Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MANUEL CAMPOS SÁNCHEZ-BORDONA
présentées le 18 novembre 2021 [1]

Affaire C-140/20

G.D.
contre
The Commissioner of the Garda Síochána,
Minister for Communications, Energy and Natural Resources,
Attorney General

[demande de décision préjudicielle formée par la Supreme Court (Cour suprême, Irlande)]

« Renvoi préjudiciel – Télécommunications – Traitement des données à caractère personnel – Confidentialité des communications – Fournisseurs de services de communications électroniques – Directive 2002/58/CE – Article 15, paragraphe 1 – Article 4, paragraphe 2, TUE – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 11 et article 52, paragraphe 1 – Conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – Accès aux données conservées – Utilisation des données conservées comme élément de preuve dans le cadre d'une procédure pénale »

1. La demande de décision préjudicielle dans la présente affaire – à laquelle s'ajoutent celles ayant donné lieu aux affaires jointes C-793/19, SpaceNet, et C-794/19, Telekom Deutschland, dans lesquelles je présente également des conclusions [2] ce jour – témoigne, 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.

[1] Langue d'origine : l'espagnol.

[2] Ci-après les « conclusions dans les affaires jointes SpaceNet et Telekom Deutschland ».

2. Dans mes conclusions dans les affaires jointes La Quadrature du Net e.a., C-511/18 et C-512/18 [3], et dans l'affaire Ordre des barreaux francophones et germanophone e.a., C-520/18 [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 une 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], dans lequel la Cour 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 quelques 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.

3 EU:C:2020:6.

4 Ci-après les « conclusions dans l'affaire Ordre des barreaux francophones et germanophone », EU:C:2020:7.

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

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 C-203/15 et C-698/15, ci-après l'« arrêt Tele2 Sverige », EU:C:2016:970.

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) (ci-après la « directive 2002/58 »).

9 C-207/16, EU:C:2018:788.

10 C-623/17, EU:C:2020:790.

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

6. Cependant, avant le 6 octobre 2020, trois autres demandes de décision préjudicielle (celle dans la présente affaire et celles dans les affaires jointes C-793/19 et C-794/19), qui, par leur contenu, remettaient à nouveau en cause la jurisprudence établie concernant 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 leurs demandes 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. Le cadre juridique

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

8. Conformément à l'article 5 (« Confidentialité des communications »), paragraphe 1, de la directive 2002/58 :

« 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. L'article 6 (« Données relatives au trafic ») de cette directive dispose :

« 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.

[...] »

[12] Points 25 et suiv. des présentes conclusions.

10. L'article 15 (« Application de certaines dispositions de la directive 95/46/CE »)[13] de ladite directive, prévoit en 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 irlandais. Le Communications (Retention of Data) Act 2011 [loi de 2011 sur les communications (conservation des données) (ci-après la « loi de 2011 »)]

11. Au point 3 de sa décision de renvoi, la Supreme Court (Cour suprême, Irlande) expose les éléments de droit national suivants :

– « [l]a loi de 2011 a été adoptée dans le but déclaré de mettre en œuvre la directive [2006/24] ;

– l'article 3 de la loi [de 2011] impos[e] à tous les fournisseurs de services de conserver les "données relatives à la téléphonie fixe en réseau et à la téléphonie mobile" pendant deux ans ;

– [i]l s'agit des données qui permettent d'identifier la source et la destination d'une communication, de déterminer la date et l'heure du début et de la fin d'une communication, de déterminer le type de communication [...], ainsi que d'identifier le type et la localisation géographique du matériel de communication utilisé. Le contenu des communications ne relève pas de ce type de données ;

– [c]es données peuvent être consultées et divulguées sur présentation d'une demande de divulgation. L'article 6 de la loi de 2011 prévoit les conditions dans lesquelles une demande de divulgation peut être introduite et le paragraphe 1 de cet article dispose qu'un fonctionnaire de [l'An Garda Síochána (police nationale, Irlande)] dont le rang n'est pas inférieur à celui de "chief superintendent" (commissaire divisionnaire) peut introduire une demande de divulgation si ce fonctionnaire estime que les données en question sont nécessaires aux fins, notamment, de la prévention, de la détection, de la recherche ou de la poursuite d'une infraction grave[, étant considérée comme telle] une infraction passible d'une peine d'emprisonnement d'une durée égale ou supérieure à [cinq] ans ou l'une des autres infractions énumérées à l'annexe 1 de la loi [de 2011] ;

– [p]armi les mécanismes de contrôle prévus par la loi de 2011 figurent la procédure de réclamation établie à l'article 10 et les fonctions du "designated judge" (juge désigné), au sens de l'article 12, qui est chargé d'analyser l'application des dispositions de la loi ;

[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).

