gesetzes von 1984 nach den Angaben im Vorabentscheidungsersuchen dem Minister gestattet, den Betreibern elektronischer Kommunikationsdienste durch Weisungen vorzuschreiben, den Sicherheits- und Nachrichtendiensten Massen-Kommunikationsdaten, zu denen Verkehrs- und Standortdaten sowie Informationen über die genutzten Dienste im Sinne von Section 21(4) und (6) des RIPA gehören, zu übermitteln, wenn er dies im Interesse der nationalen Sicherheit oder der Beziehungen zu einer ausländischen Regierung für erforderlich hält. Die letztgenannte Bestimmung erfasst u. a. die Daten, die notwendig sind, um die Quelle und den Adressaten einer Kommunikation aufzuspüren, Datum, Uhrzeit, Dauer und Art der Kommunikation zu ermitteln, das verwendete Kommunikationsmaterial zu identifizieren sowie den Standort der Endgeräte und der Kommunikationen zu bestimmen. Zu diesen Daten gehören u. a. Name und Adresse des Nutzers, die Telefonnummern des Anrufers und des Angerufenen, die IP-Adressen der Quelle und des Adressaten der Kommunikation sowie die Adressen der besuchten Websites.

52. Eine solche Offenlegung durch Übermittlung der Daten betrifft alle Nutzer elektronischer Kommunikationsmittel, ohne dass näher angegeben wird, ob die Übermittlung in Echtzeit oder zeitversetzt erfolgen muss. Im Anschluss an ihre Übermittlung werden diese Daten nach den Angaben im Vorabentscheidungsersuchen von den Sicherheits- und Nachrichtendiensten gespeichert und stehen ihnen für ihre Tätigkeiten ebenso zur Verfügung wie ihre übrigen Datenbanken. Insbesondere können die auf diese Weise gesammelten Daten, die automatisierten Massenverarbeitungen und -analysen unterzogen werden, mit anderen Datenbanken, die andere Kategorien personenbezogener Massendaten enthalten, abgeglichen oder an Stellen außerhalb dieser Dienste und an Drittstaaten weitergegeben werden. Schließlich bedürfen diese Vorgänge keiner vorherigen Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle, und die Betroffenen werden nicht davon unterrichtet.

53. Die Richtlinie 2002/58 soll, wie sich u. a. aus ihren Erwägungsgründen 6 und 7 ergibt, die Nutzer elektronischer Kommunikationsdienste vor den Risiken für ihre personenbezogenen Daten und ihre Privatsphäre schützen, die sich aus den neuen Technologien und vor allem den zunehmenden Fähigkeiten zur automatisierten Speicherung und Verarbeitung von Daten ergeben. Insbesondere soll mit der Richtlinie nach ihrem zweiten Erwägungsgrund gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM [2000] 385 endg.), aus dem die Richtlinie 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber sicherstellen wollte, ' dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt '.

54. Zu diesem Zweck sieht Art. 5 Abs. 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten ' durch innerstaatliche Vorschriften die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicher [stellen] '. Weiter heißt es dort: ' Insbesondere untersagen [die Mitgliedstaaten] das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. ' Art. 5 Abs. 1 ' steht - unbeschadet des Grundsatzes der Vertraulichkeit - der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen. '

55. In Art. 5 Abs. 1 der Richtlinie 2002/58 wird somit der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt, der u. a. das grundsätzliche Verbot für jede andere Person als die Nutzer impliziert, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern. In Anbetracht ihres allgemein gehaltenen Wortlauts gilt diese Bestimmung notwendigerweise für jeden Vorgang, der es Dritten erlaubt, zu anderen Zwecken als der Weiterleitung einer Nachricht Kenntnis von Nachrichten und den damit verbundenen Daten zu erlangen.

56. Das Verbot in Art. 5 Abs. 1 der Richtlinie 2002/58, Nachrichten und die damit verbundenen Daten abzufangen, erfasst deshalb jede Form der Bereitstellung von Verkehrs- und Standortdaten durch die Betreiber elektronischer Kommunikationsdienste für Behörden wie Sicherheits- und Nachrichtendienste sowie die Speicherung solcher Daten durch diese Behörden, unabhängig von einer späteren Verwendung dieser Daten.

57. Durch den Erlass dieser Richtlinie hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der Charta verankerten Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Daten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 109).

58. Art. 15 Abs. 1 der Richtlinie 2002/58 gestattet es den Mitgliedstaaten jedoch, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten sowie den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten zu schaffen, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten u. a. durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit aufbewahrt werden.

59. Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 der Richtlinie 2002/58 vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 89 und 104, sowie vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 111).

60. Außerdem geht aus Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 hervor, dass die Mitgliedstaaten Rechtsvorschriften, die die Tragweite der Rechte und Pflichten gemäß den Art. 5, 6 und 9 dieser Richtlinie beschränken sollen, nur unter Beachtung der allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und der durch die Charta garantierten Grundrechte erlassen dürfen. Hierzu hat der Gerichtshof bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die die Einhaltung nicht nur der die Achtung des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta betreffen, sondern auch der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 25 und 70, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 91 und 92 sowie die dort angeführte Rechtsprechung).

61. Die gleichen Fragen stellen sich auch für andere Arten der Verarbeitung von Daten, wie ihre Übermittlung an andere Personen als die Nutzer oder den Zugang zu ihnen im Hinblick auf ihre Nutzung (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 122 und 123 sowie die dort angeführte Rechtsprechung).

62. Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Rechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Rechts auf den Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt, berücksichtigt werden sowie das in Art. 11 der Charta gewährleistete Grundrecht auf freie Meinungsäußerung, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urteile vom 6. März 2001, *Connolly/Kommission*, C-274/99 P, EU: C: 2001: 127, Rn. 39, und vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 93 und die dort angeführte Rechtsprechung).

63. Die in den Art. 7, 8 und 11 der Charta verankerten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden (vgl. in diesem Sinne Urteil vom 16. Juli 2020, *Facebook Ireland und Schrems*, C-311/18, EU: C: 2020: 559, Rn. 172 und die dort angeführte Rechtsprechung).

64. Nach Art. 52 Abs. 1 der Charta sind nämlich Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

65. Hinzuzufügen ist, dass das Erfordernis, dass jede Einschränkung der Ausübung von Grundrechten gesetzlich vorgesehen sein muss, bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen muss (Urteil vom 16. Juli 2020, *Facebook Ireland und Schrems*, C-311/18, EU: C: 2020: 559, Rn. 175 und die dort angeführte Rechtsprechung).

66. In Bezug auf die Beachtung des Grundsatzes der Verhältnismäßigkeit sieht Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die vom 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 der Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem ' strikt ' angemessenen Verhältnis zum intendierten Zweck stehen muss.

67. Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Außerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der Zielsetzung und der fraglichen Rechte und Pflichten vorgenommen wird (vgl. in diesem Sinne Urteile vom 16. Dezember 2008, *Satakunnan Markkinapörssi und Satamedia*, C-73/07, EU: C: 2008: 727, Rn. 56, vom 9. November 2010, *Volker und Markus Schecke und Eifert*, C-92/09 und C-93/09, EU: C: 2010: 662, Rn. 76, 77 und 86, sowie vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 52; Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 140).

68. Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der speziellen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 54 und 55, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 117; Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 141).

69. Zu der Frage, ob eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta den Anforderungen von Art. 15 Abs. 1 der Richtlinie 2002/58 genügt, ist festzustellen, dass die Übermittlung von Verkehrs- und Standortdaten an andere Personen als die Nutzer, etwa an die Sicherheits- und Nachrichtendienste, vom Grundsatz der Vertraulichkeit abweicht. Geschieht dies, wie hier, in allgemeiner und unterschiedsloser Weise, wird die Abweichung von der grundsätzlichen Pflicht zur Gewährleistung der Vertraulichkeit der Daten zur Regel, obwohl das durch die Richtlinie 2002/58 geschaffene System verlangt, dass eine solche Abweichung die Ausnahme bleibt.

70. Zudem stellt nach ständiger Rechtsprechung des Gerichtshofs die Übermittlung von Verkehrs- und Standortdaten an einen Dritten einen Eingriff in die Grundrechte dar, die in den Art. 7 und 8 der Charta verankert sind, unabhängig davon, wie diese Daten später genutzt werden. Dabei spielt es keine Rolle, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben und ob die Betroffenen durch diesen Eingriff Nachteile erlitten haben (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung, und Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 115 und 116).

71. Der mit der Übermittlung von Verkehrs- und Standortdaten an die Sicherheits- und Nachrichtendienste verbundene Eingriff in das in Art. 7 der Charta verankerte Recht ist insbesondere angesichts des sensiblen Charakters der Informationen, die diese Daten liefern können, und vor allem angesichts der Möglichkeit, anhand von ihnen ein Profil der Betroffenen zu erstellen, als besonders schwer anzusehen, da eine solche Information ebenso sensibel ist wie der Inhalt der Kommunikationen selbst. Überdies ist er geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist (vgl. entsprechend Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 27 und 37, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 99 und 100).

72. Hinzuzufügen ist, dass eine Übermittlung von Verkehrs- und Standortdaten an Behörden zu Sicherheitszwecken für sich genommen das in Art. 7 der Charta verankerte Recht auf Achtung der Kommunikation beeinträchtigen und die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung abhalten kann. Solche abschreckenden Wirkungen können in besonderem Maß Personen treffen, deren Kommunikationen nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen, sowie Whistleblower, deren Aktivitäten durch die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (*ABl.* 2019, L 305, S. 17), geschützt werden. Außerdem sind diese Wirkungen umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 28, vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 101, und vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 118).

