Affaire C-793/19

Demande de décision préjudicielle

Date de dépôt :

29 octobre 2019

Juridiction de renvoi :

Bundesverwaltungsgericht (Allemagne)

Date de la décision de renvoi :

25 septembre 2019

Partie requérante et défenderesse en « Revision » :

SpaceNet AG

Partie défenderesse et requérante en « Revision » :

République fédérale d'Allemagne

[omissis]

Bundesverwaltungsgericht

ORDONNANCE

[omissis]

Dans le litige en matière administrative opposant

SpaceNet AG,

[omissis] Munich,

partie requérante et défenderesse en « Revision »,

à

République fédérale d'Allemagne, représentée par la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer),

[omissis] Bonn,

partie défenderesse et requérante en « Revision »,

[Or. 2]

la sixième chambre du Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne) a décidé, à la suite de l'audience du 25 septembre 2019 [omissis] :

Il est sursis à statuer.

La Cour de justice de l'Union européenne est invitée à statuer sur la question suivante :

L'article 15 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, d'une part, et de l'article 6 de la charte des droits fondamentaux de l'Union européenne ainsi que de l'article 4 du traité sur l'Union européenne, d'autre part, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale qui impose aux fournisseurs de services de communications électroniques accessibles au public de conserver les données relatives au trafic et les données de localisation des utilisateurs finals de ces services lorsque

– cette obligation n'est pas subordonnée à l'existence d'un motif spécifique d'un point de vue géographique, temporel ou territorial,

– dans le cadre de la fourniture de services téléphoniques accessibles au public – y compris la communication par SMS, message multimédia ou message similaire et les appels restés sans réponse ou infructueux –, l'obligation de conservation porte sur les données suivantes :

  – le numéro d'appel ou une autre identification des lignes appelante et appelée, ainsi que de toute autre ligne utilisée en cas de transfert d'appel ou de déviation d'appel,

  – la date et l'heure du début et de la fin de la communication ou – en cas de communication par SMS, message multimédia ou message similaire – le moment de l'envoi et de la réception du message, le fuseau horaire en cause étant précisé,

  – les indications relatives au service utilisé lorsque des services différents peuvent être utilisés dans le cadre du service téléphonique,

  – en outre, en cas de services de téléphonie mobile, **[Or. 3]**

    – l'identité internationale d'abonné mobile de l'appelant et de l'appelé,

- l'identité internationale des terminaux appelant et appelé,
- la date et l'heure de la première activation du service, le fuseau horaire en cause étant précisé, lorsque des services ont été payés à l'avance,
- la désignation des cellules qui ont été utilisées par l'appelant et l'appelé au début de la communication,

– ainsi que, dans le cas des services de téléphonie par Internet, les adresses IP (protocole internet) de l'appelant et de l'appelé et les numéros d'identifiant attribués,

– dans le cadre de la fourniture de services d'accès à Internet accessibles au public, l'obligation de conservation porte sur les données suivantes :

- l'adresse IP attribuée à l'abonné aux fins de l'utilisation d'Internet,
- l'identification claire de la connexion permettant l'accès à Internet, ainsi que le numéro d'identifiant attribué,
- la date et l'heure du début et de la fin de l'utilisation d'Internet à partir de l'adresse IP attribuée, le fuseau horaire en cause étant précisé,
- en cas d'utilisation mobile, la désignation des cellules utilisées au début de la connexion Internet,

– les données suivantes ne peuvent pas être conservées :

- le contenu de la communication,
- les données relatives aux sites Internet consultés,
- les données des services de courrier électronique,
- les données qui sous-tendent les communications vers ou à partir de certaines lignes attribuées à des personnes, des autorités **[Or. 4]** et des organisations à caractère social ou religieux,

– la durée de conservation s'élève à quatre semaines pour les données de localisation, c'est-à-dire la désignation des cellules utilisées, et à dix semaines pour les autres données,

– une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données est garantie

– les données conservées ne peuvent être utilisées qu'aux fins de la répression des infractions graves ou aux fins de la prévention d'un risque concret pour l'intégrité physique, la vie ou la liberté d'une personne ou bien pour l'existence de l'État fédéral ou d'un Land et il est fait exception à cela pour ce qui est de l'adresse IP attribuée à l'abonné pour l'utilisation d'Internet, laquelle peut être utilisée dans le cadre de la fourniture d'informations sur les données relatives à l'abonné aux fins de la répression d'une infraction pénale, quelle qu'elle soit, de la prévention d'un risque pour la sécurité et l'ordre publics ainsi qu'aux fins de l'exercice des missions des services de renseignement ?

M o t i f s :

I

1 La requérante fournit des services d'accès à Internet accessibles au public. Son action en constatation est dirigée contre l'obligation, mise à sa charge par les dispositions combinées de l'article 113a, paragraphe 1, et de l'article 113b du Telekommunikationsgesetz (loi sur les télécommunications, ci-après le « TKG ») dans sa rédaction résultant de la loi du 10 décembre 2015, de conserver les données relatives au trafic qui sont afférentes aux télécommunications de ses clients à compter du 1er juillet 2017.

2 Par arrêt du 20 avril 2018, le Verwaltungsgericht (tribunal administratif) saisi du recours a constaté que la requérante n'était pas tenue de conserver les données relatives au trafic qui sont afférentes aux télécommunications, lesquelles sont visées à l'article 113b, paragraphe 3, du TKG, des clients auxquels elle fournit un accès à Internet. Il a estimé que cette obligation de conservation était contraire au droit de l'Union et n'était donc pas applicable à la requérante. Les questions juridiques de principe relatives à la portée et aux exigences matérielles du droit de l'Union qui est pertinent dans le présent contexte ont été tranchées, selon lui, par l'arrêt du 21 décembre 2016, **[Or. 5]** Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970).