– [...] à titre de mesure interne, le [Commissioner of the Garda Síochána (chef de la police nationale, Irlande)] a décidé que les demandes de divulgation de données de téléphonie introduites en vertu de la loi de 2011 devaient faire l'objet d'un traitement centralisé, par un seul commissaire divisionnaire. En matière de divulgation des données, le commissaire divisionnaire responsable est le chef de la section de la sécurité et du renseignement [de la police nationale] et c'est lui qui décide, en dernier ressort, d'adresser ou non une demande de divulgation aux fournisseurs de services de communications conformément aux dispositions de la loi de 2011. Une petite unité indépendante appelée la "Telecommunications Liaison Unit" (unité de liaison en matière de télécommunications, ci-après la "TLU") a été créée afin de fournir un appui au commissaire divisionnaire dans l'exercice de ses fonctions et de servir de point de contact unique avec les fournisseurs de services ;

– [p]endant la période pertinente pour la présente [procédure], toutes les demandes de divulgation devaient être approuvées en premier ressort par un "superintendent" (commmissaire)[,] ou un "inspector" faisant fonction[,] et étaient ensuite envoyées à la TLU en vue de leur traitement. Les enquêteurs étaient invités à assortir leurs demandes de détails suffisants pour qu'une décision éclairée puisse être prise et à garder à l'esprit que le commissaire divisionnaire pouvait devoir justifier ultérieurement cette décision en justice ou devant le juge désigné de la High Court (Haute Cour[, Irlande]). La TLU et le commissaire divisionnaire sont tenus de vérifier la légalité, la proportionnalité et la nécessité des demandes de divulgation émanant des fonctionnaires de la police nationale. Les demandes jugées non conformes aux exigences de la loi ou des procédures internes de la police étaient renvoyées afin que des éclaircissements ou des informations complémentaires soient fourni[s]. En vertu d'un protocole d'accord publié au mois de mai 2011, les fournisseurs de services s'engageaient à ne pas traiter les demandes de données relatives à des appels qui ne leur étaient pas parvenues dans le cadre de ce processus. La TLU est également soumise au contrôle du Data Protection Commissioner (commissaire à la protection des données, Irlande). »

12. Quelques précisions supplémentaires concernant le contenu de la loi de 2011 figurent à l'annexe I de la décision de renvoi. Il est ainsi indiqué :

– l'article 1er de la loi de 2011 définit la notion de « données » comme visant « les données relatives au trafic ou les données de localisation et les données connexes nécessaires pour identifier l'abonné ou l'utilisateur » ;

– l'article 6, paragraphe 1, de la loi de 2011 autorise un fonctionnaire de police, dans les conditions décrites ci-dessus, à accéder à ces données s'il estime que celles-ci sont nécessaires à des fins « a) de prévention, de détection, de recherche ou de poursuite d'une infraction grave, b) de sauvegarde de la sûreté de l'État, c) de préservation de la vie humaine ».

II. Les faits, le litige et les questions préjudicielles

13. En 2015, G.D. a été condamné à la réclusion à perpétuité pour meurtre. Au cours de la procédure d'appel devant la Court of Appeal (Cour d'appel, Irlande), il a contesté, sans succès, l'admissibilité de certains éléments de preuve à charge reposant sur des données de téléphonie conservées conformément à la législation nationale.

14. Parallèlement au recours en appel au pénal, G.D. a engagé une procédure *civile*[14] devant la High Court (Haute Cour) afin de contester la validité de certaines dispositions de la loi de 2011 en vertu desquelles les données de téléphonie susmentionnées avaient été conservées et avaient pu être consultées.

15. Par décision du 6 décembre 2018, la High Court (Haute Cour) a fait droit à la demande de G.D. tendant à ce que soit constatée l'incompatibilité de l'article 6, paragraphe 1, sous a), de la loi de 2011 avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte.

16. Le gouvernement irlandais a contesté cette décision devant la Supreme Court (Cour suprême), qui a saisi la Cour des questions préjudicielles suivantes :

« 1) Un régime général/universel de conservation des données – même assorti de restrictions strictes en matière de conservation et d'accès – est-il, en soi, contraire aux dispositions de l'article 15 de la directive [2002/58], interprétées à la lumière de la Charte ?

2) Dans le cadre de l'examen du point de savoir s'il convient de constater l'incompatibilité d'une mesure nationale mise en œuvre conformément à la directive [2006/24] et prévoyant un régime général de conservation des données (assorti des contrôles stricts nécessaires en matière de conservation ou d'accès) et, en particulier, dans le cadre de l'appréciation de la proportionnalité d'un tel régime, une juridiction nationale est-elle fondée à tenir compte du fait que des données peuvent être conservées légalement par les fournisseurs de services pour leur propre usage commercial et que leur conservation peut être imposée pour des raisons de sécurité nationale exclues du champ d'application des dispositions de la directive [2002/58] ?