73. Schließlich birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste angesichts der großen Menge von Verkehrs- und Standortdaten, die durch eine Maßnahme allgemeiner Vorratsspeicherung kontinuierlich gespeichert werden können, sowie des sensiblen Charakters der Informationen, die diese Daten liefern können, Gefahren des Missbrauchs und des rechtswidrigen Zugangs.

74. Zu den Zielen, die solche Eingriffe rechtfertigen können, und insbesondere zu dem im Ausgangsverfahren in Rede stehenden Ziel der Wahrung der nationalen Sicherheit ist zunächst festzustellen, dass nach Art. 4 Abs. 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 135).

75. Die Bedeutung des Ziels, die nationale Sicherheit zu wahren, übersteigt im Licht von Art. 4 Abs. 2 EUV die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele, insbesondere der Ziele, die Kriminalität im Allgemeinen, auch schwere Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen. Bedrohungen wie die in der vorstehenden Randnummer genannten unterscheiden sich nämlich aufgrund ihrer Art und ihrer besonderen Schwere von der allgemeinen Gefahr des Auftretens selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 Abs. 1 der Charta ist das Ziel, die nationale Sicherheit zu wahren, daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, Rn. 136).

76. Um dem in Rn. 67 des vorliegenden Urteils angesprochenen Erfordernis der Verhältnismäßigkeit, wonach Ausnahmen vom Schutz personenbezogener Daten und dessen Beschränkungen nicht über das absolut Notwendige hinausgehen dürfen, zu genügen, muss eine nationale Regelung, die mit einem Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte verbunden ist, jedoch den Anforderungen entsprechen, die sich aus der in den Rn. 65, 67 und 68 des vorliegenden Urteils angeführten Rechtsprechung ergeben.

77. Eine solche Regelung darf sich insbesondere hinsichtlich des Zugangs einer Behörde zu personenbezogenen Daten nicht darauf beschränken, dass der behördliche Zugang zu den Daten dem mit der Regelung verfolgten Zweck zu entsprechen hat, sondern muss auch die materiellen und prozeduralen Voraussetzungen für die Verwendung der Daten vorsehen (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 192 und die dort angeführte Rechtsprechung).

78. Infolgedessen, und weil ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten ohne jeden - auch nur mittelbaren - Zusammenhang mit dem verfolgten Ziel nicht als auf das absolut Notwendige beschränkt angesehen werden kann, muss sich eine nationale Regelung des Zugangs zu Verkehrs- und Standortdaten bei der Festlegung der Umstände und Voraussetzungen, unter denen den zuständigen nationalen Behörden Zugang zu den fraglichen Daten zu gewähren ist, auf objektive Kriterien stützen (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 119 und die dort angeführte Rechtsprechung).

79. Diese Anforderungen gelten erst recht für eine Rechtsvorschrift wie die im Ausgangsverfahren in Rede stehende, auf deren Grundlage die zuständige nationale Behörde den Betreibern elektronischer Kommunikationsdienste vorschreiben kann, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen. Eine solche Übermittlung hat nämlich zur Folge, dass diese Daten den Behörden zur Verfügung gestellt werden (vgl. entsprechend Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 212).

80. Da die Verkehrs- und Standortdaten allgemein und unterschiedslos übermittelt werden, betrifft ihre Übermittlung pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen. Sie gilt somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Wahrung der nationalen Sicherheit stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Übermittlung vorgesehen ist, und einer Bedrohung der nationalen Sicherheit voraus (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights Ireland u. a.*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 57 und 58, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 105). Angesichts dessen, dass die Übermittlung solcher Daten an die Behörden nach den in Rn. 79 des vorliegenden Urteils getroffenen Feststellungen einem Zugang gleichkommt, ist davon auszugehen, dass eine Regelung, die eine allgemeine und unterschiedslose Übermittlung der Daten an die Behörden gestattet, einen allgemeinen Zugang impliziert.

81. Daraus folgt, dass eine nationale Regelung, die den Betreibern elektronischer Kommunikationsdienste vorschreibt, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen, die Grenzen des absolut Notwendigen überschreitet und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden kann, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 verlangt.

82. Nach alledem ist auf die zweite Frage zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta und ihres Art. 52 Abs. 1 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« 2. Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung ist im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union und ihres Art. 52 Abs. 1 dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die es einer staatlichen Stelle gestattet, zur Wahrung der nationalen Sicherheit den Betreibern elektronischer Kommunikationsdienste vorzuschreiben, den Sicherheits- und Nachrichtendiensten allgemein und unterschiedslos Verkehrs- und Standortdaten zu übermitteln ».

B.14. Mit ihrem Urteil *La Quadrature du Net und andere* (C-511/18, C-512/18 und C-520/18) vom 6. Oktober 2020 hat die Große Kammer des Gerichtshofes der Europäischen Union die ersten zwei vom Gerichtshof mit seinem Entscheid Nr. 96/2018 gestellten Fragen wie folgt beantwortet:

« Zur ersten Frage in den Rechtssachen C-511/18 und C-512/18 sowie zur ersten und zur zweiten Frage in der Rechtssache C-520/18

81. Mit der ersten Frage in den Rechtssachen C-511/18 und C-512/18 sowie der ersten und der zweiten Frage in der Rechtssache C-520/18, die zusammen zu prüfen sind, möchten die vorlegenden Gerichte wissen, ob Art. 15 Abs. 1 der Richtlinie 2002/58 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die die Betreiber elektronischer Kommunikationsdienste zu den in Art. 15 Abs. 1 genannten Zwecken zur allgemeinen und unterschiedslosen Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet.

[...]

Zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58

105. Einleitend ist darauf hinzuweisen, dass nach ständiger Rechtsprechung bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut zu berücksichtigen ist, sondern auch ihr Kontext und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, und insbesondere deren Entstehungsgeschichte (vgl. in diesem Sinne Urteil vom 17. April 2018, *Egenberger*, C-414/16, EU: C: 2018: 257, Rn. 44).

106. Die Richtlinie 2002/58 soll, wie sich u. a. aus ihren Erwägungsgründen 6 und 7 ergibt, die Nutzer elektronischer Kommunikationsdienste vor den Risiken für ihre personenbezogenen Daten und ihre Privatsphäre schützen, die sich aus den neuen Technologien und vor allem den zunehmenden Fähigkeiten zur automatisierten Speicherung und Verarbeitung von Daten ergeben. Insbesondere soll mit der Richtlinie nach ihrem zweiten Erwägungsgrund gewährleistet werden, dass die in den Art. 7 und 8 der Charta niedergelegten Rechte uneingeschränkt geachtet werden. Insoweit ergibt sich aus der Begründung des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM [2000] 385 endg.), aus dem die Richtlinie 2002/58 hervorgegangen ist, dass der Unionsgesetzgeber sicherstellen wollte, ' dass für alle elektronischen Kommunikationsdienste unabhängig von der zugrunde liegenden Technologie weiterhin ein hochgradiger Schutz personenbezogener Daten und der Privatsphäre gewährleistet bleibt '.

107. Zu diesem Zweck wird in Art. 5 Abs. 1 der Richtlinie 2002/58 der Grundsatz der Vertraulichkeit sowohl elektronischer Nachrichten als auch der damit verbundenen Verkehrsdaten aufgestellt, der u. a. das grundsätzliche Verbot für jede andere Person als die Nutzer, ohne deren Einwilligung solche Nachrichten und Daten auf Vorrat zu speichern, impliziert.

108. Insbesondere ergibt sich hinsichtlich der Verarbeitung und Speicherung von Verkehrsdaten durch die Betreiber elektronischer Kommunikationsdienste aus Art. 6 sowie den Erwägungsgründen 22 und 26 der Richtlinie 2002/58, dass eine solche Verarbeitung nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums zulässig ist. Danach sind die verarbeiteten und gespeicherten Daten zu löschen oder zu anonymisieren. Andere Standortdaten als Verkehrsdaten dürfen nach Art. 9 Abs. 1 der Richtlinie nur unter bestimmten Voraussetzungen und nur dann verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben (Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 86 und die dort angeführte Rechtsprechung).

109. Durch den Erlass dieser Richtlinie hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der Charta verankerten Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt.

110. Art. 15 Abs. 1 der Richtlinie 2002/58 gestattet es den Mitgliedstaaten jedoch, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten sowie den entsprechenden, u. a. in den Art. 6 und 9 der Richtlinie genannten Pflichten zu schaffen, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten u. a. durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit aufbewahrt werden.

111. Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 der Richtlinie 2002/58 vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 89 und 104).

112. Hinsichtlich der Zwecke, die eine Beschränkung der insbesondere in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten rechtfertigen können, hat der Gerichtshof bereits entschieden, dass die Aufzählung der in Art. 15 Abs. 1 Satz 1 der Richtlinie genannten Zwecke abschließend ist, so dass eine aufgrund dieser Bestimmung erlassene Rechtsvorschrift tatsächlich strikt einem von ihnen dienen muss (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, Rn. 52 und die dort angeführte Rechtsprechung).