3 La défenderesse a formé un recours (direct) en « Revision », autorisé par le Verwaltungsgericht (tribunal administratif), contre la décision de première instance. Elle conclut à la réformation de l'arrêt attaqué du Verwaltungsgericht (tribunal administratif) et au rejet du recours.

II

4 Il convient de surseoir à statuer, car la solution du litige dépend d'une décision préalable de la Cour de justice de l'Union européenne sur l'interprétation des traités (article 267 du traité sur le fonctionnement de l'Union européenne).

5 1. Le recours en « Revision » de la défenderesse contre l'arrêt en constatation du Verwaltungsgericht (tribunal administratif) n'est fondé que si les dispositions de

l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG sont compatibles avec celles du droit de l'Union, lesquelles sont assorties de la primauté. Dans le cas contraire, il y a lieu de rejeter le recours en « Revision ». Si l'obligation, imposée aux fournisseurs de services de télécommunications accessibles au public par les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG, de conserver des données relatives au trafic qui sont afférentes aux télécommunications est contraire au droit de l'Union, le recours en « Revision » ne peut pas non plus prospérer au motif qu'il n'a pas été porté atteinte aux droits de la requérante [voir article 113, paragraphe 1, première phrase, de la Verwaltungsgerichtsordnung (code de procédure administrative)]. Peu importe à cet égard de savoir si la requérante peut également, en sa qualité d'entreprise de télécommunications – et donc non en qualité d'abonné, mais uniquement en qualité de fournisseur de la communication –, se prévaloir des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel qui sont consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »). En effet, l'obligation de conservation constitue en tout état de cause, eu égard aux ressources techniques et financières qui y sont allouées, une atteinte à la liberté d'entreprise de la requérante qui est garantie par l'article 16 de la Charte. Si les dispositions de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG ne sont pas compatibles avec le droit de l'Union, elles ne sauraient – étant donné qu'une interprétation conforme au droit de l'Union est exclue – être appliquées, en vertu du principe de la primauté du droit de l'Union (jurisprudence constante de la Cour, voir arrêts du 9 mars 1978, Simmenthal, 106/77, **[Or. 6]** EU:C:1978:49 point 24 ; du 3 mai 2005, Berlusconi e.a., C-387/02, C-391/02 et C-403/02, EU:C:2005:270, point 72 ; du 22 juin 2010, Melki et Abdeli, C-188/10 et C-189/10, EU:C:2010:363, point 43, et du 18 septembre 2014, Vueling Airlines, C-487/12, EU:C:2014:2232, point 48). L'inapplicabilité des dispositions a pour conséquence que la limitation des droits fondamentaux n'est pas « prévue par la loi » au sens de l'article 52, paragraphe 1, première phrase, de la Charte.

6 Certes, il y aurait également lieu de rejeter le recours en « Revision » si les dispositions légales étaient compatibles avec le droit de l'Union, mais contraires à des droits fondamentaux garantis par le Grundgesetz (Loi fondamentale, ci-après le « GG ») et si elles étaient nulles de ce fait. Dans ce cas, la décision du Verwaltungsgericht (tribunal administratif) serait correcte pour d'autres motifs [omissis : développements relatifs à la procédure nationale en matière de contrôle de constitutionnalité].

7 2. L'obligation des opérateurs de télécommunications consistant à conserver certaines données relatives au trafic pendant une période limitée a été redéfinie par le Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (loi portant instauration de l'obligation de conserver les données relatives au trafic et fixation d'une durée maximale de conservation) du 10 décembre 2015 (BGBl. I p. 2218), après l'annulation des articles 113a et 113b du TKG, ainsi que de l'article 100g, paragraphe 1, première phrase, de la

Strafprozessordnung (code de procédure pénale, ci-après la « StPO »), dans la mesure où il autorisait la collecte des données relatives au trafic visées par l'article 113a du TKG, dans sa rédaction résultant de la loi du 21 décembre 2007 (BGBl. I p. 3198), par le Bundesverfassungsgericht (Cour constitutionnelle fédérale) au motif qu'ils étaient contraires à l'article 10, paragraphe 1, du GG [omissis] **[Or. 7]** [omissis]. La redéfinition de l'obligation avait été précédée en outre par l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014, qui avait déclaré invalide 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 (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238), laquelle servait également de base à la loi du 21 décembre 2007. La loi du 10 décembre 2015 vise à combler des lacunes en matière de répression et de prévention des risques, mais aussi à tenir compte des exigences de la constitution et du droit de l'Union qui se dégagent des décisions de justice susmentionnées [omissis]. Elle comporte notamment les dispositions modifiées du TKG et de la StPO qui sont reproduites ci-dessous.

8 L'article 113a, paragraphe 1, première phrase, du TKG est libellé comme suit :

> Les obligations relatives à la conservation de données relatives au trafic, à l'utilisation des données et à la sécurité des données qui sont définies aux articles 113b à 113g se rapportent aux opérateurs qui fournissent aux utilisateurs finals des services de télécommunications accessibles au public.

9 L'article 113b est libellé comme suit :

(1) Les opérateurs visés à l'article 113a, paragraphe 1, sont tenus de conserver les données sur le territoire national de la manière suivante :

1. pendant dix semaines pour ce qui est des données visées aux paragraphes 2 et 3,

2. pendant quatre semaines pour ce qui est des données de localisation visées au paragraphe 4.

