ECLI:EU:C:2021:939

Édition provisoire

CONCLUSIONS DE L'AVOCAT GÉNÉRAL

M. MANUEL CAMPOS SÁNCHEZ-BORDONA

présentées le 18 novembre 2021 (1)

Affaires jointes C-793/19 et C-794/19

République fédérale d'Allemagne

contre

SpaceNet AG (C-793/19) contre

Telekom Deutschland GmbH (C-794/19) contre

[Demandes de décision préjudicielle formées par le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne)]

« Renvoi préjudiciel – Télécommunications – Traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques – Directive 2002/58/CE – Article 15, paragraphe 1 – Article 4, paragraphe 2, TUE – Charte des droits fondamentaux de l'Union européenne – Articles 6, 7, 8, 11 et 52, paragraphe 1 – Conservation généralisée et indifférenciée des données de connexion aux fins de la répression des infractions pénales graves ou de la prévention d'un risque concret pour la sécurité nationale »

1. Les demandes de décision préjudicielle dans les présentes affaires, auxquelles s'ajoute celle qui a été présentée dans l'affaire C-140/20 (2), témoignent, encore une fois, de la préoccupation que suscite dans certains États membres la jurisprudence de la Cour sur la conservation des données à caractère personnel générées dans le secteur des communications électroniques et l'accès à ces données.

2. Dans mes conclusions présentées dans les affaires C-511/18 et C-512/18, La Quadrature du Net e.a. (3), et C-520/18, Ordre des barreaux francophones et germanophone e.a. (4), j'ai mentionné les arrêts suivants comme constituant, jusqu'alors, les jalons les plus importants de cette jurisprudence :

— L'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (5), dans lequel la Cour a déclaré l'invalidité de la directive 2006/24/CE (6) en ce que celle-ci prévoyait une ingérence disproportionnée dans les droits reconnus par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

— L'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (7), dans lequel la Cour a jugé que l'article 15, paragraphe 1, de la directive 2002/58/CE (8) s'opposait à une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave.

— L'arrêt du 2 octobre 2018, Ministerio Fiscal (9), qui a confirmé l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, en précisant l'importance du principe de proportionnalité à cet égard.

3. En 2018, quelques juridictions de certains États membres se sont adressées à la Cour, dans le cadre de demandes de décision préjudicielle, en faisant part de leurs doutes quant à la question de savoir si ces arrêts (de 2014, 2016 et 2018) étaient susceptibles de déposséder les autorités étatiques d'un instrument nécessaire à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité et le terrorisme.

4. Quatre de ces demandes de décision préjudicielle ont donné lieu aux arrêts Privacy International (10) et La Quadrature du Net e.a. (11), tous deux du 6 octobre 2020, qui ont corroboré, en substance, la jurisprudence issue de l'arrêt Tele2 Sverige, tout en introduisant certaines nuances complémentaires.

5. Du fait de leur origine (la grande chambre de la Cour), de leur contenu et du souci de la Cour d'y expliquer en détail, dans le cadre d'un dialogue avec les juridictions de renvoi, les raisons qui, malgré tout, étayent les thèses qui y sont exposées, on pourrait s'attendre à ce que ces deux arrêts « récapitulatifs » du 6 octobre 2020 aient clos le débat. Toute autre demande de décision préjudicielle portant sur le même sujet donnerait ainsi lieu à une ordonnance motivée conformément à l'article 99 du règlement de procédure de la Cour.

6. Cependant, avant le 6 octobre 2020, trois autres demandes de décision préjudicielle (les deux jointes dans la présente procédure et celle dans l'affaire C-140/20), qui, par leur contenu, remettaient à nouveau en cause la jurisprudence relative à l'article 15, paragraphe 1, de la directive 2002/58, étaient parvenues à la Cour.

7. La Cour a fait part aux juridictions de renvoi des arrêts du 6 octobre 2020, dans l'optique de leur demander si elles souhaitaient retirer leur demande de décision préjudicielle. Compte tenu de leur insistance à les maintenir, comme je l'exposerai dans les développements suivants (12), il a été décidé que l'article 99 du règlement de procédure ne serait pas appliqué et que la grande chambre de la Cour y répondrait.

I. Cadre juridique

A. Le droit de l'Union : La directive 2002/58

8. Selon l'article 5, paragraphe 1 (« Confidentialité des communications ») :

« 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. En particulier, ils 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. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité ».

9. Conformément à l'article 6 (« Données relatives au trafic ») :

« 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

[…] ».

10. L'article 15 (« Application de certaines dispositions de la directive 95/46/CE ») (13), prévoit, à son paragraphe 1 :

« 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. **Le droit national**

1. ***Telekommunikationsgesetz (loi sur les télécommunications) ; ci-après le « TKG »)***

11. En vertu de l'article 113a, paragraphe 1, du TKG :

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

12. L'article 113b énonce :

« (1) les opérateurs visés à l'article 113a 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, avec indication du fuseau horaire,

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,

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, pour les services de téléphonie par Internet, les adresses IP (protocole Internet) de la ligne 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 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 sans réponse ou infructueux en raison d'une intervention du gestionnaire de réseau [...].