3) Dans le cadre de l'appréciation de la compatibilité avec le droit de l'Union, et en particulier avec la Charte, d'une mesure nationale régissant l'accès aux données conservées, quels critères une juridiction nationale doit-elle appliquer lorsqu'elle examine si de telles règles d'accès prévoient le contrôle préalable indépendant qui est requis par la Cour dans sa jurisprudence ? Dans ce contexte, une juridiction nationale peut-elle, dans le cadre d'une telle appréciation, tenir compte de l'existence d'un contrôle juridictionnel ex post ou indépendant ?

4) En tout état de cause, une juridiction nationale est-elle tenue de constater l'incompatibilité d'une mesure nationale avec les dispositions de l'article 15 de la directive [2002/58] dans le cas où cette mesure nationale prévoit un régime général de conservation des données à des fins de lutte contre la criminalité grave et où la juridiction nationale a conclu, eu égard à tous les éléments de preuve disponibles, qu'une telle conservation est à la fois indispensable et strictement nécessaire à la réalisation de l'objectif constitué par la lutte contre la criminalité grave ?

5) Si une juridiction nationale est tenue de conclure qu'une mesure nationale est contraire aux dispositions de l'article 15 de la directive [2002/58], interprétées à la lumière de la Charte, est-elle fondée à limiter les effets dans le temps d'une telle constatation si elle estime que ne pas limiter ses effets entraînerait "le chaos et un préjudice grave pour l'intérêt général"

[14] Voir point 80 des présentes conclusions.

[conformément à l'approche adoptée, par exemple, dans le jugement R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs [2018] EWHC 975, point 46] ?

6) Une juridiction nationale invitée à constater l'incompatibilité de la législation nationale avec l'article 15 de la directive [2002/58] ou à écarter l'application de cette législation ou bien à déclarer que l'application d'une telle législation a violé les droits d'une personne physique, que ce soit dans le cadre d'une procédure engagée afin de faciliter la présentation d'un argument relatif à l'admissibilité des preuves dans une procédure pénale ou dans un autre cadre, peut-elle être autorisée à refuser de faire droit à cette demande en ce qui concerne les données conservées en application de la disposition nationale adoptée en vertu de l'obligation, prévue à l'article 288 TFUE, de transposer fidèlement en droit national les dispositions d'une directive ou à limiter une telle constatation à la période postérieure à la déclaration de l'invalidité de la directive [2006/24] par la Cour le 8 avril 2014 ? »

17. La Supreme Court (Cour suprême) relève que des éléments de preuve tels que ceux qui ont été avancés dans la procédure pénale engagée contre G.D. sont déterminants aux fins de la détection et de la poursuite de certaines catégories d'infractions graves. Elle souligne que, s'il n'est pas permis de procéder à la conservation à titre universel des métadonnées, même avec les conditions d'accès qui pourraient être établies, les auteurs de nombre de ces infractions ne pourraient pas être découverts ni jugés de manière satisfaisante.

18. Dans cet ordre d'idées, elle formule les remarques suivantes :

– d'autres formes de conservation des données, au moyen d'un ciblage géographique ou autre, ne permettraient pas d'atteindre les objectifs de prévention, de recherche, de détection et de poursuite de certains types au moins d'infractions graves et, de plus, pourraient entraîner une violation potentielle d'autres droits de la personne ;

– l'objectif de la conservation des données par un moyen moins lourd que le régime général de la conservation des données, assorti des garanties nécessaires, est irréalisable ; et

– les objectifs de prévention, de recherche, de détection et de poursuite des infractions graves seraient fortement compromis en l'absence d'un régime général de conservation de données.

III. La procédure devant la Cour

19. La demande de décision préjudicielle a été enregistrée au greffe de la Cour le 25 mars 2020.

20. Des observations écrites ont été déposées par G.D., le Commissioner of the Garda Síochána (chef de la police nationale), les gouvernements belge, tchèque, danois, estonien, espagnol, français, chypriote, néerlandais, polonais, portugais, finlandais et suédois, ainsi que par la Commission européenne.

21. Invitée à se prononcer sur l'éventuel retrait de la demande de décision préjudicielle après que la Cour a rendu son arrêt La Quadrature du Net, la juridiction de renvoi a indiqué, par lettre enregistrée le 27 octobre 2020, qu'elle entendait la maintenir [15].

[15] Voir points 25 et suiv. des présentes conclusions.