(2) Les fournisseurs de services téléphoniques accessibles au public conservent

1. le numéro d'appel ou une autre identification des lignes appelante et appelée, ainsi que de toute autre ligne utilisée en cas de transfert d'appel ou de déviation d'appel,

2. la date et l'heure du début et de la fin de la communication, le fuseau horaire en cause étant précisé,

3. les indications relatives au service utilisé lorsque des services différents peuvent être utilisés dans le cadre du service téléphonique,

4. en outre, en cas de services de téléphonie mobile,

   a) l'identité internationale d'abonné mobile de l'appelant et de l'appelé,

   b) l'identité internationale des terminaux appelant et appelé, **[Or. 8]**

   c) la date et l'heure de la première activation du service, le fuseau horaire en cause étant précisé, lorsque des services ont été payés à l'avance,

5. ainsi que, dans le cas des services de téléphonie par Internet, les adresses IP (protocole internet) de l'appelant et de l'appelé et les numéros d'identifiant attribués.

Le premier alinéa s'applique mutatis mutandis

1. en cas de communication par SMS, message multimédia ou message similaire ; dans ce cas, les indications visées au premier alinéa, point 2, sont remplacées par le moment de l'envoi et de la réception du message ;

2. aux appels restés sans réponse ou infructueux en raison d'une intervention du gestionnaire du réseau [omissis].

(3) Les fournisseurs de services d'accès à Internet accessibles au public conservent

1. l'adresse IP attribuée à l'abonné aux fins de l'utilisation d'Internet,

2. l'identification claire de la connexion permettant l'accès à Internet, ainsi que le numéro d'identifiant attribué,

3. la date et l'heure du début et de la fin de l'utilisation d'Internet à partir de l'adresse IP attribuée, le fuseau horaire en cause étant précisé.

(4) En cas d'utilisation de services de téléphonie mobile, il y a lieu de conserver la désignation des cellules qui ont été utilisées par l'appelant et l'appelé au début de la communication. Pour ce qui est des services d'accès à Internet accessibles au public, il y a lieu de conserver, en cas d'utilisation mobile, la désignation des cellules utilisées au début de la connexion Internet. Il convient également de conserver les données permettant de connaître la position géographique et les directions du rayonnement maximal des antennes desservant la cellule concernée.

(5) Le contenu de la communication, les données relatives aux sites Internet consultés et les données des services de courrier électronique ne peuvent être conservées en vertu de la présente disposition.

(6) Les données qui sous-tendent les communications visées à l'article 99, paragraphe 2, ne peuvent être conservées en vertu de la présente disposition. Cela s'applique, mutatis mutandis, aux communications téléphoniques émanant des entités visées à l'article 99, paragraphe 2. L'article 99, paragraphe 2, deuxième à septième phrases, s'applique mutatis mutandis.

[…]

10 Les communications visées à l'article 99, paragraphe 2, du TKG, auxquelles l'article 113b, paragraphe 6, du TKG renvoie, sont des communications avec des personnes, des autorités et des organisations à caractère social ou religieux qui proposent uniquement ou essentiellement, à des appelants restant en principe anonymes, des services d'assistance téléphonique en cas de situation d'urgence psychologique ou sociale et qui sont elles-mêmes soumises ou dont les collaborateurs sont soumis **[Or. 9]** à des obligations de confidentialité particulières à cet égard. La dérogation prévue à l'article 99, paragraphe 2, deuxième et quatrième phrases, du TKG est subordonnée à l'inscription des appelés, à leur demande, sur une liste par la Bundesnetzagentur, après que les titulaires des numéros d'appel ont établi leur mission en produisant une attestation d'une autorité, d'un organisme, d'un établissement ou d'une fondation de droit public.

11 L'article 113c du TKG est libellé comme suit :

(1) Les données conservées en vertu de l'article 113b peuvent

1. être transmises à une autorité répressive lorsque celle-ci demande la transmission en invoquant une disposition légale qui l'autorise à collecter les données visées à l'article 113b aux fins de la répression d'infractions pénales particulièrement graves ;

2. être transmises à une autorité de sûreté des Länder lorsque celle-ci demande la transmission en invoquant une disposition légale qui l'autorise à collecter les données visées à l'article 113b aux fins de la prévention d'un risque concret pour l'intégrité physique, la vie ou la liberté d'une personne ou bien pour l'existence de l'État fédéral ou d'un Land ;

3. être utilisées par le fournisseur de services de télécommunications accessibles au public aux fins de la fourniture d'informations au titre de l'article 113, paragraphe 1, troisième phrase.

(2) Les données conservées en vertu de l'article 113b ne peuvent pas être utilisées, par les débiteurs des obligations édictées à l'article 113a, paragraphe 1, à des fins autres que celles qui sont visées au paragraphe 1.