(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, avec indication du fuseau horaire.

(4) En cas d'utilisation de services de téléphonie mobile, il convient de conserver la désignation des cellules qui ont été utilisées par l'appelant et l'appelé au début de la communication. En ce qui concerne les services d'accès à Internet accessibles au public, il convient 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 de 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 (14) .

[…] ».

13. Aux termes de l'article 113c :

« (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 du *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.

[...] ».

14. Aux termes de l'article 113d :

« Le débiteur de l'obligation visée 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, dans des systèmes informatiques de traitement de données découplés,

4. la restriction de l'accès aux installations utilisées pour le traitement des 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 ».

15. L'article 113^{e} 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 visée à l'article 113a, paragraphe 1 doit veiller à ce que les données consignées soient effacées au bout d'un an ».

2. ***Strafprozessordnung (code de procédure pénale, ci-après la « StPO »)***

16. L'article 100g prévoit :

« [...]

(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 à la deuxième phrase ou, dans les cas où la tentative d'infraction est punissable, a tenté de commettre une infraction et si l'infraction est également particulièrement grave dans le cas particulier, les données relatives au trafic conservées conformément à l'article 113b du [TKG], 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 […] 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, soumet la collecte de données relatives au trafic conformément à l'article 100g de la StPO à autorisation du juge. En vertu de l'article 101a, paragraphe 2, de cette même loi, la décision du juge doit mettre en balance la nécessité et la pertinence de la mesure dans le cas particulier, dont l'adoption doit être notifiée aux participants à la communication (article 101, paragraphe 6, de la StPO).

II. **Faits, procédure et questions préjudicielles**

18. SpaceNet AG et Telekom Deutschland GmbH sont des sociétés qui fournissent, en République fédérale d'Allemagne, des services d'accès à Internet accessibles au public.

19. Ces deux sociétés ont saisi le Verwaltungsgericht (tribunal administratif, Allemagne) en s'opposant à l'obligation de stocker les données relatives au trafic des télécommunications de leurs clients à partir du 1er juillet 2017, imposée par l'article 113a, paragraphe 1, lu en combinaison avec l'article 113b, du TKG.

20. Ces parties ayant obtenu gain de cause en première instance, l'Agence fédérale des réseaux a introduit des recours en « Revision » devant le Bundesverwaltungsgericht (Cour administrative fédérale), qui, avant de rendre son arrêt, a décidé de poser, dans chacune des deux procédures, la question préjudicielle 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,

— 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 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, et

— 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 ? »

21. Ainsi que l'explique la juridiction de renvoi, la réglementation de l'obligation litigieuse a été modifiée par une loi du 10 décembre 2015 (15), dont l'adoption était nécessaire après :

— l'arrêt du Bundesverfassungsgericht (Cour constitutionnelle fédérale, Allemagne) du 2 mars 2010 (16) déclarant inconstitutionnelles les dispositions antérieures relatives à la conservation des données ; et

— la déclaration de nullité de la directive 2006/24, pour la transposition de laquelle ces dispositions avaient été adoptées.

22. La juridiction de renvoi considère que l'obligation de stockage litigieuse porte atteinte aux droits prévus aux articles 5, paragraphe 1, 6, paragraphe 1, et 9, paragraphe 1, de la directive 2002/58. Elle estime que cette restriction ne serait justifiée que si elle pouvait s'appuyer sur l'article 15, paragraphe 1, de la directive 2002/58.

23. Pour la juridiction de renvoi, nonobstant la jurisprudence tirée de l'arrêt Tele2 Sverige, l'obligation litigieuse pourrait trouver son fondement dans l'article 15, paragraphe 1, de la directive 2002/58, car :

— Les règles nationales applicables n'exigent pas le stockage de toutes les données relatives au trafic de télécommunications de *tous* les utilisateurs et abonnés pour *tous* les moyens de communication électroniques.

— Ces règles ont substantiellement réduit (jusqu'à un maximum de dix semaines) le délai de stockage par rapport à celui prévu par les législations analysées dans l'arrêt Tele2 Sverige et celui visé dans la directive 2006/24, ce qui rend l'élaboration de profils plus difficile.

— Des limitations strictes ont été imposées en matière de protection, d'accès et d'utilisation des données stockées.

— Le législateur se serait borné à remplir les devoirs d'action qu'impose le droit à la sûreté (article 6 de la Charte) (17).