113. Außerdem geht aus Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58 hervor, dass die Mitgliedstaaten Rechtsvorschriften, die die Tragweite der Rechte und Pflichten gemäß den Art. 5, 6 und 9 dieser Richtlinie beschränken sollen, nur unter Beachtung der allgemeinen Grundsätze des Unionsrechts, zu denen der Grundsatz der Verhältnismäßigkeit gehört, und der durch die Charta garantierten Grundrechte erlassen dürfen. Hierzu hat der Gerichtshof bereits entschieden, dass die den Betreibern elektronischer Kommunikationsdienste durch eine nationale Regelung auferlegte Pflicht, Verkehrsdaten auf Vorrat zu speichern, um sie gegebenenfalls den zuständigen nationalen Behörden zugänglich zu machen, Fragen aufwirft, die nicht nur die Einhaltung der die Achtung des Privatlebens und den Schutz personenbezogener Daten garantierenden Art. 7 und 8 der Charta betreffen, sondern auch der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 25 und 70, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 91 und 92 sowie die dort angeführte Rechtsprechung).

114. Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 muss somit die Bedeutung sowohl des in Art. 7 der Charta gewährleisteten Rechts auf Achtung des Privatlebens als auch des in Art. 8 der Charta gewährleisteten Rechts auf den Schutz personenbezogener Daten, wie sie sich aus der Rechtsprechung des Gerichtshofs ergibt, berücksichtigt werden sowie das in Art. 11 der Charta gewährleistete Recht auf freie Meinungsäußerung, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Union nach Art. 2 EUV gründet (vgl. in diesem Sinne Urteile vom 6. März 2001, *Connolly/Kommission*, C-274/99 P, EU: C: 2001: 127, Rn. 39, und vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 93 und die dort angeführte Rechtsprechung).

115. Insoweit ist darauf hinzuweisen, dass die Speicherung der Verkehrs- und Standortdaten als solche zum einen eine Abweichung von dem nach Art. 5 Abs. 1 der Richtlinie 2002/58 für alle anderen Personen als die Nutzer geltenden Verbot der Speicherung dieser Daten darstellt und zum anderen einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die in den Art. 7 und 8 der Charta verankert sind; dabei spielt es keine Rolle, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben und ob die Betroffenen durch diesen Eingriff Nachteile erlitten haben (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung; vgl. entsprechend, in Bezug auf Art. 8 der EMRK, EGMR, 30. Januar 2020, *Breyer gegen Deutschland*, CE: ECHR: 2020: 0130JUD005000112, § 81).

116. Irrelevant ist auch, ob die gespeicherten Daten in der Folge verwendet werden (vgl. entsprechend, in Bezug auf Art. 8 der EMRK, EGMR, 16. Februar 2000, *Amann gegen Schweiz*, CE: ECHR: 2000: 0216JUD002779895, § 69, sowie 13. Februar 2020, *Trjakovski und Chipovski gegen Nordmazedonien*, CE: ECHR: 2020: 0213JUD005320513, § 51), da der Zugriff auf solche Daten, unabhängig von ihrer späteren Verwendung, einen gesonderten Eingriff in die in der vorstehenden Randnummer genannten Grundrechte darstellt (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 124 und 126).

117. Dieser Schluss erscheint umso gerechtfertigter, als die Verkehrs- und Standortdaten Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten können, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand, wobei solche Daten im Übrigen im Unionsrecht besonderen Schutz genießen. Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren. Diese Daten ermöglichen insbesondere die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 27, und vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 99).

118. Daher kann die Vorratsspeicherung von Verkehrs- und Standortdaten zu polizeilichen Zwecken zum einen für sich genommen das in Art. 7 der Charta verankerte Recht auf Achtung der Kommunikation beeinträchtigen und die Nutzer elektronischer Kommunikationsmittel von der Ausübung ihrer durch Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung abhalten (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 28, und vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 101). Solche abschreckenden Wirkungen können in besonderem Maß Personen treffen, deren Kommunikationen nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen, sowie Whistleblower, deren Aktivitäten durch die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (*ABl.* 2019, L 305, S. 17), geschützt werden. Außerdem sind diese Wirkungen umso stärker, je größer die Menge und die Vielfalt der auf Vorrat gespeicherten Daten sind.

119. Zum anderen birgt die bloße Vorratsspeicherung durch die Betreiber elektronischer Kommunikationsdienste angesichts der großen Menge von Verkehrs- und Standortdaten, die durch eine Maßnahme allgemeiner und unterschiedsloser Vorratsspeicherung kontinuierlich gespeichert werden können, sowie des sensiblen Charakters der Informationen, die diese Daten liefern können, Gefahren des Missbrauchs und des rechtswidrigen Zugangs.

120. In Art. 15 Abs. 1 der Richtlinie 2002/58, der es den Mitgliedstaaten gestattet, die in Rn. 110 des vorliegenden Urteils angesprochenen Ausnahmen vorzusehen, kommt allerdings zum Ausdruck, dass die in den Art. 7, 8 und 11 der Charta verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen werden müssen (vgl. in diesem Sinne Urteil vom 16. Juli 2020, *Facebook Ireland und Schrems*, C-311/18, EU: C: 2020: 559, Rn. 172 und die dort angeführte Rechtsprechung).

121. Nach Art. 52 Abs. 1 der Charta sind nämlich Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

122. Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta muss somit auch berücksichtigt werden, welche Bedeutung den in den Art. 3, 4, 6 und 7 der Charta verankerten Rechten und den Zielen des Schutzes der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität als Beitrag zum Schutz der Rechte und Freiheiten anderer zukommt.

123. Insoweit ist in Art. 6 der Charta, auf den der Conseil d'État (Staatsrat) und der Verfassungsgerichtshof Bezug nehmen, das Recht jedes Menschen nicht nur auf Freiheit, sondern auch auf Sicherheit verankert, und er garantiert Rechte, die den durch Art. 5 der EMRK garantierten Rechten entsprechen (vgl. in diesem Sinne Urteile vom 15. Februar 2016, *N.*, C-601/15 PPU, EU: C: 2016: 84, Rn. 47, vom 28. Juli 2016, *JZ*, C-294/16 PPU, EU: C: 2016: 610, Rn. 48, und vom 19. September 2019, *Rayonna prokuratura Lom*, C-467/18, EU: C: 2019: 765, Rn. 42 und die dort angeführte Rechtsprechung).

124. Ferner ist darauf hinzuweisen, dass mit Art. 52 Abs. 3 der Charta die notwendige Kohärenz zwischen den in der Charta enthaltenen Rechten und den entsprechenden durch die EMRK garantierten Rechten gewährleistet werden soll, ohne dass dadurch die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt wird. Bei der Auslegung der Charta sind somit die entsprechenden Rechte der EMRK als Mindestschutzstandard zu berücksichtigen (vgl. in diesem Sinne Urteile vom 12. Februar 2019, *TC*, C-492/18 PPU, EU: C: 2019: 108, Rn. 57, und vom 21. Mai 2019, *Kommission/Ungarn* [Nießbrauchsrechte an landwirtschaftlichen Flächen], C-235/17, EU: C: 2019: 432, Rn. 72 und die dort angeführte Rechtsprechung).

125. Art. 5 der EMRK, in dem das Recht auf Freiheit und das Recht auf Sicherheit verankert sind, soll nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte den Einzelnen vor jedem willkürlichen oder ungerechtfertigten Freiheitsentzug schützen (vgl. in diesem Sinne EGMR, 18. März 2008, *Ladent gegen Polen*, CE: ECHR: 2008: 0318JUD001103603, § § 45 und 46, 29. März 2010, *Medvedyev und andere gegen Frankreich*, CE: ECHR: 2010: 0329JUD000339403, § § 76 und 77, sowie 13. Dezember 2012, *El-Masri gegen ' The former Yugoslav Republic of Macedonia '*, CE: ECHR: 2012: 1213JUD003963009, § 239). Da diese Bestimmung einen Freiheitsentzug durch eine staatliche Stelle betrifft, kann Art. 6 der Charta jedoch nicht dahin ausgelegt werden, dass er die staatlichen Stellen verpflichtet, spezifische Maßnahmen zur Ahndung bestimmter Straftaten zu erlassen.

126. In Bezug insbesondere auf die vom Verfassungsgerichtshof angesprochene wirksame Bekämpfung von Straftaten, deren Opfer u. a. Minderjährige und andere schutzbedürftige Personen sind, ist hingegen hervorzuheben, dass sich aus Art. 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz des Privat- und Familienlebens ergeben können (vgl. in diesem Sinne Urteil vom 18. Juni 2020, *Kommission/Ungarn* [Transparenz von Vereinigungen], C-78/18, EU: C: 2020: 476, Rn. 123 und die dort angeführte Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte). Solche Verpflichtungen können sich aus Art. 7 auch in Bezug auf den Schutz der Wohnung und der Kommunikation sowie aus den Art. 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben.

127. Angesichts dieser verschiedenen positiven Verpflichtungen müssen die verschiedenen betroffenen Interessen und Rechte miteinander in Einklang gebracht werden.

128. Der Europäische Gerichtshof für Menschenrechte hat nämlich entschieden, dass die den Art. 3 und 8 der EMRK zu entnehmenden positiven Verpflichtungen, denen die Garantien in den Art. 4 und 7 der Charta entsprechen, u. a. bedeuten, dass materielle und prozedurale Vorschriften zu erlassen sowie praktische Maßnahmen zu treffen sind, die eine wirksame Bekämpfung von Straftaten gegen Personen mittels effektiver Ermittlungen und Verfolgung gestatten. Diese Verpflichtung ist umso wichtiger, wenn das körperliche und geistige Wohlergehen eines Kindes bedroht ist. Die von den zuständigen Behörden zu treffenden Maßnahmen müssen aber den Rechtsschutzmöglichkeiten und übrigen Garantien, die geeignet sind, den Umfang der strafrechtlichen Ermittlungsbefugnisse zu begrenzen, sowie den sonstigen Freiheiten und Rechten umfassend Rechnung tragen. Insbesondere ist ein rechtlicher Rahmen zu schaffen, der es erlaubt, die verschiedenen zu schützenden Interessen und Rechte miteinander in Einklang zu bringen (EGMR, 28. Oktober 1998, *Osman gegen Vereinigtes Königreich*, CE: ECHR: 1998: 1028JUD002345294, § § 115 und 116, 4. März 2004, *M.C. gegen Bulgarien*, CE: ECHR: 2003: 1204JUD003927298, § 151, 24. Juni 2004, *Von Hannover gegen Deutschland*, CE: ECHR: 2004: 0624JUD005932000, § § 57 und 58, sowie 2. Dezember 2008, *K.U. gegen Finnland*, CE: ECHR: 2008: 1202JUD 000287202, § § 46, 48 und 49).