[…]

12 Aux termes de l'article 113, paragraphe 1, troisième phrase, du TKG, qui est mentionné à l'article 113c, paragraphe 1, point 3, du TKG, les données (relatives à l'abonné) devant figurer dans des informations adressées à l'une des entités visées à l'article 113, paragraphe 3, du TKG peuvent également être déterminées à l'aide d'une adresse IP attribuée à un moment donné ; à cette fin, les données relatives au trafic peuvent également être exploitées de manière automatisée. En vertu de l'article 113, paragraphe 2, première phrase, du TKG, les informations peuvent uniquement être fournies si elles sont demandées, par écrit et dans des cas individuels, par l'une des entités visées au paragraphe 3 aux fins de la répression de crimes, de délits ou de contraventions, de la prévention de risques pour la sécurité ou l'ordre publics ou de l'exercice, par les entités visées au paragraphe 3, point 3 [les autorités fédérales et régionales de protection de la constitution, le Militärischer Abschirmdienst (Service de contre-espionnage militaire) et le Bundesnachrichtendienst (Service fédéral de renseignement)], des missions qui leur incombent en vertu de la loi, la disposition légale qui les autorise à collecter les données mentionnées au paragraphe 1 étant précisée. **[Or. 10]**

13 L'article 113d du TKG est libellé comme suit :

Le débiteur de l'obligation prévue à l'article 113a, paragraphe 1, doit veiller à ce que les données conservées conformément à l'article 113b, paragraphe 1, en vertu de l'obligation de conservation soient protégées, par des mesures techniques et organisationnelles correspondant à l'état de la technique, contre le contrôle et l'utilisation non autorisés. Ces mesures comprennent en particulier :

1. l'utilisation d'un procédé de cryptage particulièrement sûr,

2. le stockage dans des infrastructures de stockage distinctes, séparées de celles qui sont affectées aux fonctions opérationnelles courantes,

3. le stockage, assorti d'un niveau de protection élevé contre les cyberattaques, sur des systèmes informatiques de traitement des données découplés,

4. la restriction de l'accès aux installations utilisées pour le traitement de données aux personnes disposant d'une habilitation spéciale conférée par le redevable de l'obligation et

5. l'obligation de faire intervenir, lors de l'accès aux données, au moins deux personnes disposant d'une habilitation spéciale conférée par le redevable de l'obligation.

14 L'article 113e du TKG est libellé comme suit :

(1) Le débiteur de l'obligation prévue à l'article 113a, paragraphe 1, doit veiller à ce que, aux fins du contrôle de la protection des données, chaque accès, et notamment la lecture, la copie, la modification, l'effacement et le verrouillage, à des données conservées conformément à l'article 113b,

paragraphe 1, en vertu de l'obligation de conservation soit consigné. Doivent être consignés

1. l'heure de l'accès,

2. les personnes accédant aux données,

3. l'objet et la nature de l'accès.

(2) Les données consignées ne peuvent pas être utilisées à des fins autres que celles du contrôle de la protection des données.

(3) Le débiteur de l'obligation prévue à l'article 113a, paragraphe 1, doit veiller à ce que les données consignées soient effacées au bout d'un an.

15 Afin de garantir un niveau de sécurité et de qualité des données particulièrement élevé, la Bundesnetzagentur établit, conformément à l'article 113f, paragraphe 1, du TKG, un ensemble d'exigences qui doit être évalué en permanence et adapté le cas échéant (article 113f, paragraphe 2, du TKG). L'article 113g du TKG exige que des mesures de sécurité spécifiques soient intégrées dans l'exposé de la politique en matière de sécurité qui doit être présenté par le débiteur.

16 L'article 100g de la StPO est libellé comme suit :

[…]

(2) Si certains faits permettent de soupçonner que quelqu'un a commis, en qualité d'auteur ou de complice, l'une des infractions pénales particulièrement graves visées dans la deuxième phrase ou, dans les cas dans lesquels la tentative est punissable, a tenté de commettre une telle infraction et si l'infraction est également particulièrement grave dans le cas particulier, les données relatives au trafic conservées **[Or. 11]** conformément à l'article 113b du Telekommunikationsgesetz peuvent être recueillies dès lors que l'enquête sur les faits ou la localisation de la personne faisant l'objet de l'enquête par d'autres moyens seraient excessivement difficiles ou vouées à l'échec et que la collecte des données est proportionnée à l'importance de l'affaire.

[…]

(4) La collecte de données relatives au trafic conformément au paragraphe 2, même lu en combinaison avec le paragraphe 3, deuxième phrase, qui est dirigée contre une personne visée à l'article 53, paragraphe 1, premier alinéa, points 1 à 5, et qui est susceptible de déboucher sur des informations au sujet desquelles elle serait habilitée à refuser de témoigner, n'est pas autorisée. […]

17 L'article 101a, paragraphe 1, de la StPO soumet la collecte de données relatives au trafic conformément à l'article 100g de la StPO [omissis] à une autorisation du juge [omissis]. En vertu de l'article 101a, paragraphe 2, de la StPO, les motifs de la décision doivent comporter les considérations essentielles relatives au caractère nécessaire et approprié de la mesure dans le cas particulier en question. L'article 101a, paragraphe 6, de la StPO prévoit une obligation d'informer les participants à la télécommunication concernée.

18 3. Le point de savoir [omissis] si l'obligation de conservation imposée par les dispositions combinées de l'article 113a, paragraphe 1, et de l'article 113b du TKG est contraire au droit de l'Union [omissis] dépend de l'interprétation 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) (JO 2002, L 201, p. 37) et il n'est pas possible de le trancher de manière définitive sans interroger la Cour de justice de l'Union européenne à titre préjudiciel. À cet égard, la chambre de céans se fonde sur les considérations suivantes :

19 a) C'est à bon droit que le Verwaltungsgericht (tribunal administratif) a considéré que la directive 2002/58/CE était applicable et qu'il a examiné les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG à l'aune de celle-ci. Le fait que les réglementations nationales portant sur la conservation des données relatives au trafic et des données de localisation ainsi que sur l'accès à ces données par les autorités nationales relèvent en principe du champ d'application de cette **[Or. 12]** directive a été établi de manière définitive par la Cour (arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 65 et suivants ainsi que 81).