— Si, d'une manière générale, le stockage de données « sans motif » (18) ne pouvait pas relever de l'article 15, paragraphe 1, de la directive 2002/58 (c'est-à-dire si les modalités de la réglementation relative aux moyens de télécommunication concernés, aux types de données stockées, à la durée du stockage, aux conditions d'accès à ces données et à la protection contre les risques d'utilisation abusive, importaient peu), la marge d'action conférée au législateur national dans un domaine qui, comme celui de la poursuite des infractions et de la sécurité publique, reste, conformément à l'article 4, paragraphe 2, troisième phrase, TUE, de la seule responsabilité des États membres, serait substantiellement réduite.

— Il convient de veiller à la cohérence entre les droits garantis par la Charte et ceux consacrés par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la « CEDH »), interprétés par la Cour européenne des droits de l'homme (ci-après la « Cour EDH »), sans préjudice de l'autonomie du droit de l'Union et de l'autorité de la Cour de justice.

III. **La procédure devant la Cour**

24. Les demandes de décision préjudicielle ont été enregistrées à la Cour le 29 octobre 2019.

25. Des observations écrites ont été déposées par SpaceNet, Telekom Deutschland, les gouvernements allemand, danois, espagnol, estonien, finlandais, français, irlandais, néerlandais, polonais et suédois, ainsi que par la Commission.

26. La juridiction de renvoi ayant été invitée à se prononcer sur l'éventuel retrait de la demande préjudicielle à la suite du prononcé de l'arrêt La Quadrature du Net, elle a, le 13 janvier 2021, exprimé son intention de la maintenir, au motif que l'on ne pouvait pas considérer qu'elle était tranchée par cet arrêt.

27. L'audience publique, qui s'est tenue conjointement avec celle de l'affaire connexe C-140/20, a eu lieu le 13 septembre 2021, et, outre les intervenants ayant présenté des observations écrites dans cette procédure, l'Agence fédérale des réseaux et le Contrôleur européen de la protection des données ont comparu.

IV. **Analyse**

A. **Considérations préliminaires**

28. Le traitement de ces deux demandes de décision préjudicielle peut être effectué soit en les analysant telles qu'elles ont été présentées initialement, soit au regard des considérations que la juridiction de renvoi a invoquées en répondant à la Cour le 13 janvier 2021 pour justifier le maintien de sa demande, après avoir pris connaissance de l'arrêt La Quadrature du Net.

29. Même si j'aborde succinctement les points les plus pertinents des demandes initiales de décision préjudicielle, je me concentrerai sur l'analyse des raisons pour lesquelles la juridiction de renvoi estime que l'intervention de la Cour reste pertinente. En résumé, toutes ces raisons reposent

sur l'idée que la situation réglementaire de base diffère de celle qui est examinée dans l'arrêt La Quadrature du Net.

30. Dans sa communication du 13 janvier 2021, la juridiction de renvoi a fait valoir les arguments suivants :

— Les différences entre les normes allemandes et les normes françaises et belges ayant donné lieu à l'arrêt La Quadrature du Net sont sensibles. Aux termes des premières, les données relatives aux sites Internet consultés, les données des services de courrier électronique et les données qui sous-tendent les communications vers ou à partir de certaines lignes à caractère social ou religieux ne peuvent être conservées.

— Une autre différence encore plus importante réside dans le fait que la durée de conservation prévue à l'article 113b, paragraphe 1, du TKG est de quatre ou dix semaines, et non d'un an. Ce facteur réduit le risque d'établissement d'un profil global des personnes concernées.

— Les normes allemandes assurent une protection efficace des données conservées contre les risques d'abus et d'accès illicite.

— Depuis une récente décision du Bundesverfassungsgericht (Cour constitutionnelle fédérale) sur l'article 113 du TKG (19), la validité de cette disposition aurait été soumise à des conditions dont la compatibilité avec le droit de l'Union ne serait pas facile à déterminer.

— Des incertitudes subsistent en ce qui concerne les exigences du droit de l'Union en matière d'adresses IP, dans la mesure où il ne ressort pas clairement de l'arrêt La Quadrature du Net si leur conservation est exclue d'une manière générale, une certaine tension étant observée entre ses points 168 et 155.

B. **Applicabilité de la directive 2002/58**

31. La République d'Irlande ainsi que les gouvernements français, néerlandais, polonais et suédois soutiennent, en substance, que la directive 2002/58 ne s'applique pas à des réglementations nationales telles que celle en cause dans ces litiges. Ces réglementations ayant pour objet la protection de la sécurité nationale ainsi que la prévention et la répression des infractions pénales graves, elles relèvent de la compétence exclusive des États membres, conformément à l'article 4, paragraphe 2, TUE.

32. La Cour a rejeté l'objection sans équivoque dans l'arrêt La Quadrature du Net en déclarant qu'« une réglementation nationale imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et des données de localisation aux fins de la protection de la sécurité nationale et de la lutte contre la criminalité, telle que celles en cause au principal, relève du champ d'application de la directive 2002/58 » (20).

