Numéros du rôle : 6590, 6597, 6599 et 6601
Arrêt n° 57/2021 du 22 avril 2021

A R R Ê T

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.

Par ordonnance du 21 octobre 2020, la Cour, après avoir entendu les juges-rapporteurs M. Pâques et T. Merckx-Van Goey, a décidé :

- de rouvrir les débats;

- d'inviter les parties à exposer, dans un mémoire complémentaire à introduire le 23 novembre 2020 au plus tard, et à communiquer aux autres parties dans le même délai, leur point de vue sur l'incidence sur les présentes affaires de l'arrêt de la Cour de justice de l'Union européenne précité;

- qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et

- qu'en l'absence d'une telle demande, les débats seraient clos le 25 novembre 2020 et les affaires mises en délibéré.

Des mémoires complémentaires ont été introduits par :

- la partie requérante dans l'affaire n° 6590;

- les parties requérantes dans l'affaire n° 6599;

- les parties requérantes dans l'affaire n° 6601;

- le Conseil des ministres, assisté et représenté par Me E. de Lophem et Me S. Depré, avocats au barreau de Bruxelles (dans les affaires n^{os} 6590 et 6597)

- le Conseil des ministres, assisté et représenté par Me J. Vanpraet, avocat au barreau de Flandre occidentale (dans les affaires n^{os} 6599 et 6601).

À la suite des demandes de plusieurs parties à être entendues, la Cour, par ordonnance du 12 novembre 2020, a fixé l'audience au 9 décembre 2020.

À l'audience publique du 9 décembre 2020 :

- ont comparu :

. Me E. Kiehl, avocat au barreau de Liège, *loco* Me E. Lemmens, et Me J.-F. Henrotte, pour la partie requérante dans l'affaire n° 6590;

. Me R. Jespers et Me J. Fermon, avocat au barreau de Bruxelles, pour les parties requérantes dans l'affaire n° 6599;

. Me D. Pattyn, pour les parties requérantes dans l'affaire n° 6601;

. Me E. de Lophem, qui comparaissait également *loco* Me S. Depré, pour le Conseil des ministres (dans les affaires n^{os} 6590 et 6597);

. Me J. Vanpraet, pour le Conseil des ministres (dans les affaires n^{os} 6599 et 6601);

- les juges-rapporteurs M. Pâques et T. Merckx-Van Goey ont fait rapport;

- les avocats précités ont été entendus;

- les affaires ont été mises en délibéré.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

- A -

Quant aux mémoires complémentaires introduits à la suite de l'arrêt rendu par la Cour de justice de l'Union européenne le 6 octobre 2020

A.1.1. L'Ordre des barreaux francophones et germanophone (ci-après : l'OBFG) soutient que la loi « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » (ci-après : la loi attaquée) ne remplit aucune des conditions relatives aux exceptions à l'interdiction de la conservation généralisée

des données, admises par la Cour de justice de l'Union européenne par son arrêt du 6 octobre 2020 en cause *La Quadrature du Net et autres* (C-511/18, C-512/18 et C-520/18), et qu'elle ne prévoit pas les garanties effectives requises.

A.1.2. Selon l'OBFG, la loi attaquée n'organise à aucun stade de la procédure un contrôle juridictionnel de la collecte des données ni de leur conservation. En effet, le contrôle judiciaire sur l'accès demandé dans le cadre d'une enquête pénale ou le contrôle exercé par la commission BIM, en ce qui concerne les services de renseignement, porte uniquement sur l'accès aux données. Ces contrôles ne sont par ailleurs pas des recours ouverts aux tiers intéressés.

En ce qui concerne la possibilité pour un État membre de prendre des mesures législatives permettant le recours à une injonction faite aux fournisseurs de services de procéder à une conservation généralisée et indifférenciée de certaines données, indépendamment de l'absence de garanties suffisantes, la loi attaquée ne se limite pas à viser des situations ponctuelles liées à une menace grave et effective pour la sécurité nationale. La loi attaquée ne prévoit pas davantage une obligation de conservation ciblée des données relatives au trafic et des données de localisation et ne fait aucune distinction entre les personnes concernées, qu'elles soient impliquées ou non dans une enquête ou soumises ou non à un secret professionnel.