20 b) L'obligation de conserver les données relatives au trafic afférentes aux télécommunications, qui est régie par les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG, limite les droits découlant de l'article 5, paragraphe 1, de l'article 6, paragraphe 1, et de l'article 9, paragraphe 1, de la directive 2002/58/CE. Elle porte atteinte à la confidentialité des communications électroniques garantie à l'article 5, paragraphe 1, première phrase, de la directive et est contraire au principe de l'interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. De plus, elle ne respecte pas les prescriptions de l'article 6 de la directive, en vertu desquelles les données relatives au trafic peuvent uniquement être traitées et conservées pour établir les factures et afin de commercialiser et de fournir des services à valeur ajoutée, dans la mesure et pour la durée nécessaire à cet égard. Pour le cas où des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées,

l'article 9, paragraphe 1, première phrase, de la directive 2002/58/CE dispose que ces données ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. La législation déroge également à cette prescription, dans la mesure où les dispositions combinées de l'article 113b, paragraphe 1, point 2 et de l'article 113b, paragraphe 4, du TKG imposent également de conserver les données de localisation qui y sont mentionnées.

21 c) La limitation des droits tirés de l'article 5, paragraphe 1, de l'article 6, paragraphe 1, et de l'article 9, paragraphe 1, de la directive 2002/58/CE n'est justifiée que si les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG peuvent s'appuyer sur la base juridique constituée par l'article 15, paragraphe 1, de cette même directive. Aux termes de cette disposition, 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 ladite 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 **[Or. 13]** 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 paragraphe [1]. Toutes les mesures visées dans le paragraphe [1] 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 (article 15, paragraphe 1, deuxième phrase, de la directive 2002/58/CE).

22 aa) Selon l'arrêt susmentionné rendu par la Cour le 21 décembre 2016, 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, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique (arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 82 et suivants).

23 Dans l'arrêt précité, qui portait sur les réglementations en matière de conservation des données qui visaient à transposer la directive 2006/24/CE en Suède et au Royaume-Uni, la Cour a également établi des conditions régissant la licéité d'une législation nationale fondée sur l'article 15, paragraphe 1, de la directive 2002/58/CE (arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 108 et suivants). Selon cet arrêt, 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, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données 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. Pour satisfaire à ces exigences, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données **[Or. 14]** ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire. En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné. S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données 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. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

24 Aux termes des motifs précités de la Cour, la licéité, au regard de l'article 15, paragraphe 1, de la directive 2002/58/CE, d'une réglementation nationale en matière de conservation des données suppose par conséquent qu'il y ait un motif suffisant, que seules soient visées les personnes pour lesquelles il existe un élément indiquant un rapport avec des actes de criminalité grave, qu'une limitation à la région, à la période et aux moyens de communication qui sont pertinents pour le motif en question soit prévue et que seules soient visées les **[Or. 15]** données qui sont indispensables pour faire la lumière sur les actes indiqués. Le point de vue de la défenderesse selon lequel la circonstance de l'utilisation de services d'accès à Internet ou de services téléphoniques doit déjà

être considérée comme un motif suffisant de procéder à la conservation n'est manifestement pas conforme à ces règles. La thèse de l'incompatibilité générale avec le droit de l'Union de toute conservation de données sans motif, qui ressort des motifs de la Cour, n'est pas non plus remise en cause par la référence de la défenderesse à l'avis 1/15 rendu ultérieurement – le 26 juillet 2017 – par la Cour sur l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers. La Cour a certes souligné, dans le cadre de l'examen du caractère nécessaire des ingérences que comporte l'accord dans les droits fondamentaux au respect de la vie privée et familiale (article 7 de la Charte) et à la protection des données à caractère personnel (article 8 de la Charte), que le transfert des données dites PNR (Passenger Name Records) vers le Canada a lieu indépendamment de tout élément objectif permettant de considérer que les passagers sont susceptibles de présenter un risque pour la sécurité publique au Canada [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), point 186]. Il ne s'agit cependant pas d'une conservation des données sans motif, dès lors que la conservation et le transfert sont liés aux contrôles aux frontières auxquels l'ensemble des passagers aériens désireux d'entrer au Canada ou de sortir de ce pays sont soumis, en vertu du droit canadien en vigueur [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592), point 188]. Ce motif de conservation disparaît lors du départ des passagers aériens. Il ressort du point 3, sous d), du dispositif de l'avis que la conservation des données au-delà de cette date suppose par conséquent – à titre de nouveau motif – qu'il existe des éléments objectifs permettant de considérer que les passagers aériens en question pourraient présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave.

25 bb) S'il y a lieu d'interpréter la jurisprudence de la Cour en ce sens qu'une conservation des données sans motif ne saurait en aucun cas être compatible avec le droit de l'Union, le recours en « Revision » de la défenderesse contre l'arrêt attaqué du Verwaltungsgericht (tribunal administratif) est voué à l'échec. En effet, tout comme les réglementations suédoise et britannique en matière de conservation des données sur lesquelles portait l'arrêt de la Cour du 21 décembre 2016, les dispositions combinées de l'article 113a, paragraphe 1, **[Or. 16]** première phrase, et de l'article 113b du TKG n'exigent – outre la simple utilisation de services d'accès à Internet ou de services téléphoniques – ni un motif pour la conservation ni un lien entre les données conservées et une infraction pénale ou un risque pour la sécurité publique. Il s'agit au contraire d'une réglementation qui impose la conservation, sans motif, généralisée et non différenciée d'un point de vue personnel, temporel et géographique, de la majeure partie de toutes les données pertinentes relatives au trafic qui sont afférentes à des télécommunications.