129. In Bezug auf die Beachtung des Grundsatzes der Verhältnismäßigkeit sieht Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 vor, dass die Mitgliedstaaten eine Vorschrift erlassen können, die vom 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 der Richtlinie wird klargestellt, dass eine derartige Maßnahme in einem ' strikt ' angemessenen Verhältnis zum intendierten Zweck stehen muss.

130. Insoweit ist darauf hinzuweisen, dass der Schutz des Grundrechts auf Achtung des Privatlebens nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. Außerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen wird (vgl. in diesem Sinne Urteile vom 16. Dezember 2008, *Satakunnan Markkinapörssi und Satamedia*, C-73/07, EU: C: 2008: 727, Rn. 56, vom 9. November 2010, *Volker und Markus Schecke und Eifert*, C-92/09 und C-93/09, EU: C: 2010: 662, Rn. 76, 77 und 86, sowie vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 52; Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 140).

131. Insbesondere geht aus der Rechtsprechung des Gerichtshofs hervor, dass die Möglichkeit für die Mitgliedstaaten, eine Beschränkung der u. a. in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen Rechte und Pflichten zu rechtfertigen, zu beurteilen ist, indem die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, Rn. 55 und die dort angeführte Rechtsprechung).

132. Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss eine Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz dieser Daten vor Missbrauchsrisiken ermöglichen. Die Regelung muss nach nationalem Recht bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisiert verarbeitet werden, vor allem wenn eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. Diese Erwägungen gelten in besonderem Maß, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 54 und 55, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 117; Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 141).

133. Eine Regelung, die eine Vorratsspeicherung personenbezogener Daten vorsieht, muss daher stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 191 und die dort angeführte Rechtsprechung, sowie Urteil vom 3. Oktober 2019, *A u. a.*, C-70/18, EU: C: 2019: 823, Rn. 63).

- Zu den Rechtsvorschriften, die zum Schutz der nationalen Sicherheit eine präventive Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen

134. Das von den vorlegenden Gerichten und den Regierungen, die Erklärungen abgegeben haben, angesprochene Ziel des Schutzes der nationalen Sicherheit ist vom Gerichtshof in seinen Urteilen zur Auslegung der Richtlinie 2002/58 noch nicht spezifisch geprüft worden.

135. Insoweit ist zunächst festzustellen, dass nach Art. 4 Abs. 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten.

136. Die Bedeutung des Ziels des Schutzes der nationalen Sicherheit übersteigt im Licht von Art. 4 Abs. 2 EUV die der übrigen von Art. 15 Abs. 1 der Richtlinie 2002/58 erfassten Ziele, insbesondere der Ziele, die Kriminalität im Allgemeinen, auch schwere Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen. Bedrohungen wie die in der vorstehenden Randnummer genannten unterscheiden sich nämlich aufgrund ihrer Art und ihrer besonderen Schwere von der allgemeinen Gefahr des Auftretens selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit. Vorbehaltlich der Erfüllung der übrigen Anforderungen von Art. 52 Abs. 1 der Charta ist das Ziel des Schutzes der nationalen Sicherheit daher geeignet, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten.

137. Somit steht Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta in Situationen wie den in den Rn. 135 und 136 des vorliegenden Urteils beschriebenen einer Rechtsvorschrift, mit der den zuständigen Behörden gestattet wird, den Betreibern elektronischer Kommunikationsdienste aufzugeben, die Verkehrs- und Standortdaten aller Nutzer elektronischer Kommunikationsmittel für begrenzte Zeit zu speichern, grundsätzlich nicht entgegen, sofern hinreichend konkrete Umstände die Annahme zulassen, dass sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit im Sinne der Rn. 135 und 136 des vorliegenden Urteils gegenübersieht. Auch wenn eine solche Maßnahme unterschiedslos alle Nutzer elektronischer Kommunikationsmittel erfasst, ohne dass *prima facie* ein Zusammenhang im Sinne der in Rn. 133 des vorliegenden Urteils angeführten Rechtsprechung zwischen ihnen und einer Bedrohung der nationalen Sicherheit dieses Mitgliedstaats zu bestehen scheint, ist gleichwohl davon auszugehen, dass das Vorliegen einer derartigen Bedrohung als solches geeignet ist, diesen Zusammenhang herzustellen.

138. Die Anordnung, die Daten aller Nutzer elektronischer Kommunikationsmittel präventiv auf Vorrat zu speichern, muss jedoch in zeitlicher Hinsicht auf das absolut Notwendige beschränkt werden. Zwar kann nicht ausgeschlossen werden, dass die an die Betreiber elektronischer Kommunikationsdienste gerichtete Anordnung, Daten auf Vorrat zu speichern, wegen des Fortbestands einer solchen Bedrohung verlängert werden kann, doch darf die Laufzeit jeder Anordnung einen absehbaren Zeitraum nicht überschreiten. Überdies muss eine solche Vorratsdatenspeicherung Beschränkungen unterliegen und mit strengen Garantien verbunden sein, die einen wirksamen Schutz der personenbezogenen Daten der Betroffenen vor Missbrauchsrisiken ermöglichen. Die Speicherung darf somit keinen systematischen Charakter haben.

139. Angesichts der Schwere des aus einer solchen allgemeinen und unterschiedslosen Speicherung resultierenden Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, muss gewährleistet sein, dass darauf tatsächlich nur in Situationen wie den in den Rn. 135 und 136 des vorliegenden Urteils angesprochenen zurückgegriffen wird, in denen eine ernste Bedrohung für die nationale Sicherheit besteht. Dabei ist es unabdingbar, dass eine an die Betreiber elektronischer Kommunikationsdienste gerichtete Anordnung einer solchen Vorratsdatenspeicherung Gegenstand einer wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist, sein kann, mit der das Vorliegen einer dieser Situationen sowie die Beachtung der vorzusehenden Bedingungen und Garantien geprüft werden.

- Zu den Rechtsvorschriften, die zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine präventive Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen

140. Was das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten anbelangt, sind im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit geeignet, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, zu rechtfertigen. Daher können nur Eingriffe in die genannten Grundrechte, die nicht schwer sind, durch das Ziel der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein (vgl. in diesem Sinne Urteile vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 102, und vom 2. Oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, Rn. 56 und 57; Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU: C: 2017: 592, Rn. 149).

141. Eine nationale Regelung, die zur Bekämpfung schwerer Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, überschreitet 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 von Art. 52 Abs. 1 der Charta verlangt (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 107).

142. Angesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, ist deren Vertraulichkeit nämlich von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens. In Anbetracht zum einen der in Rn. 118 des vorliegenden Urteils angesprochenen abschreckenden Wirkungen, die die Speicherung dieser Daten auf die Ausübung der in den Art. 7 und 11 der Charta verankerten Grundrechte haben kann, und zum anderen der Schwere des mit ihr verbundenen Eingriffs muss eine solche Speicherung in einer demokratischen Gesellschaft, wie es das durch die Richtlinie 2002/58 geschaffene System vorsieht, die Ausnahme und nicht die Regel sein, und solche Daten dürfen nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein. Dies gilt auch in Anbetracht der Ziele der Bekämpfung schwerer Kriminalität und der Verhütung ernster Bedrohungen der öffentlichen Sicherheit sowie der Bedeutung, die ihnen beizumessen ist.

143. Außerdem hat der Gerichtshof hervorgehoben, dass eine Regelung, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, die elektronischen Kommunikationen fast der gesamten Bevölkerung erfasst, ohne jede Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels. Eine solche Regelung betrifft entgegen dem in Rn. 133 des vorliegenden Urteils angesprochenen Erfordernis 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 somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Bekämpfung schwerer Straftaten stehen könnte, und setzt insbesondere keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit voraus (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 57 und 58, sowie vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 105).

144. Insbesondere beschränkt eine solche Regelung, wie der Gerichtshof bereits entschieden hat, 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 schwerer Kriminalität beitragen könnten (vgl. in diesem Sinne Urteile vom 8. April 2014, *Digital Rights*, C-293/12 und C-594/12, EU: C: 2014: 238, Rn. 59, und vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 106).

145. Selbst die positiven Verpflichtungen, die sich, je nach Fall, für die Mitgliedstaaten aus den Art. 3, 4 und 7 der Charta ergeben können und, wie in den Rn. 126 und 128 des vorliegenden Urteils ausgeführt worden ist, die Schaffung von Regeln für eine wirksame Bekämpfung von Straftaten betreffen, können aber keine so schwerwiegenden Eingriffe rechtfertigen, wie sie mit einer Regelung, die eine Speicherung von Verkehrs- und Standortdaten vorsieht, für die in den Art. 7 und 8 der Charta verankerten Grundrechte fast der gesamten Bevölkerung verbunden sind, ohne dass die Daten der Betroffenen einen zumindest mittelbaren Zusammenhang mit dem verfolgten Ziel aufweisen.