33. La juridiction de renvoi se fonde sur cette prémisse en corroborant l'appréciation de la juridiction de première instance et en ajoutant que l'applicabilité de la directive 2005/58 dans cette hypothèse avait été « établie de manière définitive » par l'arrêt Tele2 Sverige (21).

34. Je ne m'étendrai donc pas sur ce point, sur lequel j'ai eu l'occasion de m'exprimer à l'époque, conformément à la ligne adoptée par la Cour, dans le cadre des conclusions La Quadrature du Net (22).

C. **Conservation généralisée et indifférenciée *par opposition à* conservation ciblée des données relatives au trafic et des données de localisation.**

35. L'idée qui est au cœur de la jurisprudence de la Cour concernant la directive 2002/58 est 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 anonymes et ne puissent pas faire l'objet d'un enregistrement, sauf s'ils y consentent (23).

36. L'article 15, paragraphe 1, de la directive 2002/58 admet des dérogations à l'obligation de garantir la confidentialité et aux obligations y afférentes, dans les conditions que j'exposerai dans les développements suivants. Dans l'arrêt La Quadrature du Net, la Cour procède à l'examen approfondi de la conciliation de ces dérogations avec les droits fondamentaux dont l'exercice est susceptible d'être affecté (24).

37. La conservation généralisée et indifférenciée des données relatives au trafic ne pourrait être justifiée, selon la Cour, que par l'objectif de sauvegarde de la sécurité nationale, dont l'importance « dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58 ».(25)

38. Dans ce cas (sécurité nationale), la Cour a jugé 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, « 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 […] pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible » (26).

39. Il est certain que ces prescriptions donnent lieu à un régime plus rigoureux et plus strict que celui qui ressort de la jurisprudence de la Cour EDH lue en combinaison avec l'article 8 de la CEDH. Le fait que « [le] sens et [la] portée des droits » de la Charte correspondant à ceux de la CEDH doivent être les mêmes que ceux que leur confère cette dernière, ne fait pas obstacle, conformément à l'article 52, paragraphe 3, in fine, de la Charte, à ce que le droit de l'Union accorde une protection plus étendue.

40. Au demeurant, la jurisprudence de la Cour EDH issue de ses arrêts du 25 mai 2021, Big Brother Watch e.a. c. Royaume-Uni (27) et Centrum för Rättvisa c. Suède (28), ainsi que de celui du 4 décembre 2015, Zakharov c. Russie (29), concerne des cas de figure qui, comme il a été majoritairement soutenu lors de l'audience, ne sont pas comparables à ceux qui sont débattus dans le cadre des renvois préjudiciels en cause ici. La solution à ces derniers doit être trouvée en appliquant des normes nationales réputées conformes à la réglementation *exhaustive* de la directive 2002/58, telle qu'interprétée par la Cour de justice.

41. Quoi qu'on pense de l'invocation de la sécurité nationale, dans l'arrêt La Quadrature du Net, comme motif pour lever, sous certaines conditions, l'interdiction de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (les limites fixées par la Cour me semblent excessivement larges), les prescriptions énumérées aux points 137 à 139 de cet arrêt doivent être respectées.

42. En dehors de cette hypothèse, il conviendra d'examiner si la réglementation nationale repose sur des critères suffisamment *sélectifs* pour satisfaire aux conditions qui, conformément à la

jurisprudence de la Cour, peuvent justifier une ingérence particulièrement grave, telle que la conservation de données, dans les droits fondamentaux concernés.

43. La *conservation ciblée* des données relatives au trafic et des données de localisation (30) est la pierre angulaire du raisonnement des arrêts de la Cour en la matière. Cette délimitation peut se faire, entre autres, en fonction des catégories de personnes concernées (31) ou être fondée sur un critère géographique (32).

44. Tant la juridiction de renvoi que la plupart des parties ayant présenté des observations s'accordent pour souligner les difficultés que comportent les critères indiqués par la Cour. J'ai moi-même signalé certaines de ces difficultés (33) dans les conclusions Ordre des barreaux francophones et germanophone (34).

45. Or, il ne faut pas exclure certaines formules de conservation ciblées fondées sur ces critères qui pourraient être efficaces tout en étant non discriminatoires. Il appartient aux législateurs nationaux, et non à la Cour, de les concevoir d'une manière qui soit respectueuse des droits fondamentaux garantis par la Charte (35).

46. J'insiste, par ailleurs, sur le fait qu'il serait erroné de considérer que les critères d'ordre personnel et géographique sont les seuls compatibles avec l'article 15, paragraphe 1, de la directive 2002/58, au regard des droits protégés dans la Charte.

47. Même si le gouvernement français soutient qu'elles se sont avérées inefficaces (36), je ne crois pas non plus que l'on puisse négliger les modalités proposées par les groupes de travail réunis au sein du Conseil (37) pour définir des règles de conservation et d'accès compatibles avec la jurisprudence de la Cour (38).