26 cc) Toutefois, la chambre de céans considère, en dépit des formulations précitées figurant dans l'arrêt de la Cour du 21 décembre 2016, qu'il n'est pas exclu que l'obligation, régie par les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG, de conserver sans motif les données relatives au trafic qui sont afférentes à des télécommunications

puisse être fondée sur l'article 15, paragraphe 1, de la directive 2002/58/CE. Cette appréciation repose sur les considérations suivantes :

27 (1) Il y a lieu de constater tout d'abord que les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG n'exigent pas la conservation de l'ensemble des données relatives au trafic qui sont afférentes aux télécommunications de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, au sens de la jurisprudence de la Cour qui portait sur la directive antérieure, la directive 2006/24/CE, et sur les réglementations suédoise et britannique fondées sur celle-ci. Non seulement le contenu de la communication est exclu de l'obligation de conservation, mais les données relatives aux sites Internet consultés, les données des services de courrier électronique et les données qui sous-tendent les communications à caractère social ou religieux vers ou à partir de certaines lignes ne peuvent être conservées (voir article 113b, paragraphes 5 et 6, du TKG). La chambre de céans ne saurait se ranger d'emblée à l'avis du Verwaltungsgericht (tribunal administratif) selon lequel les différences par rapport aux réglementations suédoise et britannique sur lesquelles portait l'arrêt susmentionné de la Cour du 21 décembre 2016 n'étaient pas déterminantes eu égard aux conditions auxquelles la Cour a subordonné la licéité de règles nationales en matière de conservation des données relatives au trafic qui sont afférentes aux télécommunications. En effet, la Cour a souligné, à l'appui de sa décision, que la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication **[Or. 17]** électronique était susceptible de permettre d'en 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. Il est ainsi possible 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 (arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 99). Si certains moyens de communication ou catégories de données, en particulier, sont exclus de l'obligation de conservation, cela ne suffit certes pas à éliminer le risque de l'établissement d'un profil complet des personnes concernées, mais cela le réduit tout au moins considérablement.

28 (2) Une différence encore plus importante entre les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG, d'une part, et la directive précédente, la directive 2006/24/CE, sur laquelle les réglementations suédoise et britannique en matière de conservation des données étaient fondées, d'autre part, réside dans le fait que la durée de conservation comprise entre six mois et deux ans (voir article 6 de la directive 2006/24/CE) est nettement réduite par l'article 113b, paragraphe 1, du TKG, en vertu duquel elle est comprise entre quatre et dix semaines. Or, il y a lieu de considérer que le

risque de l'établissement d'un profil complet des personnes concernées, souligné par la Cour, est d'autant plus faible que les périodes au cours desquelles les données relatives au trafic sont conservées sont courtes. Ce n'est qu'en compilant les différentes données pendant une longue période que l'on peut en tirer, selon la jurisprudence de la Cour, des conclusions suffisamment fiables sur les habitudes, les lieux de séjour, les déplacements, les activités exercées, les relations sociales des personnes concernées et les milieux sociaux fréquentés par celles-ci. Plus la durée de conservation est courte, plus le profil de personnalité est nécessairement lacunaire et plus l'ingérence dans les droits fondamentaux est faible.

29 (3) Il faut également tenir compte du fait que les dispositions introduites par la loi du 10 décembre 2015 comportent des limitations strictes pour ce qui est de la protection des données conservées et de l'accès à celles-ci. D'une part, les prescriptions des articles 113d et suivants du TKG garantissent une protection efficace des **[Or. 18]** données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données. D'autre part, les données conservées ne peuvent, aux termes de l'article 113c, paragraphe 1, du TKG, être utilisées qu'aux fins de la lutte contre les infractions graves ou aux fins de la prévention d'un risque concret pour l'intégrité physique, la vie ou la liberté d'une personne ou bien pour l'existence de l'État fédéral ou d'un Land. La collecte de données relatives au trafic à des fins répressives suppose, en vertu de l'article 100g, paragraphe 2, de la StPO, qu'il existe un soupçon relatif à l'une des infractions pénales particulièrement graves limitativement énumérées dans la loi, que l'infraction soit également particulièrement grave dans le cas particulier, que l'enquête sur les faits ou la localisation de la personne faisant l'objet de l'enquête par d'autres moyens seraient excessivement difficiles ou vouées à l'échec et que la collecte des données soit proportionnée à l'importance de l'affaire. La collecte ou l'utilisation de données relatives au trafic qui concernent les personnes tenues au secret professionnel qui sont visées à l'article 53, paragraphe 1, premier alinéa, point 1 à 5, de la StPO, lesquelles comprennent notamment les avocats, les médecins ou les journalistes, est interdite en vertu de l'article 100g, paragraphe 4, de la StPO. L'article 101a, paragraphe 1, de la StPO soumet en outre la collecte de données relatives au trafic conformément à l'article 100g de la StPO à une autorisation du juge [omissis]. En vertu de l'article 101a, paragraphe 2, de la StPO, les motifs de la décision doivent comporter les considérations essentielles relatives au caractère nécessaire et approprié de la mesure dans le cas particulier en question. L'article 101a, paragraphe 6, de la StPO prévoit une obligation d'informer les participants à la télécommunication concernée.