22. L'audience publique, qui s'est tenue conjointement avec celle des affaires jointes C-793/19, SpaceNet, et C-794/19, Telekom Deutschland, a eu lieu le 13 septembre 2021. Les parties qui avaient déposé des observations écrites (à l'exception des gouvernements belge, tchèque et portugais) et le Contrôleur européen de la protection des données ont comparu.

IV. Analyse

A. Considérations liminaires

23. La majorité des parties à la procédure s'accorde à considérer que les six questions préjudicielles de la Supreme Court (Cour suprême) portant sur l'article 15, paragraphe 1, de la directive 2002/58 peuvent être regroupées en trois thèmes, à savoir :

– la licéité d'un régime de *conservation* généralisée et indifférenciée des données en lui-même et en lien avec la lutte contre la criminalité grave (première, deuxième et quatrième questions) ;

– les caractéristiques que doit remplir, le cas échéant, l'*accès* aux données conservées (troisième question) ;

– la possibilité de limiter dans le temps les effets d'une éventuelle constatation d'incompatibilité avec le droit de l'Union de la réglementation nationale en la matière (cinquième et sixième questions).

24. Selon moi, la Cour a pleinement répondu à toutes ces questions dans les arrêts La Quadrature du Net et du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) [16].

25. À propos de l'arrêt La Quadrature du Net, il a été communiqué à la juridiction de renvoi et celle-ci a ensuite répondu de manière particulièrement laconique à la Cour.

26. Après avoir reconnu que cet arrêt contribuait à clarifier le droit de l'Union, elle a affirmé, sans plus d'indications, que « le type d'affaire à l'origine de la procédure dans laquelle le renvoi a été effectué par la Supreme Court [Cour suprême] diffère significativement du type de situations à l'origine des procédures ayant donné lieu à cet arrêt » [17].

27. Dans ces affirmations, postérieures à sa demande de décision préjudicielle, la juridiction de renvoi n'en vient pas à remettre en cause la jurisprudence issue de l'arrêt La Quadrature du Net (ce qu'ont fait, quant à eux, certains gouvernements intervenus dans la procédure) ni ne demande d'éclaircissements concernant son contenu.

[16] C-746/18, ci-après l'« arrêt Prokuratuur », EU:C:2021:152. Le contenu de cet arrêt a fait l'objet de débats lors de l'audience.

[17] C'est en ces termes que la Supreme Court (Cour Suprême) s'est exprimée dans la lettre enregistrée le 27 octobre 2020, par laquelle elle a répondu à l'invitation de la Cour à indiquer si elle maintenait la demande de décision préjudicielle, à la suite du prononcé de l'arrêt La Quadrature du Net.

28. Bien que les « situations à l'origine »[18] des procédures dans lesquelles la Cour a statué par l'arrêt La Quadrature du Net diffèrent de celle du renvoi préjudiciel dans la présente affaire, ce qui est important est que la jurisprudence établie par la Cour dans cet arrêt, à titre général, s'impose erga omnes et lie toutes les juridictions des États membres en ce qui concerne l'interprétation de la directive 2002/58.

29. Quant à l'accès aux données conservées, j'estime également que l'arrêt Prokuratuur, postérieur à la décision de la juridiction de renvoi de maintenir le renvoi préjudiciel, dissipe les doutes exprimés dans ce cadre.

30. Dans ces conditions, et à la différence de l'approche que je suis dans les conclusions dans les affaires jointes SpaceNet et Telekom Deutschland[19], je me bornerai, dans les présentes conclusions, à tirer les conséquences qui découlent des arrêts La Quadrature du Net et Prokuratuur aux fins du renvoi préjudiciel dans la présente affaire, tel qu'il a été formulé à l'origine.

B. Conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (première, deuxième et quatrième questions préjudicielles)

31. La juridiction de renvoi cherche à savoir, en substance :

– si l'article 15, paragraphe 1, de la directive 2002/58, interprété à la lumière de la Charte, s'oppose à un régime général de conservation des données ;

– si, aux fins de l'examen d'une réglementation nationale qui instaure un régime de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, assorti de contrôles stricts, le fait que ces données peuvent être conservées légalement par les fournisseurs de services pour leur propre usage commercial et que cette conservation peut être imposée pour des raisons de sécurité nationale constitue un élément pertinent ;

– si l'incompatibilité d'une législation nationale avec l'article 15 de la directive 2002/58 subsiste lorsque cette législation impose la conservation généralisée des données susmentionnées aux fins de la lutte contre la criminalité grave.

32. Comme je le préconise également dans les conclusions dans les affaires jointes SpaceNet et Telekom Deutschland[20], la réponse à ces questions ne saurait être différente de celle apportée par la Cour dans l'arrêt La Quadrature du Net, *récapitulant* la jurisprudence à cet égard.