48. Selon moi, il convient de favoriser la conservation temporaire de certaines *catégories* de données relatives au trafic et de données de localisation, limitées en fonction de ce qui est strictement nécessaire pour atteindre l'objectif poursuivi, qui ne permettent pas, prises ensemble, d'obtenir une image précise et détaillée de la vie des personnes concernées. En pratique, cela signifie que, pour les deux principales catégories (les données relatives au trafic et les données de localisation), seules les données *minimales* considérées comme absolument indispensables pour la prévention et le contrôle efficaces de la criminalité et pour la sauvegarde de la sécurité nationale devraient être conservées, au moyen de filtres appropriés (39).

49. En tout état de cause, je le répète, il appartient aux États membres ou aux institutions de l'Union de procéder à cet exercice de sélection par voie législative (avec l'aide de leurs propres experts), en renonçant à toute tentative d'imposer une conservation généralisée et indifférenciée de toutes les données relatives au trafic et données de localisation (40).

50. C'est pourquoi, dans les conclusions Ordre des barreaux francophones et germanophone, j'affirmais que « la difficulté législative – que je reconnais – de définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne justifie pas que les États membres, en faisant de l'exception une règle, érigent la conservation généralisée des données personnelles en principe central de leur législation. Si tel était le cas, une atteinte importante d'une durée indéterminée au droit à la protection des données à caractère personnel serait admise » (41).

D. **Point 168 de l'arrêt La Quadrature du Net**

51. Dans ce contexte, les éléments indispensables pour répondre à la juridiction de renvoi découlent, selon moi, directement de la jurisprudence de la Cour relative à l'article 15, paragraphe 1, de la directive 2002/58, qui est récapitulée dans l'arrêt La Quadrature du Net.

52. Ainsi, je me dois, tout d'abord, de rappeler la jurisprudence de la Cour dans cet arrêt, que le point 168 résume comme suit :

« L'article 15, paragraphe 1, de la directive 2002/58, lu en combinaison avec les articles 7, 8, 11 et 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues audit 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 ».

E. Évaluation de la législation litigieuse dans ces renvois préjudiciels à la lumière de l'arrêt La Quadrature du Net

53. Selon la juridiction de renvoi, à qui son interprétation incombe exclusivement, la législation allemande 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 » (42).

54. La réglementation nationale en cause ne se borne pas à autoriser les autorités compétentes à demander la conservation des données relatives au trafic et des données de localisation pour une période limitée : c'est le législateur qui impose directement, et de manière indéfinie, l'obligation de les conserver.

55. Cette prémisse étant posée, cette juridiction a énuméré, dans sa communication du 13 janvier 2021, les différences entre les règles nationales et celles visées dans l'arrêt La Quadrature du Net, qui pourraient donner lieu à une solution différente de celle retenue à l'époque.

56. Je procéderai à l'analyse de ces différences dans le même ordre que celui dans lequel la juridiction de renvoi les expose, mais je dois avant tout reconnaître que le législateur allemand s'est appliqué avec sérieux à adapter la réglementation nationale aux exigences découlant, dans ce domaine, de la jurisprudence dégagée par la Cour.

57. Ainsi que la juridiction de renvoi le souligne, la réglementation litigieuse procède d'une modification législative rendue possible par la jurisprudence du Bundesverfassgericht (Cour constitutionnelle fédérale) et par les effets de la jurisprudence issue de l'arrêt Digital Rights.

58. Il convient donc de saluer les progrès réalisés dans la législation nationale litigieuse, qui résultent d'une volonté déterminée de se conformer à la jurisprudence de la Cour.

59. Toutefois, l'effort législatif a peut-être davantage mis l'accent sur les aspects liés à la protection et à l'accès aux données conservées que sur les aspects liés à la délimitation ciblée de celles dont la conservation est requise.

1. *Typologie des données conservées*

60. La typologie des données conservées (celles qui sont relatives aux sites Internet consultés, celles du courrier électronique et celles qui sous-tendent les communications vers ou à partir de services de centre d'appel à caractère social ou religieux ne sont pas stockées) n'empêche pas, à mon avis, d'ignorer que l'obligation de stockage généralisée et indifférenciée s'étend à un ensemble très large de nombreuses autres données relatives au trafic et de localisation, qui est similaire, dans l'ensemble, à celui qui a été examiné dans l'arrêt La Quadrature du Net.

61. À cet égard, il est presque indifférent, compte tenu de leurs caractéristiques particulières et de leur très faible impact sur le calcul global (43), que les données qui sous-tendent les communications vers certaines lignes de services de centre d'appel attribuées à des personnes, des autorités ou des organisations à caractère social ou religieux soient exclues.

62. Il n'est pas non plus déterminant que l'obligation de conserver ne s'étende pas aux contenus (qu'il s'agisse des sites visités sur Internet ou des courriers électroniques), puisque l'arrêt La Quadrature du Net ne faisait pas référence à ceux-ci, mais aux données relatives au trafic et aux données de localisation des communications électroniques.