En ce qui conserve la possibilité de prévoir une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, la loi attaquée vise trois catégories de données : les données d'identification, les données d'accès et de connexion, ainsi que les données de communication. En outre, la période temporelle n'est pas limitée au strict nécessaire.

L'OBFG fait valoir que les conditions relatives aux deux dernières exceptions admises par la Cour de justice ne sont pas remplies, dès lors que le but poursuivi, de même que les données conservées, est trop large, et qu'aucun contrôle effectif n'est prévu.

L'OBFG renvoie aux points 117 et 118 de l'arrêt de la Cour de justice concernant les avocats et les autres personnes soumises au secret professionnel et précise que les données collectées et conservées en vertu de la loi attaquée permettent de déterminer si un avocat a été consulté par une personne physique ou morale, d'identifier cet avocat et ses interlocuteurs, ainsi que les dates et heures de la communication.

A.1.3. Enfin, l'OBFG considère que la Cour n'est pas autorisée à maintenir les effets de la loi attaquée, en cas d'annulation.

A.2.1. Les parties requérantes dans l'affaire n° 6599 soutiennent qu'il résulte de l'arrêt de la Cour de justice du 6 octobre 2020 que les moyens sont fondés et que la loi attaquée doit être annulée dans son intégralité. En effet, l'ensemble des dispositions de la loi attaquée sont liées à l'obligation de conservation générale et indifférenciée des données de trafic et de localisation, qui a été censurée par la Cour de justice.

A.2.2. Les parties requérantes considèrent qu'aucune des dispositions de la loi attaquée ne correspond à l'une des cinq hypothèses que la Cour de justice a jugées compatibles avec 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 » (ci-après : la directive 2002/58/CE). Ainsi, la loi attaquée ne contient aucune disposition spécifique portant sur la conservation des adresses IP pour une période temporellement limitée au strict nécessaire, sur la conservation des données relatives l'identité civile des utilisateurs, sur l'obligation qui pourrait être imposée à ceux qui conservent les données et aux opérateurs de procéder en temps réel à une analyse des données relatives au trafic et des données de localisation, ou sur la conservation en temps réel de données techniques relatives à la localisation des équipements terminaux. En tout état de cause, la loi attaquée ne contient pas de règles claires et précises selon lesquelles la conservation des données a lieu conformément aux modalités matérielles et procédurales qui y sont attachées, ni de garanties effectives contre le risque d'abus, comme l'exige pourtant la Cour de justice.

A.2.3. Les parties requérantes estiment que l'arrêt de la Cour de justice ne permet pas de maintenir, en cas d'annulation, les effets de la loi attaquée et que le juge pénal n'est pas autorisé à utiliser des informations ou éléments de preuve recueillis en application de cette loi, ces informations ou éléments devant dès lors être écartés du dossier. Elles se demandent si les trois conditions mentionnées par la Cour de justice qui, lorsqu'elles sont

réunies, imposent au juge pénal d'écarter les informations ou éléments de preuve qui ont été obtenus par la conservation généralisée et indifférenciée des données, sont cumulatives ou non, et considèrent à titre subsidiaire que l'existence d'une seule des trois conditions suffit pour écarter les informations ou éléments précités des débats.

A.3.1. En ce qui concerne la première branche du premier moyen, les parties requérantes dans l'affaire n° 6601 font valoir que la loi attaquée ne met pas en place un système permettant une injonction générale de conservation des données, ni une conservation ciblée, ni une injonction de conservation rapide, au sens où l'entend la Cour de justice. L'obligation de conservation est la conséquence directe et exclusive de la loi attaquée, sans qu'une autorité compétente doive, à cet effet, y enjoindre les fournisseurs et aux opérateurs visés dans la loi.