33. 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 à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif,

[18] Par ces « situations », il convient de comprendre, à défaut d'autres d'explications, les éléments relatifs aux faits visés par la procédure et aux règles nationales applicables.

[19] Le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne) a décrit les différences que présente sa législation nationale par rapport à celles examinées dans l'arrêt La Quadrature du Net et a sollicité une décision de la Cour au regard de ces différences.

[20] Les points 33 à 41 des présentes conclusions reproduisent les points 36 à 42 de ces conclusions.

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. »

34. 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 [21].

35. 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 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 [22].

36. La conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation 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 » [23].

37. 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 » [24].

38. Il est vrai que ces prescriptions donnent lieu à un régime plus rigoureux et strict que celui découlant de la jurisprudence de la Cour européenne des droits de l'homme, lue en combinaison avec l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950. Le fait que « [le] sens et [la] portée des droits » de la Charte correspondant à ceux de cette convention 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.

39. Au demeurant, la jurisprudence de la Cour européenne des droits de l'homme dans ses arrêts du 25 mai 2021, Big Brother Watch e.a. c. Royaume-Uni [25] et Centrum för Rättvisa c. Suède [26], ainsi que dans celui du 4 décembre 2015, Zakharov c. Russie [27], concerne des cas de figure qui, comme il a été majoritairement soutenu lors de l'audience, ne sont pas comparables à celui qui est débattu dans le cadre du renvoi préjudiciel ici en cause. 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.

21 Arrêt La Quadrature du Net, point 109.

22 Arrêt La Quadrature du Net, points 111 à 133.

23 Arrêt La Quadrature du Net, point 136.

24 Arrêt La Quadrature du Net, point 137 (mise en italique 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 » (arrêt La Quadrature du Net, point 137).

25 CE:ECHR:2021:0525JUD005817013.

26 CE:ECHR:2021:0525JUD003525208.

27 CE:ECHR:2015:1204JUD004714306.

40. 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 (selon moi, les limites établies par la Cour sont excessivement larges), les prescriptions énoncées aux points 137 à 139 de cet arrêt doivent être respectées.

41. 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.

42. Or, le sens de l'arrêt La Quadrature du Net ne serait pas respecté si les considérations qu'il contient concernant la sécurité nationale pouvaient être étendues aux infractions, même graves, qui ne portent pas atteinte à celle-ci, mais à la sécurité publique ou à d'autres intérêts juridiquement protégés.

43. La Cour a donc soigneusement distingué les mesures législatives nationales prévoyant la conservation préventive, généralisée et indifférenciée, des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale (points 134 à 139 de l'arrêt La Quadrature du Net) de celles ayant trait à la lutte contre la criminalité et à la sauvegarde de la sécurité publique (points 140 à 151 de cet arrêt). Les unes et les autres ne sauraient avoir la même portée, sous peine de priver cette distinction de tout sens.

44. Les instruments de conservation des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave sont indiqués, je le répète, aux points 140 à 151 de l'arrêt La Quadrature du Net. Il convient d'y ajouter ceux qui autorisent, avec la même finalité, la conservation préventive des adresses IP et des données relatives à l'identité civile de la personne (points 152 à 159 de cet arrêt), ainsi que la « conservation rapide » des données relatives au trafic et des données de localisation (points 160 à 166 dudit arrêt).

45. La juridiction de renvoi s'interroge, spécifiquement, sur l'incidence du « fait que des données peuvent être conservées légalement par les fournisseurs de services pour leur propre usage commercial et que leur conservation peut être imposée pour des raisons de sécurité nationale exclues du champ d'application des dispositions de la directive 2002/58 ».

46. Or, s'agissant des données que ces opérateurs stockent à des fins commerciales, la Cour, dans l'arrêt La Quadrature du Net, les lie à l'objectif pour lequel elles ont été collectées et autorise uniquement leur éventuelle « conservation rapide » dans les conditions énoncées aux points 160 à 166 susmentionnés de cet arrêt.

47. Les impératifs de la sécurité nationale autorisent, de la manière et avec les garanties et restrictions indiquées dans l'arrêt La Quadrature du Net, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. Tel n'est pas le cas, cependant, s'agissant de l'objectif de poursuite des infractions, même graves, auxquelles fait référence l'article 6, paragraphe 1, sous a), de la loi de 2011, sur lequel porte le renvoi préjudiciel.

48. En ce qui concerne les problèmes soulevés par la *conservation ciblée* des données relatives au trafic et des données de localisation [28], je renvoie, par ailleurs, aux points 43 à 50 de mes conclusions dans les affaires jointes SpaceNet et Telekom Deutschland.