2. ***Durée de l'obligation de conserver les données***

63. La plus grande différence par rapport aux règles nationales analysées dans l'arrêt La Quadrature du Net concerne la durée du stockage qui, selon l'article 113b, paragraphe 1, du TKG, est de quatre ou dix semaines (quatre semaines pour les données de localisation et dix semaines pour les autres), et non d'un an.

64. Tant la juridiction de renvoi que certains gouvernements qui sont intervenus dans la procédure insistent sur cette circonstance, en soulignant que la réglementation litigieuse réduit sensiblement la durée de conservation des données. Pour la juridiction de renvoi, la durée moindre diminue le risque d'établissement d'un profil global des personnes concernées.

65. Comme je l'ai indiqué dans les conclusions Ordre des barreaux francophones et germanophone, en faisant précisément écho à la réglementation nationale qui nous occupe, les données conservées ne peuvent l'être que pendant une période limitée (44), selon qu'elles appartiennent à une catégorie ou à une autre (45).

66. Or, si la limitation temporelle de la période de conservation constitue un élément pertinent pour apprécier la réglementation litigieuse, cette circonstance ne saurait compenser le fait qu'elle impose une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

67. J'ai déjà expliqué que, conformément à la jurisprudence de la Cour, en dehors du cas de figure justifié par la défense de la sécurité nationale, seul un stockage sélectif des données relatives aux communications électroniques peut être envisagé en raison du risque sérieux que comporterait leur conservation généralisée.

68. C'est ce risque qui a, en définitive, inspiré la jurisprudence de la Cour en la matière : « 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 » (46).

69. Certes, et comme l'affirme la juridiction de renvoi, une conservation très limitée dans le temps peut rendre l'établissement de profils plus difficile.

70. Toutefois, la plus ou moins grande difficulté à cet égard est fonction non seulement du temps de conservation, mais également de la quantité et de la qualité des données conservées : plus le nombre de données est important, plus il est possible d'obtenir des informations sensibles sur des périodes de temps dont l'ampleur dépendra du développement de techniques de suivi, de corrélation et d'évaluation de l'ensemble des données relatives aux communications électroniques. Ce qui peut être insuffisant aujourd'hui pour accumuler des informations facilitant l'établissement de profils, peut être plus que suffisant pour y parvenir dans un avenir plus ou moins proche (47).

71. En tout état de cause, et selon la Cour, « l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès, par une autorité publique, à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise, présente en tout état de cause un caractère grave *indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité* et de la quantité ou de la nature des données disponibles pour une telle période, lorsque […] cet ensemble de données est susceptible de permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées » (48).

72. En définitive, j'estime que, malgré les différences relevées par la juridiction de renvoi, les similitudes sur ce point entre la réglementation en cause dans les procédures au principal et les législations impliquées dans les procédures ayant donné lieu à l'arrêt La Quadrature du Net ne permettent pas de faire abstraction de la jurisprudence issue de ce dernier.

3. *Protection des données contre leur accès illicite*

73. Selon la juridiction de renvoi, les normes allemandes offrent une protection efficace des données conservées contre les risques d'abus et d'accès illicite.

74. Sans vouloir déprécier l'effort réglementaire qui a été fait en matière de protection des données et d'accès aux données, on ne peut pas oublier que, pour la Cour, « la conservation des données relatives au trafic et des données de localisation constitue, *par elle-même*, […] une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel » (49). À cet égard, « l'accès à de telles données constitu[e], quelle que soit l'utilisation qui en est faite ultérieurement, une *ingérence distincte* » dans les droits fondamentaux susvisés (50).

75. Il est donc indifférent, aux fins de la présente affaire, que le régime de protection des données conservées prévu par le législateur allemand : a) garantisse de manière effective l'inviolabilité de ces données ; b) encadre strictement et effectivement les conditions d'accès, en limitant le cercle de ceux qui peuvent y accéder ; et c) n'autorise l'utilisation des données stockées qu'à des fins d'enquêtes sur des infractions graves et de prévention de risques concrets pour la vie ou la liberté des personnes ou pour la sûreté de l'État.

76. Ce qui importe vraiment, comme le répète également la juridiction de renvoi, c'est que l'obligation de conservation litigieuse, en tant que telle, ne soit soumise à aucune condition spécifique.

4. *Incidence de l'arrêt du Bundesverfassungsgericht (Cour constitutionnelle fédérale) du 27 mai 2020*

77. La juridiction de renvoi évoque une décision du Bundesverfassungsgericht (Cour constitutionnelle fédérale) relative à l'article 113 du TKG (51), à l'issue de laquelle, après la déclaration de son inconstitutionnalité, la validité de cette disposition aurait été soumise à des conditions dont la compatibilité avec le droit de l'Union ne serait pas facile à déterminer.

78. La Cour n'a rien à dire, à ce stade, sur les effets de cet arrêt et encore moins sur les contours des nouvelles règles que le législateur allemand serait amené à adopter (ou qu'il a adoptées, le cas échéant).

79. Si, comme le soutient la juridiction de renvoi, elle doit rendre son arrêt en « Revision » au regard du droit en vigueur à la date de son prononcé, elle devra elle-même déterminer sa compatibilité avec le droit de l'Union à la lumière de la jurisprudence de la Cour relative à la protection des données des communications électroniques.

5. *Adresses IP*

80. Selon la juridiction de renvoi, il ressortirait du point 168 de l'arrêt La Quadrature du Net que la Cour exige, pour les adresses IP, un motif de conservation lié à l'objectif de sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique. Toutefois, il ressortirait du point 155 que ces adresses IP peuvent être conservées sans motif particulier, et que seule l'utilisation des données conservées nécessiterait un motif lié à cet objectif.

81. Toutefois, il ne me semble pas que cette tension existe (et encore moins une contradiction). Si la Cour affirme, au point 155, que la conservation généralisée et indifférenciée des 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 », elle déclare immédiatement après, au point 156, que, « [e]u égard au caractère grave de l'ingérence dans les droits fondamentaux […] 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 […] ».

82. C'est donc de la combinaison des points 155 et 156 de l'arrêt La Quadrature du Net que découle la réponse cohérente que la Cour a donnée, au point 168, aux questions préjudicielles posées à l'époque sur la conservation des adresses IP.

83. Au cours de l'audience, certains problèmes ont été mis en évidence – qui, de l'avis de certains intervenants, nécessiteraient une clarification de la Cour – concernant la conservation des adresses IP. La solution de ces problèmes (notamment ceux causés par la différence entre les adresses IP dynamiques et statiques ainsi que par l'incidence du protocole IPv6) va, à mon avis, au-delà de l'objet de la consultation de la juridiction de renvoi, dont les demandes de décision préjudicielle initiales (52) et la communication du 13 janvier 2021 ont, sur ce point, une portée beaucoup plus limitée.

V. **Conclusion**

84. À la lumière de ce qui précède, je suggère à la Cour de répondre au Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne) en ces termes :

« 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 en combinaison avec les articles 7, 8, 11 et 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et de l'article 4, paragraphe 2, TUE, doit 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, de manière préventive, générale et indifférenciée, les données relatives au trafic et les données de localisation des utilisateurs finals de ces services à des fins autres que celles de la protection de la sécurité nationale contre une menace grave réelle et actuelle ou prévisible ».

1 Langue originale : l'espagnole.

2 Affaire C-140/20, Commissioner of the Garda Síochána e.a., dans laquelle je présente des conclusions ce jour.

3 Ci-après les « conclusions La Quadrature du Net » (EU:C:2020:6).

4 Ci-après les « conclusions Ordre des barreaux francophones et germanophone » (EU:C:2020:7).

5 Affaires C-293/12 et C-594/12 (EU:C:2014:238 ; ci-après l'« arrêt Digital Rights »).

6 Directive 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 (JO 2006, L 105, p. 54).

7 Affaires C-203/15 et C-698/15 (EU:C:2016:970 ; ci-après l'« arrêt Tele2 Sverige »).

8 Directive 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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11).

9 Affaire C-207/16 (EU:C:2018:788).

10 Affaire C-623/17 (EU:C:2020:790).

11 Affaires C-511/18, C-512/18 et C-520/18 (EU:C:2020:791 ; ci-après l'« arrêt La Quadrature du Net »).

---

12 Point 30 des présentes conclusions.

---

13 Directive 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 (JO 1995, L 281, p. 31).

---

14 Les communications visées à l'article 99, paragraphe 2, du TKG sont des communications avec des personnes, des autorités et des organisations à caractère social ou religieux qui offrent à des appelants, en principe anonymes, des services d'assistance téléphonique en cas de situations d'urgence psychologique ou sociale et qui sont soumis à des obligations de confidentialité particulières. Conformément à l'article 99, paragraphe 2, deuxième à quatrième phrases, du TKG, cette dérogation est subordonnée à l'inscription sur une liste gérée par la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agence fédérale des réseaux d'électricité, du gaz, des télécommunications, des postes et des chemins de fer ; ci-après l'« Agence fédérale des réseaux »), après accréditation de la nature de ses services par une attestation délivrée par une entité, un organisme ou une fondation de droit public.

---

15 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).

---

16 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (DE:BVerfG:2010:rs20100302.1bvr025608).

---

17 Selon la juridiction de renvoi, la jurisprudence de la Cour ne ferme pas totalement la porte à la possibilité, pour les législateurs nationaux, de prévoir 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.