146. Hingegen können nach den Ausführungen in den Rn. 142 bis 144 des vorliegenden Urteils und angesichts dessen, dass die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, die Ziele der Bekämpfung schwerer Kriminalität, der Verhütung schwerer Beeinträchtigungen der öffentlichen Sicherheit und erst recht des Schutzes der nationalen Sicherheit in Anbetracht ihrer Bedeutung im Hinblick auf die in der vorstehenden Randnummer angesprochenen positiven Verpflichtungen, auf die insbesondere der Verfassungsgerichtshof abgestellt hat, den mit einer gezielten Vorratsspeicherung von Verkehrs- und Standortdaten verbundenen besonders schwerwiegenden Eingriff rechtfertigen.

147. Wie der Gerichtshof bereits entschieden hat, untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta es einem Mitgliedstaat somit nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sowie zum Schutz der nationalen Sicherheit präventiv eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern ihre Speicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 108).

148. Die erforderliche Begrenzung einer solchen Vorratsdatenspeicherung kann insbesondere anhand der Kategorien betroffener Personen vorgenommen werden, da Art. 15 Abs. 1 der Richtlinie 2002/58 einer auf objektiven Kriterien beruhenden Regelung nicht entgegensteht, mit der Personen erfasst werden können, deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit oder eine Gefahr für die nationale Sicherheit zu verhüten (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 111).

149. Insoweit ist hinzuzufügen, dass zu den erfassten Personen insbesondere diejenigen gehören können, die zuvor im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden.

150. Die Begrenzung einer Maßnahme zur Vorratsspeicherung von Verkehrs- und Standortdaten kann auch auf ein geografisches Kriterium gestützt werden, wenn die zuständigen nationalen Behörden aufgrund objektiver und nicht diskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation besteht (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 111). Dabei kann es sich insbesondere um Orte handeln, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, um Orte, an denen die Gefahr, dass schwere Straftaten begangen werden, besonders hoch ist, wie Orte oder Infrastrukturen, die regelmäßig von einer sehr hohen Zahl von Personen aufgesucht werden, oder um strategische Orte wie Flughäfen, Bahnhöfe oder Mautstellen.

151. Um sicherzustellen, dass der Eingriff, mit dem die in den Rn. 147 bis 150 des vorliegenden Urteils beschriebenen Maßnahmen gezielter Speicherung verbunden sind, mit dem Grundsatz der Verhältnismäßigkeit im Einklang steht, darf ihre Dauer das im Hinblick auf das verfolgte Ziel sowie die sie rechtfertigenden Umstände absolut Notwendige nicht überschreiten, unbeschadet einer etwaigen Verlängerung wegen des fortbestehenden Erfordernisses einer solchen Speicherung.

- Zu den Rechtsvorschriften, die zur Bekämpfung der Kriminalität und zum Schutz der öffentlichen Sicherheit eine präventive Vorratsspeicherung von IP-Adressen und die Identität betreffenden Daten vorsehen

152. IP-Adressen gehören zwar zu den Verkehrsdaten, werden aber ohne Anknüpfung an eine bestimmte Kommunikation erzeugt und dienen in erster Linie dazu, über die Betreiber elektronischer Kommunikationsdienste die natürliche Person zu ermitteln, der ein Endgerät gehört, von dem aus eine Kommunikation über das Internet stattfindet. Sofern im Bereich von E-Mail und Internettelefonie nur die IP-Adressen der Kommunikationsquelle gespeichert werden und nicht die des Adressaten einer Kommunikation, lässt sich diesen Adressen als solchen keine Information über die Dritten entnehmen, mit denen die Person, von der die Kommunikation ausging, in Kontakt stand. Diese Kategorie von Daten weist daher einen geringeren Sensibilitätsgrad als die übrigen Verkehrsdaten auf.

153. Da die IP-Adressen jedoch insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden können, ermöglichen sie die Erstellung eines detaillierten Profils dieses Nutzers. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP-Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar und können abschreckende Wirkungen wie die in Rn. 118 des vorliegenden Urteils dargelegten entfalten.

154. Um die widerstreitenden Rechte und Interessen miteinander in Einklang zu bringen, wie es die in Rn. 130 des vorliegenden Urteils angeführte Rechtsprechung verlangt, ist aber zu berücksichtigen, dass im Fall einer im Internet begangenen Straftat die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde. Hinzu kommt, dass die Vorratsspeicherung der IP-Adressen durch die Betreiber elektronischer Kommunikationsdienste über die Dauer ihrer Zuweisung hinaus im Prinzip nicht erforderlich erscheint, um eine Rechnung für die fraglichen Dienste zu erstellen, so dass sich die Feststellung im Internet begangener Straftaten, wie mehrere Regierungen in ihren beim Gerichtshof eingereichten Erklärungen angegeben haben, ohne Rückgriff auf eine Rechtsvorschrift nach Art. 15 Abs. 1 der Richtlinie 2002/58 als unmöglich erweisen kann. Dies kann, wie diese Regierungen geltend gemacht haben, u. a. bei besonders schweren Straftaten im Bereich der Kinderpornografie im Sinne von Art. 2 Buchst. c der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (*ABl.* 2011, L 335, S. 1) der Fall sein, etwa wenn Kinderpornografie erworben, verbreitet, weitergegeben oder im Internet bereitgestellt wird.

155. Unter diesen Umständen trifft es zwar zu, dass eine Rechtsvorschrift, die eine Vorratsspeicherung der IP-Adressen aller natürlichen Personen vorsieht, denen ein Endgerät gehört, von dem aus ein Internetzugang möglich ist, Personen erfassen würde, die *prima facie* keinen Zusammenhang mit den verfolgten Zielen im Sinne der in Rn. 133 des vorliegenden Urteils angeführten Rechtsprechung aufweisen, und dass die Internetnutzer nach der Feststellung in Rn. 109 des vorliegenden Urteils aufgrund der Art. 7 und 8 der Charta erwarten dürfen, dass ihre Identität grundsätzlich nicht preisgegeben wird. Gleichwohl verstößt eine Rechtsvorschrift, die eine allgemeine und unterschiedslose Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung vorsieht, grundsätzlich nicht gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen.

156. Angesichts der Schwere des mit dieser Vorratsdatenspeicherung verbundenen Eingriffs in die Grundrechte, die in den Art. 7 und 8 der Charta verankert sind, sind neben dem Schutz der nationalen Sicherheit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Außerdem darf die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten. Schließlich muss eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen.

157. Was schließlich die die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten angeht, ermöglichen sie es für sich genommen weder, das Datum, die Uhrzeit, die Dauer und die Adressaten der Kommunikationen in Erfahrung zu bringen, noch die Orte, an denen sie stattfanden, oder wie häufig dies mit bestimmten Personen innerhalb eines gegebenen Zeitraums geschah, so dass sie, abgesehen von Kontaktdaten wie ihren Adressen, keine Informationen über die konkreten Kommunikationen und infolgedessen über ihr Privatleben liefern. Der mit einer Vorratsspeicherung dieser Daten verbundene Eingriff kann somit grundsätzlich nicht als schwer eingestuft werden (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, Rn. 59 und 60).

158. Daraus ergibt sich im Einklang mit den Ausführungen in Rn. 140 des vorliegenden Urteils, dass Rechtsvorschriften, die auf die Verarbeitung dieser Daten als solcher, insbesondere auf ihre Speicherung und den Zugang zu ihnen zum alleinigen Zweck der Identifizierung des betreffenden Nutzers abzielen, ohne dass die Daten mit Informationen über die erfolgten Kommunikationen in Verbindung gebracht werden können, durch den in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannten Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen gerechtfertigt sein können (vgl. in diesem Sinne Urteil vom 2. Oktober 2018, *Ministerio Fiscal*, C-207/16, EU: C: 2018: 788, Rn. 62).

159. Unter diesen Umständen ist angesichts dessen, dass die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, aus den in den Rn. 131 und 158 des vorliegenden Urteils genannten Gründen davon auszugehen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta, auch wenn es keine Verbindung zwischen der Gesamtheit der Nutzer elektronischer Kommunikationsmittel und den verfolgten Zielen gibt, einer Rechtsvorschrift nicht entgegensteht, die den Betreibern elektronischer Kommunikationsdienste ohne besondere Frist auferlegt, zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten sowie zum Schutz der öffentlichen Sicherheit Daten über die Identität aller Nutzer elektronischer Kommunikationsmittel auf Vorrat zu speichern, ohne dass es sich um schwere Straftaten, Bedrohungen oder Beeinträchtigungen der öffentlichen Sicherheit handeln muss.

- Zu den Rechtsvorschriften, die zur Bekämpfung schwerer Kriminalität eine umgehende Sicherung von Verkehrs- und Standortdaten vorsehen

160. Die von den Betreibern elektronischer Kommunikationsdienste auf der Grundlage der Art. 5, 6 und 9 der Richtlinie 2002/58 oder auf der Grundlage von Rechtsvorschriften der in den Rn. 134 bis 159 des vorliegenden Urteils beschriebenen Art, die gemäß Art. 15 Abs. 1 der Richtlinie erlassen wurden, verarbeiteten und gespeicherten Verkehrs- und Standortdaten müssen grundsätzlich nach Ablauf der gesetzlichen Fristen, innerhalb deren sie gemäß den nationalen Bestimmungen zur Umsetzung der Richtlinie verarbeitet und gespeichert werden müssen, entweder gelöscht oder anonymisiert werden.