49. Si l'on ne peut pas demander à la Cour d'assumer des fonctions réglementaires et de préciser, en détail, quelles catégories de données peuvent être conservées et pour combien de temps [29], il conviendrait encore moins que, dans le cadre de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, la Cour s'arroge le rôle de législateur en introduisant dans cette disposition des catégories intermédiaires entre la sécurité nationale et la sécurité publique, pour appliquer à la seconde les exigences inhérentes à la première.

50. Comme la Cour l'a indiqué, « l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de [la directive 2002/58] revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs » [30].

51. La proposition formulée par la Commission lors de l'audience [31] (introduire un tertium genus d'infractions) étendrait jusqu'à des limites imprécises le seul motif susceptible de justifier une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, à savoir la sécurité nationale, en assimilant les menaces contre cette dernière à celles découlant de la criminalité grave.

52. Les difficultés qui se sont manifestées à l'occasion de ce débat lors de l'audience publique, pour délimiter les types d'infractions qui pourraient former ce tertium genus, confirment que cela n'est pas une tâche qui incombe à une juridiction.

53. Il y a lieu de signaler, de plus, que, pour décrire les « activités de nature à déstabiliser gravement les structures » d'un pays et qui, dans cette même mesure, portent atteinte aux « fonctions essentielles de l'État et [aux] intérêts fondamentaux de la société », la Cour se réfère aux « structures constitutionnelles, politiques, économiques ou sociales fondamentales » de ce pays [32].

54. Ces prémisses étant posées, la réglementation irlandaise décrite par la juridiction de renvoi ne diffère pas significativement des législations examinées dans les procédures ayant donné lieu à l'arrêt La Quadrature du Net. Quel que soit le régime d'accès aux données prévu par la loi de 2011 (sur lequel porte la troisième question préjudicielle), les règles de conservation imposées dans cette dernière s'apparentent à celles qui ont été examinées dans cet arrêt, de sorte qu'elles sont également contraires à l'article 15, paragraphe 1, de la directive 2002/58.

[28] Voir arrêt La Quadrature du Net, point 147, selon lequel « 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.

[29] Voir conclusions dans l'affaire Ordre des barreaux francophones et germanophone, point 101.

[30] Arrêt La Quadrature du Net, point 112, citant la jurisprudence.

[31] Avec le soutien d'une bonne partie des gouvernements ayant comparu.

[32] Arrêt La Quadrature du Net, point 135.

55. En effet, la réglementation irlandaise autorise, pour des raisons allant au-delà de celles inhérentes à la protection de la sécurité nationale, la conservation préventive, généralisée et indifférenciée des données relatives au trafic et des données de localisation de tous les abonnés pour une durée de deux ans.

56. En définitive, je propose de répondre aux première, deuxième et quatrième questions préjudicielles posées par la Supreme Court (Cour suprême) dans les mêmes termes que ceux dans lesquels la Cour s'est prononcée dans l'arrêt La Quadrature du Net.

C. Accès aux données conservées (troisième question préjudicielle)

57. La juridiction de renvoi souhaite savoir quels sont les critères dont elle devrait tenir compte pour déterminer si les règles nationales d'accès aux données conservées prévoient le contrôle préalable exigé par la jurisprudence de la Cour, ou si un contrôle, juridictionnel ou indépendant, ex post suffirait.

58. La Cour a également répondu à cette question, dans l'arrêt Prokuratuur. Aux fins de garantir le respect des conditions auxquelles doit satisfaire la réglementation régissant l'accès aux données conservées [33], « il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un *contrôle préalable* effectué soit par une juridiction, soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales » [34].

59. Selon la Cour, ce « contrôle préalable requiert entre autres [...] que la juridiction ou l'entité chargée d'effectuer ledit contrôle préalable dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès » [35].

60. Si le contrôle préalable est confié à une autorité indépendante, celle-ci « doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure » [36].

[33] Réglementation qui « doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause. À cet égard, un tel accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités ». Arrêt Prokuratuur, point 50.

[34] Arrêt Prokuratuur, point 51, mise en italique par mes soins. Dans le même sens que le point 189 de l'arrêt La Quadrature du Net, ce point indique que, « [e]n cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais ».

[35] Arrêt Prokuratuur, point 52.

[36] Arrêt Prokuratuur, point 53.

61. Précisément, « l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable [...] impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique [...] que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale » [37].

62. Ainsi qu'il ressort de la description des règles irlandaises fournie par la juridiction de renvoi, l'accès aux données conservées ne semble pas être soumis au contrôle préalable d'une juridiction ou d'une autorité indépendante, mais à la discrétion d'un fonctionnaire de police d'un certain rang, qui décidera d'introduire ou non la demande auprès des fournisseurs de services.