Les parties requérantes font valoir que la loi attaquée ne prévoit pas un régime spécifique à l'égard des adresses IP et des données d'identification. L'article 126, § 3, alinéa 4, de la loi du 13 juin 2005 « relative aux communications électroniques » (ci-après : la loi du 13 juin 2005) opère une délégation au Roi à cet égard. Cette délégation ne décrit pas suffisamment précisément les données à conserver ni ne fixe les conditions essentielles auxquelles ces données doivent répondre. Elle ne satisfait dès lors pas aux exigences de la Cour de justice. En outre, la loi attaquée ne fait aucune distinction, limitation ou exception en fonction du but poursuivi par la conservation des données. Elle concerne toutes les personnes qui font usage des moyens de communication électronique, même s'il n'y a aucune indication que leur comportement est lié à des faits répréhensibles graves. La conservation de ces données n'est pas non plus limitée à ce qui est strictement nécessaire en vue de la réalisation des buts poursuivis. Il appartient au législateur de mettre en place un tout nouveau régime complet.

En ce qui concerne la troisième branche, les parties requérantes renvoient au point 118 de l'arrêt de la Cour de justice concernant l'incidence de l'obligation de conservation généralisée des données sur les personnes qui sont tenues au secret professionnel et sur les lanceurs d'alerte.

A.3.2. En ce qui concerne le deuxième moyen, les parties requérantes soutiennent que l'annulation de l'obligation de conservation des données entraîne nécessairement l'annulation de l'accès à celles-ci.

En ce qui concerne la première branche, les parties requérantes font valoir que la loi attaquée autorise les autorités judiciaires à avoir accès aux données pour toute infraction. En outre, les services de renseignement et de sécurité peuvent accéder aux données dans le cadre d'un grand nombre de menaces potentielles insuffisamment délimitées, sans que leur habilitation soit suffisamment limitée. La loi attaquée ne limite donc pas l'accès aux données ainsi conservées aux fins de garantir la sécurité nationale et de lutter contre la criminalité grave.

Les parties requérantes font valoir qu'à la différence de l'arrêt du 2 octobre 2018, *Ministerio Fiscal* (C-207/16), qui porte sur des données d'identification de nature commerciale, auxquelles les autorités compétentes peuvent avoir accès sans que cet accès soit limité aux fins de la lutte contre la criminalité grave, l'arrêt de la Cour de justice du 6 octobre 2020 restreint l'accès aux données à des finalités bien précises, à savoir garantir la sécurité nationale, lutter contre la criminalité grave et prévenir les menaces graves pour la sécurité publique.

Les parties requérantes font valoir que l'arrêt de la Cour de justice du 6 octobre 2020 n'est pas pertinent pour apprécier la deuxième branche du moyen, qui concerne l'absence de contrôle préalable de l'accès aux données que doit exercer une instance judiciaire ou une autorité administrative indépendante, puisque les données qui ont été collectées sur la base d'une obligation de conservation jugée contraire au droit de l'Union ne peuvent pas être traitées, indépendamment de la question de savoir si un contrôle préalable est organisé ou non.

L'article 88*bis* du Code d'instruction criminelle, tel qu'il a été modifié par l'article 9 de la loi attaquée, permet au juge d'instruction d'accéder aux données conservées pour la recherche, l'examen et les poursuites d'infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde. Cet accès vise le 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 et la localisation de l'origine ou de la destination de communications électroniques. Cet accès ne concerne donc pas les données d'identification. L'article 88*bis*,

précité, ne saurait donc être maintenu en vue d'obtenir l'accès à ces données. Les données d'identification (commerciales) ne peuvent être communiquées par les fournisseurs et par les opérateurs qu'après que le juge d'instruction a rendu une ordonnance à cet effet, conformément à l'article 88*quater*, § 2, du Code d'instruction criminelle.

A.3.3. En ce qui concerne le troisième moyen, les parties requérantes font valoir que l'annulation de l'obligation de conservation s'étend nécessairement aussi aux délais de conservation de ces données et qu'il appartient aux personnes concernées (fournisseurs et opérateurs, services de renseignement et de sécurité, etc.) d'effacer les données de télécommunication recueillies en application de la loi attaquée.

A.3.4. En ce qui concerne le quatrième moyen, les parties requérantes renvoient à l'arrêt du 16 juillet 2020 en cause *Schrems II*, par lequel la Cour de justice annule la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 « conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis ».

A.3.5. Les parties requérantes font valoir que l'arrêt de la Cour de justice C-511/18 s'oppose au maintien des effets de la loi attaquée, en cas d'annulation. L'article 32 du titre préliminaire du Code de procédure pénale doit être interprété comme obligeant le juge à exclure les données collectées en application de la loi attaquée en tant que preuves. L'usage de ces données est en effet contraire au droit à un procès équitable, si les personnes suspectées d'avoir commis une infraction ne disposent pas d'une réelle possibilité de commenter utilement ces informations et les éléments de preuve, si ces informations et éléments de preuve portent sur un domaine technique au sujet duquel le juge n'a pas de connaissances et s'ils peuvent avoir une influence déterminante sur son appréciation des faits. Pour le reste, en ce qui concerne l'utilisation des données autrement qu'en tant que preuve dans une procédure pénale, ces données doivent être supprimées par les personnes concernées (fournisseurs et opérateurs, services de renseignement et de sécurité, etc.).

A.4.1. Selon le Conseil des ministres, il résulte de l'arrêt de la Cour de justice du 6 octobre 2020 qu'une obligation légale généralisée et indifférenciée de conservation, en tout cas pour ce qui concerne les adresses IP attribuées à la source d'une connexion et les données d'identité civile des utilisateurs de moyens de communications électroniques, est compatible avec la directive 2002/58/CE et avec la Charte des droits fondamentaux de l'Union européenne.

A.4.2. Le Conseil des ministres soutient que l'obligation de conservation des adresses IP attribuées à la source, telle que la prévoit la loi attaquée, a lieu « en vue de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique […], à l'instar de la sauvegarde de la sécurité nationale », comme le montre le fait que l'accès à ces données soit réglé à l'article 126, § 2, de la loi du 13 juin 2005. C'est d'autant plus vrai que l'accès aux données doit toujours respecter les principes de proportionnalité et de subsidiarité.

Ainsi, selon la Conseil des ministres, l'accès à ces données dans le cadre d'une instruction pénale n'est possible que pour la détection des infractions visées à l'article 88*bis*, § 2, du Code d'instruction criminelle. En revanche, dans le cadre d'une information, il n'est possible d'accéder aux données d'identification visées à l'article 46*bis* du même Code qu'en vue de détecter des crimes et des délits et sous réserve de respecter les principes de proportionnalité et de subsidiarité. Quant aux services de renseignement et de sécurité, ils ne peuvent avoir accès aux adresses IP attribuées à la source que dans l'intérêt de l'accomplissement de leurs missions, telles qu'elles sont légalement décrites. Tout officier de police judiciaire de l'IBPT ne peut avoir accès aux données qu'en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et 126 de la loi du 13 juin 2005. Enfin, l'accès à ces données par un officier de la Cellule des personnes disparues, pour une période limitée à 48 heures, contribue également aux objectifs définis par la Cour de justice. À cet égard, le Conseil des ministres juge que la durée de conservation des adresses IP attribuées à la source, qui est de douze mois, n'excède pas ce qui est strictement nécessaire pour atteindre l'objectif poursuivi.

Selon le Conseil des ministres, la conservation et l'accès aux adresses IP précitées sont soumis à des conditions strictes et font l'objet des mécanismes de contrôle requis.

A.4.3. Le Conseil des ministres soutient que l'obligation de conserver les données d'identité civile des utilisateurs de moyens de communications électroniques est compatible avec les dispositions invoquées dans les moyens. Il rappelle que cette obligation de conservation est entourée des garanties nécessaires en termes d'accès, de conservation et de contrôle.

A.4.4. En ce qui concerne l'incidence de l'arrêt de la Cour de justice sur la loi attaquée, le Conseil des ministres souligne que les adresses IP attribuées à la source constituent des données d'identification au sens de l'article 126, § 3, alinéa 1er, de la loi du 13 juin 2005. Ce type de données ne constituent pas des données relatives au trafic. Tant l'obligation généralisée et indifférenciée de conserver les données relatives à l'identité civile des utilisateurs de communications électroniques que l'obligation généralisée et indifférenciée de conserver les adresses IP attribuées à la source d'une connexion sont visées par l'article 126, § 3, alinéa 1er, de la loi du 13 juin 2005. De l'avis du Conseil des ministres, la loi attaquée est donc en tout état de cause compatible sur ces points avec les dispositions invoquées dans les moyens. Une éventuelle annulation de la loi attaquée devrait se limiter à l'article 126, § 3, alinéas 2 et 3, de la loi du 13 juin 2005. Dès lors que l'obligation généralisée et indifférenciée de conserver ces deux types de données est compatible avec les dispositions invoquées dans les moyens, les autres dispositions de la loi attaquée ne devraient pas non plus être annulées. En effet, elles contiennent les garanties nécessaires en termes de conservation et d'accès à ces données.

- *B* -

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 n° 84/2015 de la Cour constitutionnelle, les modifications suivantes sont apportées :

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

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

b) au lieu du 74°, annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré un 74° rédigé comme suit :

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

Art. 3. L'article 125, § 2, de la même loi est abrogé.

Art. 4. Dans la même loi, à la place de l'article 126 annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré un article 126 rédigé comme suit :

' Art. 126. § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, les opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, conservent les données visées au paragraphe 3, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

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

L'obligation de conserver les données visées au paragraphe 3 s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :

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

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

§ 2. Seules les autorités suivantes peuvent obtenir, sur simple demande, des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, des données conservées en vertu du présent article, pour les finalités et selon les conditions énumérées ci-dessous :

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

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

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

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

5° l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, dans le cadre de sa mission d'assistance à personne en danger, de recherche de

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

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

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

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

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

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

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre.

§ 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs visés au paragraphe 1er, alinéa 1er :

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

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite,

la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

3° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er;

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

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

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

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

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

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

Ces statistiques comprennent notamment :

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

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

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

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, 1°, sont également jointes au rapport que le ministre de la Justice doit faire au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

Le Roi détermine, sur proposition du ministre de la Justice et du ministre et sur avis de l'Institut, les statistiques que les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er,

transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 6. Sans préjudice du rapport visé au paragraphe 5, alinéa 4, le ministre et le ministre de la Justice font un rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 3, alinéa 4, sur la mise en œuvre du présent article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation. '.

Art. 5. Dans la même loi, un article 126/1 est inséré rédigé comme suit :

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

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

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

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

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

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

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

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

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

Chaque opérateur et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, veille à la confidentialité des données traitées par la Cellule de coordination et communique sans délai à

l’Institut et à la Commission pour la protection de la vie privée les coordonnées de la Cellule de coordination et de ses membres ainsi que toute modification de ces données.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2° le paragraphe 6 est abrogé.

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

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

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

3° au lieu du paragraphe 3*ter*, annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré un paragraphe 3*ter* rédigé comme suit :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1° la nature de la méthode spécifique;

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

3° la menace potentielle qui justifie la méthode spécifique;

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

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

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

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

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

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

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

11° la date de la décision;

12° la signature du dirigeant du service. ';

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B.2. 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 n^{os} 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 » (points 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 n^{os} 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