30 Certes, ces dispositions restrictives de l'accès ne s'appliquent pas à l'adresse IP attribuée à l'abonné pour l'utilisation d'Internet ; en effet, aux termes de l'article 113c, paragraphe 1, point 3, du TKG, celle-ci peut également être utilisée dans le cadre de la fourniture d'informations sur des données relatives à l'abonné aux fins de la répression d'une infraction pénale, quelle qu'elle soit, de la prévention des risques pour la sécurité et l'ordre publics ainsi que, de manière générale, aux fins de l'exercice des missions des services de renseignement. Il convient toutefois de partir de l'idée que le fait d'indiquer quel titulaire de la

connexion était abonné à Internet sous quelle adresse IP déjà connue ne permet pas d'établir des profils de personnalité ou de déplacement [omissis]. Même à supposer, comme le fait la requérante, que des procédés techniques dans le cadre desquels une adresse IP ne peut plus être clairement rattachée à une certaine connexion de télécommunications, **[Or. 19]** mais peut uniquement l'être à un plus grand groupe de connexions, soient de plus en plus utilisés, si bien que la fourniture d'informations sur les données relatives à l'abonné est devenue une mesure assortie d'un spectre considérable de possibilités, l'ingérence impliquée par une telle fourniture d'informations sur les données relatives à l'abonné est bien moindre que celle qui découle de la consultation et de l'utilisation des données relatives au trafic qui sont afférentes aux télécommunications.

31 (4) La thèse selon laquelle l'obligation de conservation, sans motif, des données relatives au trafic et afférentes aux télécommunications, qui est régie par les dispositions combinées de l'article 113a, paragraphe 1, première phrase, et de l'article 113b du TKG, pourrait, eu égard aux limitations exposées, être fondée sur l'article 15, paragraphe 1, de la directive 2002/58/CE est corroborée, dans le cadre d'une appréciation globale et en sus des dispositions restrictives relatives aux moyens de communication, aux catégories de données et aux durées de conservation visés, ainsi que des prescriptions strictes en matière de sécurité des données et de consultation de celles-ci, par le fait que le législateur national s'est ainsi acquitté des obligations d'agir qui découlent, pour les États membres, du droit à la sécurité garanti par l'article 6 de la Charte.

32 Dans son arrêt du 8 avril 2014, qui concernait la validité de la directive 2006/24/CE, la Cour a expressément mentionné l'article 6 de la Charte et a rappelé dans ce contexte, en se référant à sa jurisprudence, que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales et qu'il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 42). La Cour a cependant également indiqué que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et que son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, selon la Cour, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24/CE soit considérée comme nécessaire aux fins de ladite lutte **[Or. 20]** (arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 51 et 60, ainsi que du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 101 et 102).

33 En ce qui concerne l'obligation d'agir des États membres qui découle de l'article 6 de la Charte, la juridiction de céans s'interroge sur le point de savoir si cette affirmation de la Cour doit être comprise en ce sens que c'est uniquement lorsqu'elle est aménagée comme elle l'était dans le cadre de la directive

2006/24/CE et des réglementations suédoise et britannique qui la transposaient qu'une conservation des données sans motif ne peut pas être fondée sur l'article 15, paragraphe 1, de la directive 2002/58/CE ou si elle ne peut pas être fondée sur cet article de manière générale. En effet, le principe de base de la conservation des données est difficilement conciliable avec l'exigence, formulée sans réserves par la Cour, selon laquelle il convient, pour ce qui est des données à conserver, d'opérer une distinction en fonction des personnes, des périodes et des zones géographiques (voir déjà, en ce sens, conclusions de l'avocat général Saugmandsgaard Øe dans les affaires jointes Tele2 Sverige e.a., C-203/15 et C-698/15, EU:C:2016:572, points 213 et suivants). Une telle distinction ne peut, par nature, être opérée que pour l'avenir, dès lors que l'on dispose déjà de certains éléments. Or, la conservation des données a précisément pour but de reconstituer des faits anciens sur la base des données relatives au trafic et afférentes aux télécommunications qui sont déjà disponibles au moment où le motif est invoqué. Il est possible que ce but ne puisse pas être atteint s'il faut par exemple opérer une distinction en fonction des personnes – notamment en observant le comportement en matière de communication sur les réseaux sociaux – qui sont jugées capables de commettre des infractions graves, ou si, d'un point de vue géographique, seules peuvent être visées les cellules comportant des installations pour lesquelles il existe, en raison d'éléments concrets, un risque élevé de passage à l'acte ou un potentiel de nuisance important. En particulier, une limitation géographique n'est précisément guère appropriée pour des infractions pénales qui sont commises au moyen de services de télécommunications électroniques.

34 De l'avis de la chambre de céans, la thèse selon laquelle la conservation sans motif de données relatives au trafic est en elle-même incompatible avec la Charte est infirmée en outre par la nécessité de définir un point d'équilibre entre l'obligation incombant aux États membres d'assurer la sécurité des individus se trouvant sur leur territoire et le respect des droits fondamentaux à la vie privée et à la protection des données à caractère personnel **[Or. 21]** consacrés aux articles 7 et 8 de la Charte (voir conclusions de l'avocat général Saugmandsgaard Øe dans les affaires jointes Tele2 Sverige e.a., C-203/15 et C-698/15, EU:C:2016:572, points 5 et 163). Selon la chambre de céans, il ne ressort donc pas clairement de la jurisprudence de la Cour qu'il ne serait plus possible au législateur national d'introduire une conservation des données sans motif – le cas échéant assortie de dispositions strictes en matière d'accès – dans le cadre d'une appréciation d'ensemble, afin de tenir compte des risques potentiels spécifiques liés aux nouveaux moyens de télécommunication [omissis].

35 (5) S'il convenait d'interpréter la jurisprudence précitée de la Cour en ce sens qu'une conservation des données sans motif ne peut pas, de manière générale, être fondée sur l'article 15, paragraphe 1, de la directive 2002/58/CE et que les dispositions concrètes relatives aux moyens de communication visés, aux catégories de données à conserver, à la durée de conservation, aux conditions d'accès aux données conservées et à la prévention des risques d'abus importent dès lors peu, cela restreindrait considérablement la marge de manœuvre du législateur national dans un domaine touchant à la répression et à la sécurité

publique, lequel reste en tout cas en principe, aux termes de l'article 4, paragraphe 2, troisième phrase, TUE, de la seule responsabilité de chaque État membre. Dans ce domaine, il appartient – comme nous l'avons indiqué – au législateur national de définir un point d'équilibre entre le respect des droits fondamentaux à la vie privée et à la protection des données à caractère personnel et l'obligation incombant aux États membres d'assurer la sécurité de leur population. Selon la chambre de céans, il ne ressort pas de manière certaine de la décision de la Cour du 21 décembre 2016 que la possibilité d'introduire, lorsque cela est jugé nécessaire, une technique d'enquête telle que la conservation des données sans motif dans le domaine de la répression et de la sécurité publique, sur le fondement de l'article 15, paragraphe 1, de la directive 2002/58/CE, devrait être totalement refusée aux organes législatifs des États membres, qui bénéficient d'une légitimité démocratique, indépendamment de la nature des risques et de la forme concrète des dispositions. **[Or. 22]**

36 (6) La chambre de céans considère que le point de savoir si les motifs de la Cour dans l'arrêt du 21 décembre 2016 doivent être interprétés comme interdisant aux États membres de se fonder sur l'article 15, paragraphe 1, de la directive 2002/58/CE pour introduire une obligation de conserver, sans motif, les données relatives au trafic qui sont afférentes aux télécommunications n'a pas été définitivement tranché, et ce notamment au regard de la jurisprudence récente de la Cour européenne des droits de l'homme. En effet, la Cour européenne des droits de l'homme a récemment jugé, dans un arrêt du 19 juin 2018, que les dispositions suédoises relatives à l'interception massive des flux transfrontières de données étaient conformes à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la « CEDH »). Compte tenu des menaces auxquelles sont confrontés de nombreux États (dont le fléau du terrorisme international et d'autres formes graves de criminalité telles que le trafic de stupéfiants, la traite d'êtres humains, l'exploitation sexuelle des enfants et la cybercriminalité), des progrès technologiques qui permettent aux terroristes et aux criminels d'échapper plus facilement à la détection sur Internet et de l'impossibilité de prévoir les voies par lesquelles les communications électroniques seront transmises, la Cour européenne des droits de l'homme a considéré que la décision de recourir à un régime d'interception massive afin de repérer des menaces jusqu'alors inconnues pour la sécurité nationale relevait toujours de la marge d'appréciation des États (Cour EDH, 19 juin 2018, Centrum för Rättvisa c. Suède, CE:ECHR:2018:0619JUD003525208, § 112). En se référant à l'impossibilité de prévoir les voies par lesquelles les communications électroniques seront transmises et aux progrès technologiques qui permettent aux terroristes et aux criminels d'échapper plus facilement à la détection sur Internet, la Cour européenne des droits de l'homme souligne avec encore plus de force que la Cour de justice de l'Union européenne les risques potentiels spécifiques qui sont liés aux nouveaux moyens de télécommunication.

37 De l'avis de la chambre de céans, il n'est pas possible de ne pas tenir compte en l'espèce de la jurisprudence de la Cour européenne des droits de l'homme,

laquelle met l'accent sur des aspects différents. En effet, le considérant 11 de la directive 2002/58/CE souligne, d'une part, que des mesures telles que celles visées à l'article 15, paragraphe 1, de la directive doivent respecter la CEDH, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. D'autre part, la Cour de justice de l'Union européenne a itérativement relevé que, **[Or. 23]** dans la mesure où la Charte contient des droits correspondant à des droits garantis par la CEDH, l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans celle-ci et les droits correspondants garantis par la CEDH, sans que cela porte atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne (voir arrêt du 29 juillet 2019, Funke Medien NRW, C-469/17, EU:C:2019:623, point 73 et jurisprudence citée).

38 (7) Enfin, il ressort de plusieurs demandes de décision préjudicielle émanant d'autres États membres dans le cadre d'affaires pendantes devant la Cour que les juridictions de renvoi s'interrogent, notamment au regard de l'article 6 de la Charte et de l'article 4 TUE, sur le point de savoir si les motifs de la Cour dans l'arrêt du 21 décembre 2016 doivent être interprétés comme une interdiction générale de la conservation sans motif des données, à laquelle il ne peut être dérogé ni au vu de la pertinence des risques combattus pour la sécurité publique ni dans le cadre d'une « compensation » par des dispositions restrictives de l'accès et des exigences strictes en matière de sécurité. La chambre de céans se réfère à cet égard à la demande de décision préjudicielle introduite par le Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête) de Londres (Royaume-Uni) qui a donné lieu à l'affaire pendante devant la Cour sous le numéro C-623/17 (JO 2018, C 22, p. 29), aux deux demandes de décision préjudicielle du Conseil d'État (France) qui ont donné lieu aux affaires pendantes devant la Cour sous les numéros C-511/18 et C-512/18 (JO 2018, C 392, p. 7), ainsi qu'à la demande de décision préjudicielle de la Cour constitutionnelle (Belgique) qui a donné lieu à l'affaire pendante devant la Cour sous le numéro C-520/18 (JO 2018, C 408, p. 39).

[omissis]