---

18 Telle est l'expression littérale employée par la juridiction de renvoi.

---

19 Arrêt du 27 mai 2020, 1 BvR 1873/13, 1 BvR 2618/13 (DE:BVerfG:2020:rs20200527.1bvr187313). Conformément à cet arrêt, l'article 113 du TKG est incompatible avec les articles 2, paragraphe 1, et 10, paragraphe 1, de la Grundgesetz (Loi fondamentale) et ne peut être appliqué que jusqu'à l'adoption de nouvelles règles, au plus tard le 31 décembre 2021.

---

20 Arrêt La Quadrature du Net, point 104.

---

21 Point 19, sous a), de l'ordonnance de renvoi.

---

22 Conclusions La Quadrature du Net, points 40 à 90.

---

23 Arrêt La Quadrature du Net, point 109.

---

24 Ibidem, points 111 à 133.

---

25 Arrêt La Quadrature du Net, point 136.

---

26 Ibidem, point 137 (mise en italiques par mes soins). Il en est ainsi, poursuit la Cour, « [m]ême 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 […] avec une menace pour la sécurité nationale de cet État membre », puisqu'il y a alors lieu de « considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport » (Ibidem).

---

27 CE:ECHR:2021:0525JUD005817013.

---

28 CE:ECHR:2021:0525JUD003525208.

---

29 CE:ECHR:2015:1204JUD004714306.

30 Arrêt La Quadrature du Net, point 147 : « 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 ». Mise en italique par mes soins

31 Arrêt La Quadrature du Net, points 148 et 149.

32 Arrêt La Quadrature du Net, point 150.

33 Outre leur caractère insuffisant, la possibilité qu'ils conduisent à l'instauration d'un régime de suspicion générale à l'égard de certains segments de la population ou à la stigmatisation de zones géographiques.

34 Conclusions Ordre des barreaux francophones et germanophone, points 88 et 89.

35 Ibidem, point 90.

36 Point 47 de ses observations. Ce point a également été souligné par certains gouvernements au cours de l'audience.

37 Groupe Échange d'informations et protection des données (DAPIX). Le gouvernement suédois a adopté le même point de vue au point 21 de ses observations.

38 Au point 92 des conclusions Ordre des barreaux francophones et germanophone, j'ai souligné que ces groupes de travail avaient considéré, comme des pistes à explorer, la limitation des catégories de données conservées ; la pseudonymisation des données ; l'introduction de périodes de conservation limitées ; l'exclusion de certaines catégories de fournisseurs de services de communications électroniques ; les autorisations de conservation renouvelables ; l'obligation de

conserver les données dans l'Union ou le contrôle systématique et régulier, par une autorité administrative indépendante, des garanties offertes par les fournisseurs de services de communications électroniques contre l'utilisation abusive des données.

---

39 Conclusions Ordre des barreaux francophones et germanophone, points 93 et 94.

---

40 Ibidem, point 95.

---

41 Ibidem, point 104.

---

42 Point 25b, sous b), de l'original allemand de l'ordonnance de renvoi.

---

43 Lors de l'audience, le gouvernement allemand a évalué à 1 300 le nombre d'entités dont les communications électroniques sont exclues de l'obligation de conservation et a précisé que l'exclusion ne pouvait pas s'appliquer aux professionnels soumis à des obligations de secret professionnel (comme les avocats ou les médecins), compte tenu du grand nombre de ces professionnels.

---

44 Conclusions Ordre des barreaux francophones et germanophone, point 96 : de sorte qu'elles « ne permettent pas de donner une image détaillée de la vie des personnes concernées. Cette période de conservation doit également être adaptée en fonction de la nature des données, de sorte que celles qui fournissent des informations plus précises sur les modes de vie et les habitudes de ces personnes soient stockées pendant une période plus courte ».

---

45 Ibidem, point 97 : « En d'autres termes, la différenciation de la période de conservation de chaque catégorie de données, en fonction de leur utilité pour atteindre les objectifs de sécurité, est une voie à explorer. En limitant la durée pendant laquelle les différentes catégories de données sont stockées simultanément (et peuvent donc être utilisées pour trouver des corrélations qui révèlent le mode de vie des personnes concernées), le droit garanti par l'article 8 de la Charte est davantage protégé ».

---

46 Arrêt La Quadrature du Net, point 117.

---

47 Comme cela a été souligné à l'audience, même une période de dix semaines d'accumulation de métadonnées (données relatives au trafic et de localisation) pourrait suffire à identifier des schémas de comportement de l'abonné qui, par leur répétition, révéleraient des caractéristiques sensibles de sa personnalité et de sa vie.

---

48 Arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152, point 39). Mise en italiques par mes soins.

---

49 Arrêt La Quadrature du Net, point 115.

---

50 Ibidem, point 116. Mise en italiques par mes soins.

---

51 Voir la note 19 des présentes conclusions.

---

52 Point 30 de l'ordonnance de renvoi.