161. Während dieser Verarbeitung und Speicherung können jedoch Situationen auftreten, die es erforderlich machen, die betreffenden Daten zur Aufklärung schwerer Straftaten oder von Beeinträchtigungen der nationalen Sicherheit über diese Fristen hinaus zu speichern, und zwar sowohl dann, wenn die Taten oder Beeinträchtigungen bereits festgestellt werden konnten, als auch dann, wenn nach einer objektiven Prüfung aller relevanten Umstände der begründete Verdacht besteht, dass sie vorliegen.

162. Insoweit ist darauf hinzuweisen, dass das von den 27 Mitgliedstaaten unterzeichnete und von 25 von ihnen ratifizierte Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität (Sammlung Europäischer Verträge - Nr. 185), das die Bekämpfung von Straftaten, die mittels Rechnernetzen begangen wurden, erleichtern soll, in Art. 14 vorsieht, dass die Vertragsstaaten für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren bestimmte Maßnahmen hinsichtlich bereits gespeicherter Verkehrsdaten treffen, zu denen die umgehende Sicherung dieser Daten gehört. Dazu heißt es in Art. 16 Abs. 1 des Übereinkommens insbesondere, dass die Vertragsparteien die erforderlichen gesetzgeberischen Maßnahmen treffen, damit ihre zuständigen Behörden die umgehende Sicherung von Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass diese Daten verloren gehen oder verändert werden könnten.

163. In einer Situation wie der in Rn. 161 des vorliegenden Urteils beschriebenen steht es den Mitgliedstaaten angesichts dessen, dass nach den Ausführungen in Rn. 130 des vorliegenden Urteils die widerstreitenden Rechte und Interessen miteinander in Einklang gebracht werden müssen, frei, in Rechtsvorschriften, die sie gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen, vorzusehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben wird, für einen festgelegten Zeitraum die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

164. Da die Zielsetzung einer solchen umgehenden Sicherung nicht mehr den Zielsetzungen entspricht, aufgrund deren die Daten ursprünglich gesammelt und gespeichert wurden, und da nach Art. 8 Abs. 2 der Charta jede Datenverarbeitung für festgelegte Zwecke zu erfolgen hat, müssen die Mitgliedstaaten in ihren Rechtsvorschriften angeben, mit welcher Zielsetzung die umgehende Sicherung der Daten vorgenommen werden kann. Angesichts der Schwere des Eingriffs in die Grundrechte der Art. 7 und 8 der Charta, der mit einer solchen Speicherung verbunden sein kann, sind nur die Bekämpfung schwerer Kriminalität und, *a fortiori*, der Schutz der nationalen Sicherheit geeignet, diesen Eingriff zu rechtfertigen. Um sicherzustellen, dass der mit einer derartigen Maßnahme verbundene Eingriff auf das absolut Notwendige beschränkt bleibt, darf sich die Speicherungspflicht zudem zum einen nur auf Verkehrs- und Standortdaten erstrecken, die zur Aufdeckung der schweren Straftat oder der Beeinträchtigung der nationalen Sicherheit beitragen können. Zum anderen muss die Speicherungsdauer der Daten auf das absolut Notwendige beschränkt bleiben, kann allerdings verlängert werden, wenn die Umstände und das mit der fraglichen Maßnahme verfolgte Ziel es rechtfertigen.

165. Insoweit ist hinzuzufügen, dass sich eine solche umgehende Sicherung nicht auf die Daten der Personen beschränken muss, die konkret im Verdacht stehen, eine Straftat begangen oder die nationale Sicherheit beeinträchtigt zu haben. Unter Beachtung des durch Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta vorgegebenen Rahmens und angesichts der Erwägungen in Rn. 133 des vorliegenden Urteils kann eine solche Maßnahme nach Wahl des Gesetzgebers, unter Einhaltung der Grenzen des absolut Notwendigen, auf die Verkehrs- und Standortdaten anderer als der Personen erstreckt werden, die im Verdacht stehen, eine schwere Straftat oder eine Beeinträchtigung der nationalen Sicherheit geplant oder begangen zu haben, sofern diese Daten auf der Grundlage objektiver und nicht diskriminierender Kriterien zur Aufdeckung einer solchen Straftat oder einer solchen Beeinträchtigung der nationalen Sicherheit beitragen können. Dazu gehören die Daten des Opfers, seines sozialen oder beruflichen Umfelds oder bestimmter geografischer Zonen, etwa der Orte, an denen die fragliche Straftat oder Beeinträchtigung der nationalen Sicherheit begangen oder vorbereitet wurde. Außerdem müssen beim Zugang der zuständigen Behörden zu den gespeicherten Daten die Voraussetzungen eingehalten werden, die sich aus der Rechtsprechung zur Auslegung der Richtlinie 2002/58 ergeben (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU: C: 2016: 970, Rn. 118 bis 121 und die dort angeführte Rechtsprechung).

166. Ferner ist hinzuzufügen, dass - wie sich insbesondere aus den Rn. 115 und 133 des vorliegenden Urteils ergibt - der Zugang zu den von den Betreibern elektronischer Kommunikationsdienste in Anwendung einer gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Rechtsvorschrift gespeicherten Verkehrs- und Standortdaten grundsätzlich nur mit dem dem Gemeinwohl dienenden Ziel gerechtfertigt werden kann, zu dem die Speicherung den Betreibern auferlegt wurde. Daraus folgt insbesondere, dass keinesfalls ein Zugang zu solchen Daten zwecks Verfolgung und Ahndung einer gewöhnlichen Straftat gewährt werden kann, wenn ihre Speicherung mit dem Ziel der Bekämpfung schwerer Kriminalität oder gar dem Schutz der nationalen Sicherheit gerechtfertigt wurde. Dagegen kann, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach seiner Auslegung in Rn. 131 des vorliegenden Urteils, ein Zugang zu Daten, die im Hinblick auf die Bekämpfung schwerer Kriminalität gespeichert wurden, mit dem Ziel des Schutzes der nationalen Sicherheit gerechtfertigt werden, sofern die in der vorstehenden Randnummer genannten materiellen und prozeduralen Voraussetzungen für einen solchen Zugang eingehalten werden.

167. Insoweit steht es den Mitgliedstaaten frei, in ihren Rechtsvorschriften vorzusehen, dass ein Zugang zu Verkehrs- und Standortdaten bei Einhaltung der fraglichen materiellen und prozeduralen Voraussetzungen zur Bekämpfung schwerer Kriminalität oder zum Schutz der nationalen Sicherheit erfolgen kann, wenn diese Daten von einem Betreiber in einer mit den Art. 5, 6 und 9 oder mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Einklang stehenden Weise gespeichert wurden.

168. Nach alledem ist auf die erste Frage in den Rechtssachen C-511/18 und C-512/18 sowie auf die erste und die zweite Frage in der Rechtssache C-520/18 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 Abs. 1 der Richtlinie im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta Rechtsvorschriften nicht entgegen, die

- es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

- es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« 1. Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Dagegen steht Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte Rechtsvorschriften nicht entgegen, die

- es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

- es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

[...] ».

B.15. Aus dem vorerwähnten Urteil des Gerichtshofes in der Rechtssache *La Quadrature du Net und andere* vom 6. Oktober 2020 geht hervor, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen ist, dass er Rechtsvorschriften entgegensteht, die zu den in Artikel 15 Absatz 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, außer in den von dem vorerwähnten Urteil beschriebenen begrenzten Fällen.

Insofern es grundsätzlich und ohne Begrenzung auf diese Fälle eine allgemeine und unterschiedslose Vorratsspeicherung von Identifizierungs-, Zugangs- und Verbindungsdaten sowie der in Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 erwähnten Kommunikationsdaten durch die Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsieht, verstößt das angefochtene Gesetz folglich gegen Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Lichte der vorerwähnten Bestimmungen der Charta der Grundrechte der Europäischen Union und in Verbindung mit den Artikeln 10 und 11 der Verfassung.

B.16.1. Im Tenor des vorerwähnten Urteils in der Rechtssache *La Quadrature du Net und andere* vom 6. Oktober 2020 hat der Gerichtshof der Europäischen Union jedoch präzisiert, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union verschiedenen Arten von Rechtsvorschriften nicht entgegensteht, die darin aufgezählt sind. So sind unter anderem Rechtsvorschriften zulässig, die « zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen » oder auch Rechtsvorschriften, die « zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen ». Diese Rechtsvorschriften müssen « durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen ».

B.16.2. Auf der Grundlage dieser Präzisierungen des Gerichtshofes der Europäischen Union führt der Ministerrat in seinen Ergänzungsschriftsätzen an, dass das angefochtene Gesetz in jedem Fall nicht für nichtig zu erklären sei, insofern es die allgemeine und unterschiedslose Pflicht zur Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, einerseits und der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten andererseits durch die Betreiber und Anbieter von elektronischen Kommunikationsdiensten vorsehe.

Der Ministerrat zieht daraus den Schluss, dass gegebenenfalls nur die Absätze 2 und 3 von Artikel 126 § 3 des Gesetzes vom 13. Juni 2005, die jeweils die Verbindungs- und Standortdaten und die Kommunikationsdaten betreffen, für nichtig zu erklären seien. Er ist der Auffassung, dass Absatz 1 des vorerwähnten Artikels 126 § 3, der sich auf die Identifizierungsdaten bezieht, hingegen nicht für nichtig erklärt werden muss, ebenso wenig wie die anderen Bestimmungen des angefochtenen Gesetzes, da sie die notwendigen Garantien hinsichtlich der Vorratsspeicherung der Daten und des Zugangs zu ihnen enthielten.

B.17. Im vorliegenden Fall ist festzustellen, dass das angefochtene Gesetz im Grundsatz auf einer allgemeinen und unterschiedslosen Vorratsspeicherungspflicht für sämtliche in Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 erwähnten Daten beruht und dass es allgemein, wie in B.3 und B.4 erwähnt, umfassendere Ziele als die Bekämpfung schwerer Kriminalität oder die Gefahr einer schwerwiegenden Beeinträchtigung der öffentlichen Sicherheit verfolgt.

Die Unterscheidung, die in Artikel 126 § 3 des Gesetzes vom 13. Juni 2005 zwischen drei Datenkategorien (nämlich den Identifizierungsdaten, den Zugangs- und Verbindungsdaten sowie den Kommunikationsdaten) vorgenommen wird, wirkt sich nur auf den Anfangszeitpunkt der Dauer der Datenspeicherung von in jedem Fall zwölf Monaten und eventuell auf die Möglichkeiten, auf sie zuzugreifen, für die ermächtigten Stellen aus (siehe Artikel 46*bis* des Strafprozessgesetzbuches und Artikel 126 § 2 des Gesetzes vom 13. Juni 2005). Diese Kategorisierung entspricht außerdem nicht den Unterscheidungen, die vom Gerichtshof der Europäischen Union in seinem Urteil vom 6. Oktober 2020 in Bezug auf die verschiedenen Datenkategorien, die Gegenstand einer allgemeinen und unterschiedslosen Vorratsspeicherungspflicht unter Einhaltung mehrere Bedingungen sein können (nämlich im vorliegenden Fall: die IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, und die Daten, die die Identität der Nutzer elektronischer Kommunikationsmittel betreffen), vorgenommen werden.

B.18. Das Urteil des Gerichtshofes vom 6. Oktober 2020 verpflichtet zu einer Änderung der Perspektive hinsichtlich der Entscheidung des Gesetzgebers: Die Pflicht zur Speicherung von Daten über die elektronische Kommunikation muss die Ausnahme sein und nicht die Regel. Eine Regelung, die eine solche Pflicht vorsieht, muss zudem klaren und präzisen Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme unterliegen und Mindesterfordernisse aufstellen (Randnr. 133). Diese Regelung muss gewährleisten, dass sich der Eingriff auf das absolut Notwendige beschränkt und muss stets « objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen » (Randnrn. 132 und 133).

B.19. Es obliegt dem Gesetzgeber, eine Regelung auszuarbeiten, mit der die auf dem Gebiet des Schutzes personenbezogener Daten geltenden Grundsätze im Lichte der Rechtsprechung des Gerichtshofes der Europäischen Union eingehalten werden, und gegebenenfalls die von diesem angegebenen Präzisierungen in Bezug auf die verschiedenen Arten von Rechtsvorschriften, die als vereinbar mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Lichte der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union betrachtet werden, zu berücksichtigen. Insbesondere obliegt es ebenfalls dem Gesetzgeber, in diesem Kontext die Unterscheidungen vorzunehmen, die zwischen den verschiedenen der Vorratsspeicherung unterliegenden Datenarten notwendig sind, sodass gewährleistet ist, dass sich der Eingriff für jede Datenart auf das absolut Notwendige beschränkt.

B.20. In Anbetracht des Vorstehenden sind die Artikel 2 Buchstabe *b)*, 3 bis 11 und 14 des angefochtenen Gesetzes, die untrennbar miteinander verbunden sind, für nichtig zu erklären.

B.21. Die anderen Klagegründe in den Rechtssachen Nrn. 6599 und 6601 betreffen ebenfalls die allgemeine und unterschiedslose Vorratsspeicherung von Daten über die elektronische Kommunikation und den Zugang zu ihnen. Da sie nicht zu einer weitergehenden Nichtigerklärung führen können, erübrigt sich ihre Prüfung.

In Bezug auf die Aufrechterhaltung der Folgen

B.22. In seinen Gegenerwiderungsschriftsätzen beantragt der Ministerrat äußerst hilfsweise, die Folgen der Bestimmungen, die gegebenenfalls für nichtig erklärt würden, aufrechtzuerhalten, um die Arbeit zur Ermittlung und Verfolgung von Straftaten der Polizei- und Nachrichtendienste nicht zu gefährden.

B.23.1. Artikel 8 Absatz 3 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof bestimmt:

« Wenn der Verfassungsgerichtshof es für notwendig erachtet, gibt er im Wege einer allgemeinen Verfügung die Folgen der für nichtig erklärten Bestimmungen an, die als endgültig zu betrachten sind oder für die von ihm festgelegte Frist vorläufig aufrechterhalten werden ».

B.23.2. Der Gerichtshof muss diesbezüglich die Einschränkungen berücksichtigen, die sich aus dem Recht der Europäischen Union bezüglich der Aufrechterhaltung der Folgen innerstaatlicher Normen, die für nichtig zu erklären sind, weil sie im Widerspruch zu diesem Recht stehen, ergeben (EuGH, Große Kammer, 8. September 2010, C-409/06, *Winner Wetten*, Randnrn. 53-69; EuGH, Große Kammer, 28. Februar 2012, C-41/11, *Inter-Environnement Wallonie und Terre wallonne*, Randnrn. 56-63).

In der Regel kann diese Aufrechterhaltung der Folgen nur unter den Bedingungen geschehen, die durch den Europäischen Gerichtshof in der Antwort auf eine Vorabentscheidungsfrage festgelegt werden.

B.24.1. In Beantwortung der dritten vom Gerichtshof gestellten Vorabentscheidungsfrage zu einer etwaigen Aufrechterhaltung der Folgen des angefochtenen Gesetzes hat der Gerichtshof der Europäischen Union geurteilt:

« *Zur dritten Frage in der Rechtssache C-520/18*

213. Mit der dritten Frage in der Rechtssache C-520/18 möchte das vorlegende Gericht wissen, ob ein nationales Gericht eine Bestimmung seines nationalen Rechts anwenden darf, aufgrund deren es, wenn es im Einklang mit seinem nationalen Recht eine nationale Rechtsvorschrift, mit der den Betreibern elektronischer Kommunikationsdienste u. a. zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta für rechtswidrig erklärt, zu einer Beschränkung der zeitlichen Wirkungen dieser Erklärung befugt ist.

214. Der Grundsatz des Vorrangs des Unionsrechts besagt, dass das Unionsrecht dem Recht der Mitgliedstaaten vorgeht. Dieser Grundsatz verpflichtet daher alle mitgliedstaatlichen Stellen, den verschiedenen unionsrechtlichen Vorschriften volle Wirksamkeit zu verschaffen, wobei das Recht der Mitgliedstaaten die diesen verschiedenen Vorschriften zuerkannte Wirkung in ihrem Hoheitsgebiet nicht beeinträchtigen darf (Urteile vom 15. Juli 1964, Costa, 6/64, EU: C: 1964: 66, S. 1270 und 1271, sowie vom 19. November 2019, *A. K. u. a.* [Unabhängigkeit der Disziplinarkammer des Obersten Gerichts], C-585/18, C-624/18 und C-625/18, EU: C: 2019: 982, Rn. 157 und 158 sowie die dort angeführte Rechtsprechung).

215. Nach dem Grundsatz des Vorrangs des Unionsrechts ist ein nationales Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat und eine nationale Regelung nicht im Einklang mit den Anforderungen des Unionsrechts auslegen kann, verpflichtet, für die volle Wirksamkeit dieser Bestimmungen Sorge zu tragen, indem es erforderlichenfalls jede - auch spätere - entgegenstehende Bestimmung des nationalen Rechts aus eigener Entscheidungsbefugnis unangewendet lässt, ohne dass es ihre vorherige Beseitigung auf gesetzgeberischem Weg oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste (Urteile vom 22. Juni 2010, *Melki und Abdeli*, C-188/10 und C-189/10, EU: C: 2010: 363, Rn. 43 und die dort angeführte Rechtsprechung, vom 24. Juni 2019, *Popławski*, C-573/17, EU: C: 2019: 530, Rn. 58, und vom 19. November 2019, *A. K. u. a.* [Unabhängigkeit der Disziplinarkammer des Obersten Gerichts], C-585/18, C-624/18 und C-625/18, EU: C: 2019: 982, Rn. 160).

216. Nur der Gerichtshof kann in Ausnahmefällen und aus zwingenden Erwägungen der Rechtssicherheit eine vorübergehende Aussetzung der Verdrängungswirkung herbeiführen, die eine unionsrechtliche Vorschrift gegenüber mit ihr unvereinbarem nationalem Recht ausübt. Eine solche zeitliche Beschränkung der Wirkungen einer Auslegung des Unionsrechts durch den Gerichtshof kann nur in dem Urteil vorgenommen werden, in dem über die begehrte Auslegung entschieden wird (vgl. in diesem Sinne Urteile vom 23. Oktober 2012, *Nelson u. a.*, C-581/10 und C-629/10, EU: C: 2012: 657, Rn. 89 und 91, vom 23. April 2020, *Herst*, C-401/18, EU: C: 2020: 295, Rn. 56 und 57, sowie vom 25. Juni 2020, *A u. a.* [Windkraftanlagen in Aalter und Nevele], C-24/19, EU: C: 2020: 503, Rn. 84 und die dort angeführte Rechtsprechung).

217. Der Vorrang und die einheitliche Anwendung des Unionsrechts würden beeinträchtigt, wenn nationale Gerichte befugt wären, nationalen Bestimmungen, sei es auch nur vorübergehend, Vorrang vor dem Unionsrecht einzuräumen, gegen das sie verstoßen (vgl. in diesem Sinne Urteil vom 29. Juli 2019, *Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU: C: 2019: 622, Rn. 177 und die dort angeführte Rechtsprechung).

218. Der Gerichtshof hat jedoch in einer Rechtssache, in der es um die Rechtmäßigkeit von Maßnahmen ging, die unter Verstoß gegen die durch das Unionsrecht auferlegte Pflicht zur Durchführung einer vorherigen Prüfung der Umweltverträglichkeit eines Projekts und seiner Verträglichkeit mit einem geschützten Gebiet ergangen waren, entschieden, dass ein nationales Gericht, wenn das innerstaatliche Recht es gestattet, die Wirkungen solcher Maßnahmen ausnahmsweise aufrechterhalten kann, sofern dies durch zwingende Erwägungen gerechtfertigt ist, die im Zusammenhang mit der Notwendigkeit stehen, die tatsächliche und schwerwiegende Gefahr einer Unterbrechung der Stromversorgung im betreffenden Mitgliedstaat abzuwenden, der nicht mit anderen Mitteln und Alternativen, insbesondere im Rahmen des Binnenmarkts, entgegengetreten werden kann. Ihre Aufrechterhaltung darf aber nur für den Zeitraum gelten, der absolut notwendig ist, um die Rechtswidrigkeit zu beseitigen (vgl. in diesem Sinne Urteil vom 29. Juli 2019, *Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU: C: 2019: 622, Rn. 175, 176, 179 und 181).

219. Im Gegensatz zu dem Versäumnis, einer prozeduralen Pflicht wie der vorherigen Prüfung der Auswirkungen eines Projekts im speziellen Bereich des Umweltschutzes nachzukommen, kann ein Verstoß gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta aber nicht durch ein Verfahren wie das in der vorstehenden Randnummer erwähnte geheilt werden. Würden die Wirkungen nationaler Rechtsvorschriften wie der im Ausgangsverfahren in Rede stehenden aufrechterhalten, würde dies nämlich bedeuten, dass durch die betreffenden Rechtsvorschriften den Betreibern elektronischer Kommunikationsdienste weiterhin Verpflichtungen auferlegt würden, die gegen das Unionsrecht verstoßen und mit schwerwiegenden Eingriffen in die Grundrechte der Personen verbunden sind, deren Daten gespeichert wurden.

220. Das vorlegende Gericht darf somit eine Bestimmung seines nationalen Rechts nicht anwenden, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung der Rechtswidrigkeit der im Ausgangsverfahren in Rede stehenden nationalen Rechtsvorschriften in ihren zeitlichen Wirkungen zu beschränken.

221. VZ, WY und XX machen in ihren beim Gerichtshof eingereichten Erklärungen geltend, die dritte Frage werfe implizit, aber zwangsläufig die Frage auf, ob das Unionsrecht dem entgegenstehe, dass im Rahmen eines Strafverfahrens Informationen und Beweise verwertet würden, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt worden seien.

222. Insoweit ist, um dem vorlegenden Gericht eine sachgerechte Antwort zu geben, darauf hinzuweisen, dass es beim gegenwärtigen Stand des Unionsrechts grundsätzlich allein Sache des nationalen Rechts ist, die Vorschriften für die Zulässigkeit und die Würdigung der durch eine solche unionsrechtswidrige Vorratsdatenspeicherung erlangten Informationen und Beweise im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, schwere Straftaten begangen zu haben, festzulegen.

223. Nach ständiger Rechtsprechung ist es mangels einschlägiger unionsrechtlicher Vorschriften nach dem Grundsatz der Verfahrensautonomie Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats, die Verfahrensmodalitäten für Klagen, die den Schutz der den Einzelnen aus dem Unionsrecht erwachsenden Rechte gewährleisten sollen, zu regeln, wobei sie jedoch nicht ungünstiger sein dürfen als diejenigen, die gleichartige, dem innerstaatlichen Recht unterliegende Sachverhalte regeln (Äquivalenzgrundsatz), und die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren dürfen (Effektivitätsgrundsatz)

(vgl. in diesem Sinne Urteile vom 6. Oktober 2015, *Târşia*, C-69/14, EU: C: 2015: 662, Rn. 26 und 27, vom 24. Oktober 2018, *XC u. a.*, C-234/17, EU: C: 2018: 853, Rn. 21 und 22 sowie die dort angeführte Rechtsprechung, und vom 19. Dezember 2019, *Deutsche Umwelthilfe*, C-752/18, EU: C: 2019: 1114, Rn. 33).

224. Was den Äquivalenzgrundsatz anbelangt, obliegt es dem nationalen Gericht, das mit einem Strafverfahren aufgrund von Informationen oder Beweisen befasst ist, die unter Verstoß gegen die Anforderungen aus der Richtlinie 2002/58 erlangt wurden, zu prüfen, ob das für dieses Verfahren geltende nationale Recht Vorschriften vorsieht, die in Bezug auf die Zulässigkeit und die Verwertung solcher Informationen und Beweise ungünstiger sind als die Vorschriften für Informationen und Beweise, die unter Verstoß gegen innerstaatliches Recht erlangt wurden.

225. Zum Effektivitätsgrundsatz ist festzustellen, dass die nationalen Vorschriften über die Zulässigkeit und die Verwertung von Informationen und Beweisen darauf abzielen, nach Maßgabe der im nationalen Recht getroffenen Entscheidungen zu verhindern, dass rechtswidrig erlangte Informationen und Beweise einer Person, die im Verdacht steht, Straftaten begangen zu haben, unangemessene Nachteile zufügen. Dieses Ziel kann aber im nationalen Recht nicht nur durch ein Verbot der Verwertung solcher Informationen und Beweise erreicht werden, sondern auch durch nationale Vorschriften und Praktiken für die Würdigung und Gewichtung der Informationen und Beweise oder durch eine Berücksichtigung ihrer Rechtswidrigkeit im Rahmen der Strafzumessung.

226. Nach der Rechtsprechung des Gerichtshofs ist das Erfordernis, Informationen und Beweise auszuschließen, die unter Verstoß gegen unionsrechtliche Vorschriften erlangt wurden, insbesondere anhand der Gefahr zu beurteilen, die mit der Zulässigkeit solcher Informationen und Beweise für die Wahrung des Grundsatzes des kontradiktorischen Verfahrens und damit für das Recht auf ein faires Verfahren verbunden ist (vgl. in diesem Sinne Urteil vom 10. April 2003, *Steffensen*, C-276/01, EU: C: 2003: 228, Rn. 76 und 77). Kommt ein Gericht zu dem Ergebnis, dass eine Partei nicht in der Lage ist, sachgerecht zu einem Beweismittel Stellung zu nehmen, das einem Bereich entstammt, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet ist, die Würdigung der Tatsachen maßgeblich zu beeinflussen, muss es eine Verletzung des Rechts auf ein faires Verfahren feststellen und dieses Beweismittel ausschließen, um eine solche Verletzung zu verhindern (vgl. in diesem Sinne Urteil vom 10. April 2003, *Steffensen*, C-276/01, EU: C: 2003: 228, Rn. 78 und 79).

227. Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht somit dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen.

228. Nach alledem ist auf die dritte Frage in der Rechtssache C-520/18 zu antworten, dass ein nationales Gericht eine Bestimmung seines nationalen Rechts nicht anwenden darf, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung, dass nationale Rechtsvorschriften, mit denen den Betreibern elektronischer Kommunikationsdienste u. a. zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta rechtswidrig sind, in ihren zeitlichen Wirkungen zu beschränken. Art. 15 Abs. 1 der Richtlinie verpflichtet bei einer Auslegung im Licht des Effektivitätsgrundsatzes ein nationales Strafgericht dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen ».

Im Tenor des Urteils hat der Europäische Gerichtshof für Recht erkannt:

« 4. Ein nationales Gericht darf eine Bestimmung seines nationalen Rechts nicht anwenden, die es ermächtigt, die ihm nach nationalem Recht obliegende Feststellung, dass nationale Rechtsvorschriften, mit denen den Betreibern elektronischer Kommunikationsdienste u. a. zur Verfolgung der Ziele des Schutzes der nationalen Sicherheit und der Bekämpfung der Kriminalität eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte rechtswidrig sind, in ihren zeitlichen Wirkungen zu beschränken. Art. 15 Abs. 1 der Richtlinie verpflichtet bei einer Auslegung im Licht des Effektivitätsgrundsatzes ein nationales Strafgericht dazu, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen ».

B.24.2. Aus dem vorerwähnten Urteil geht hervor, dass der Gerichtshof die Folgen der für nichtig erklärten Bestimmungen nicht vorläufig aufrechterhalten darf.

B.24.3. Es obliegt dem zuständigen Strafrichter, gegebenenfalls gemäß Artikel 32 des einleitenden Titels des Strafprozessgesetzbuches und im Lichte der vom Gerichtshof der Europäischen Union im vorerwähnten Urteil vom 6. Oktober 2020 angegebenen Präzisierungen über die Zulässigkeit von Beweisen zu befinden, die bei der Umsetzung der für nichtig erklärten Bestimmungen gesammelt wurden.

Aus diesen Gründen:

Der Gerichtshof

erklärt die Artikel 2 Buchstabe *b)*, 3 bis 11 und 14 des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation » für nichtig und weist die Klagen im Übrigen zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 22. April 2021.

Der Kanzler, Der Präsident,

F. Meersschaut F. Daoût