63. Il appartient à la juridiction de renvoi de vérifier si le fonctionnaire auquel la législation nationale confie le contrôle préalable de l'accès aux données relatives au trafic et aux données de localisation conservées bénéficie du statut d'« autorité indépendante » et de la qualité de « tiers » exigés par la jurisprudence de la Cour.

64. En effectuant cette vérification, la juridiction compétente devra tenir compte du fait que, dans l'arrêt Prokuratuur, la Cour a refusé que ces qualités d'indépendance et de « tiers » soient reconnues au ministère public d'un État membre lorsque celui-ci exerce, par ailleurs, des fonctions d'instruction dans le cadre d'une procédure pénale.

65. En ce qui concerne la possibilité que le contrôle visé par la juridiction de renvoi ait lieu ex post, l'arrêt Prokuratuur apporte également la réponse (négative) :

– « il [ne] peut être suppléé à l'absence de contrôle effectué par une autorité indépendante par un contrôle ultérieur exercé par une juridiction de la légalité de l'accès d'une autorité nationale aux données relatives au trafic et aux données de localisation » ;

– « le contrôle indépendant doit intervenir [...] préalablement à tout accès, sauf cas d'urgence dûment justifiée, auquel cas le contrôle doit intervenir dans de brefs délais » [38].

D. Possibilité de limiter dans le temps les effets d'une constatation d'incompatibilité de la règle nationale avec le droit de l'Union (cinquième et sixième questions)

66. La Supreme Court (Cour suprême) demande, enfin, si :

– elle peut limiter les effets dans le temps d'une constatation d'incompatibilité de la règle nationale avec l'article 15 de la directive 2002/58, lorsque ne pas le faire entraînerait « le chaos et un préjudice grave pour l'intérêt général » ;

– elle peut, lorsqu'elle est saisie d'une demande visant à ce que la règle nationale adoptée pour transposer les dispositions d'une directive ne soit pas appliquée, refuser de faire droit à cette demande ou limiter sa constatation à la période postérieure à l'arrêt de la Cour du 8 avril 2014 [39], dans lequel l'invalidité de la directive 2006/24 a été déclarée.

[37] Arrêt Prokuratuur, point 54.

[38] Arrêt Prokuratuur, point 58.

[39] Arrêt Digital Rights.

67. Là encore, la solution à ces interrogations se trouve dans l'arrêt La Quadrature du Net, dans lequel la Cour a suivi la jurisprudence traditionnelle en la matière.

68. Dans l'affaire C-520/18, la Cour constitutionnelle (Belgique) avait posé à la Cour une question analogue à celle de la Supreme Court (Cour suprême) faisant l'objet du renvoi préjudiciel dans la présente affaire [40].

69. En répondant à cette question dans l'arrêt La Quadrature du Net, la Cour, après avoir rappelé les exigences découlant du principe de primauté du droit de l'Union (points 214 et 215), a réaffirmé sa jurisprudence relative à la limitation des effets de ses arrêts : « Seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit [de l'Union] donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée » [41].

70. Immédiatement après, la Cour a indiqué que, « contrairement à l'omission d'une obligation procédurale telle que l'évaluation préalable des incidences d'un projet dans le domaine spécifique de la protection de l'environnement, une méconnaissance de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle mentionnée au point précédent. En effet, le maintien des effets d'une législation nationale, telle que celle en cause au principal, signifierait que cette législation continue à imposer aux fournisseurs de services de communications électroniques des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées » [42].

71. La Cour a déduit de ces prémisses que « la juridiction de renvoi ne saurait faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, de la législation nationale en cause au principal » [43].

72. Ces considérations sont pleinement applicables aux cinquième et sixième questions préjudicielles posées par la Supreme Court (Cour suprême).

73. Premièrement, il est sans importance que la réglementation nationale litigieuse ait été adoptée en vue de transposer en droit interne la directive 2006/24. Ce qui est déterminant, à cet égard, est que la règle nationale soit conforme, dans son contenu, au droit de l'Union dans son ensemble, ce qui n'est pas le cas en l'espèce.

[40] Au point 213 de l'arrêt La Quadrature du Net, la Cour présente le contenu de la troisième question préjudicielle posée dans l'affaire C-520/18 dans les termes suivants : « la juridiction de renvoi cherche, en substance, à savoir si une juridiction nationale peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, *en vue, entre autres, de la poursuite des objectifs de sauvegarde de la sécurité nationale et de lutte contre la criminalité*, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, résultant de son caractère incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte ». Mise en italique par mes soins.

[41] Arrêt La Quadrature du Net, point 216.

[42] Arrêt La Quadrature du Net, point 219.

[43] Arrêt La Quadrature du Net, point 220.

74. L'invalidité d'une directive, constatée par la Cour en raison de son incompatibilité avec des dispositions matérielles des traités, implique que cette même incompatibilité avec le droit primaire de l'Union affecte les règles nationales qui se bornent à transposer cette directive.

75. La juridiction de renvoi indique que la loi de 2011 a été promulguée afin de satisfaire aux exigences de l'article 288 TFUE, en transposant en droit irlandais la directive 2006/24. Personne ne conteste que ce soit le cas, mais, comme je viens de l'indiquer, ce qui importe est que cette directive était invalide depuis l'origine (ainsi qu'il a été jugé dans l'arrêt Digital Rights), en ce qu'elle impliquait une ingérence disproportionnée dans les droits reconnus par les articles 7 et 8 de la Charte, et que la conservation des données relatives au trafic et des données de localisation doit être régie par la directive 2002/58, telle qu'interprétée par la Cour.

76. Deuxièmement, il est bien connu que les arrêts préjudiciels en interprétation de la Cour produisent des effets dès le moment de l'entrée en vigueur de la règle du droit de l'Union faisant l'objet de l'interprétation [44].

77. Si la limitation dans le temps des effets de l'interprétation du droit de l'Union opérée par la Cour ne peut être admise que dans l'arrêt même statuant sur l'interprétation demandée, je rappellerai que la Cour ne s'est pas prononcée en ce sens dans l'arrêt Digital Rights, que la juridiction de renvoi invoque.

78. Cela n'a pas non plus été le cas dans :

– l'arrêt Tele2 Sverige, rendu le 21 décembre 2016, dans lequel la Cour a interprété la directive 2002/58 en jugeant que celle-ci s'opposait à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans le cadre de la lutte contre la criminalité grave ;

– l'arrêt La Quadrature du Net, dans lequel la Cour a, le 6 octobre 2020, encore confirmé l'interprétation de la directive 2002/58 dans le sens qui a déjà été expliqué.

79. Troisièmement, le présent renvoi préjudiciel n'a pas pour objet la résolution des problèmes liés à l'exclusion des éléments de preuve dans la procédure pénale menée contre la personne condamnée pour meurtre. Il s'agit ici, au contraire, d'une procédure *civile* [comme la qualifie la Supreme Court (Cour suprême)] dans laquelle il y a lieu de statuer au regard du contraste objectif entre la législation nationale et le droit de l'Union.

80. La juridiction de renvoi le signale dans les termes suivants : « Dans le cadre de l'appel actuellement pendant devant la juridiction de céans [la Supreme Court (Cour suprême)], la seule question qui se pose est celle de savoir si c'est à juste titre que la High Court (Haute Cour) a jugé que l'article 6, paragraphe 1, sous a), [de la loi de 2011] était contraire au droit de l'Union » [45].

[44] Conformément à une jurisprudence constante, l'interprétation que la Cour effectue d'une règle du droit de l'Union, dans l'exercice de la compétence que lui confère l'article 267 TFUE, éclaire et précise la signification et la portée de cette règle, telle qu'elle doit ou aurait dû être comprise et appliquée depuis le moment de sa mise en vigueur. Il en résulte que le juge peut et doit appliquer la règle ainsi interprétée à des rapports juridiques nés et constitués avant le prononcé de l'arrêt statuant sur la demande d'interprétation si, par ailleurs, les conditions permettant de porter devant les juridictions compétentes un litige relatif à l'application de cette règle se trouvent réunies (arrêts du 3 octobre 2019, Schuch-Ghannadan, C-274/18, EU:C:2019:828, point 60, et du 16 septembre 2020, Romenergo et Aris Capital, C-339/19, EU:C:2020:709, point 47).

[45] Décision de renvoi, point 6 de l'annexe II, in fine.

81. La réponse à cette « seule question » est que l'article 6, paragraphe 1, sous a), de la loi de 2011 n'est pas conforme au droit de l'Union et qu'il n'y a pas de raison de reporter dans le temps la portée de l'arrêt qui doit ainsi le constater.

V. Conclusion

82. Eu égard à ce qui précède, je propose à la Cour de répondre à la Supreme Court (Cour suprême, Irlande) comme suit :

1) L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne 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 finaux de ces services à des fins autres que la sauvegarde de la sécurité nationale face à une menace qui s'avère réelle et actuelle ou prévisible ;

   – ne subordonne pas l'accès des autorités compétentes aux données relatives au trafic et aux données de localisation conservées à un contrôle préalable effectué par une juridiction ou par une entité administrative indépendante.

2) Une juridiction nationale ne saurait limiter dans le temps les effets d'une déclaration d'illégalité d'une réglementation interne imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux.