ARRÊT DE LA COUR (grande chambre)
20 septembre 2022 (*)

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Confidentialité des communications – Fournisseurs de services de communications électroniques – Conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – Directive 2002/58/CE – Article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 6, 7, 8 et 11 ainsi que article 52, paragraphe 1 – Article 4, paragraphe 2, TUE »

Dans les affaires jointes C-793/19 et C-794/19,

ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne), par décisions du 25 septembre 2019, parvenues à la Cour le 29 octobre 2019, dans les procédures

Bundesrepublik Deutschland, représentée par la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

contre

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. A. Arabadjiev, M^me^ A. Prechal, MM. S. Rodin, I. Jarukaitis et M^me^ I. Ziemele, présidents de chambre, MM. T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (rapporteur), N. Piçarra, M^me^ L. S. Rossi et M. A. Kumin, juges,

avocat général : M. M. Campos Sánchez-Bordona,

greffier : M. D. Dittert, chef d'unité,

vu la procédure écrite et à la suite de l'audience du 13 septembre 2021,

considérant les observations présentées :

pour la Bundesrepublik Deutschland, représentée par la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, par M. C. Mögelin, en qualité d'agent,

pour SpaceNet AG, par M^e^ M. Bäcker, Rechtsanwalt,

pour Telekom Deutschland GmbH, par M^e^ T. Mayen, Rechtsanwalt,

pour le gouvernement allemand, par MM. J. Möller, F. Halibi, M. Hellmann, D. Klebs et E. Lankenau, en qualité d'agents,

pour le gouvernement danois, par MM. M. Jespersen, J. Nymann-Lindegren, M^mes^ V. Pasternak Jørgensen et M. Søndahl Wolff, en qualité d'agents,

pour le gouvernement estonien, par M^mes^ A. Kalbus et M. Kriisa, en qualité d'agents,

pour l'Irlande, par M. A. Joyce et M^me^ J. Quaney, en qualité d'agents, assistés de M. D. Fennelly, BL, et de M. P. Gallagher, SC,

pour le gouvernement espagnol, par M. L. Aguilera Ruiz, en qualité d'agent,

pour le gouvernement français, par M^me^ A. Daniel, MM. D. Dubois, J. Illouz, M^me^ E. de Moustier et M. T. Stéhelin, en qualité d'agents,

pour le gouvernement chypriote, par M^me^ I. Neophytou, en qualité d'agent,

pour le gouvernement néerlandais, par M^mes^ M. K. Bulterman, A. Hanje et C. S. Schillemans, en qualité d'agents,

pour le gouvernement polonais, par M. B. Majczyna, M^mes^ D. Lutostańska et J. Sawicka, en qualité d'agents,

pour le gouvernement finlandais, par M^mes^ A. Laine et M. Pere, en qualité d'agents,

pour le gouvernement suédois, par M^mes^ H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson et H. Shev, en qualité d'agents,

pour la Commission européenne, par MM. G. Braun, S. L. Kalėda, H. Kranenborg, M. Wasmeier et F. Wilman, en qualité d'agents,

pour le Contrôleur européen de la protection des données, par M^me^ A. Buchta, MM. D. Nardi, N. Stolič et K. Ujazdowski, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 18 novembre 2021,

rend le présent

Arrêt

Les demandes de décision préjudicielle portent sur l'interprétation de 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) (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 »), lu à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») et de l'article 4, paragraphe 2, TUE.

Ces demandes ont été présentées dans le cadre de litiges opposant la Bundesrepublik Deutschland (République fédérale d'Allemagne), représentée par la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer, Allemagne), à SpaceNet AG (affaire C-793/19) et à Telekom Deutschland GmbH (affaire C-794/19) au sujet de l'obligation imposée à ces dernières de conserver des données relatives au trafic et des données de localisation afférentes aux télécommunications de leurs clients.

Le cadre juridique

Le droit de l'Union

La directive 95/46/CE

La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31), a été abrogée, avec effet au 25 mai 2018, par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46 (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

L'article 3, paragraphe 2, de la directive 95/46 disposait :

« La présente directive ne s'applique pas au traitement de données à caractère personnel :

mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

La directive 2002/58

Les considérants 2, 6, 7 et 11 de la directive 2002/58 énoncent :

La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la [Charte]. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de [celle-ci].

L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

À l'instar de la directive [95/46], la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, [signée à Rome le 4 novembre 1950], telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. »

L'article 1er de cette directive, intitulé « Champ d'application et objectif », dispose :

« 1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive [95/46] aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du [traité FUE], telles que celles visées dans les titres V et VI du traité [UE], et, en tout état de cause, aux activités concernant la sécurité publique,

la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal. »

Aux termes de l'article 2 de ladite directive, intitulé « Définitions » :

« Sauf disposition contraire, les définitions figurant dans la directive [95/46] et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive "cadre") [(JO 2002, L 108, p. 33),] s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

"utilisateur" : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

"données relatives au trafic" : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ;

"données de localisation" : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ;

"communication" : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit ;

[...] »

L'article 3 de la directive 2002/58, intitulé « Services concernés », prévoit :

« La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification. »

Aux termes de l'article 5 de cette directive, intitulé « Confidentialité des communications » :

« 1. 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.

[...]

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive [95/46], une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »

L'article 6 de la directive 2002/58, intitulé « Données relatives au trafic », 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.

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

[...]

5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée ; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

[...] »

L'article 9 de cette directive, intitulé « Données de localisation autres que les données relatives au trafic », prévoit, à son paragraphe 1 :

« Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au

public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. [...] »

L'article 15 de la directive 2002/58, intitulé « Application de certaines dispositions de la directive [95/46] », énonce, 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]. 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, [TUE]. »

Le droit allemand

Le TKG

L'article 113a, paragraphe 1, première phrase, du Telekommunikationsgesetz (loi sur les télécommunications), du 22 juin 2004 (BGBl. 2004 I, p. 1190), dans sa version applicable au litige au principal (ci-après le « TKG »), est libellé comme suit :

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

En vertu de l'article 113b du TKG :

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

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

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 :

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, 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,

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

Le premier alinéa s'applique mutatis mutandis

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

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

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

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.

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

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

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

[...] »

Les communications visées à l'article 99, paragraphe 2, du TKG, auxquelles l'article 113b, paragraphe 6, du TKG renvoie, sont des communications avec des personnes, des autorités et des organisations à caractère social ou religieux qui proposent uniquement ou essentiellement à des appelants restant en principe anonymes des services

d'assistance téléphonique en cas de situation d'urgence psychologique ou sociale et qui sont elles-mêmes soumises ou dont les collaborateurs sont soumis à des obligations de confidentialité particulières à cet égard. La dérogation prévue à l'article 99, paragraphe 2, deuxième et quatrième phrases, du TKG est subordonnée à l'inscription des appelés, à leur demande, sur une liste établie par l'Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer, après que les titulaires des numéros d'appel ont établi leur mission en produisant une attestation d'une autorité, d'un organisme, d'un établissement ou d'une fondation de droit public.

Aux termes de l'article 113c, paragraphes 1 et 2, du TKG :

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

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 ;

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

[...]

(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. »

L'article 113d du TKG énonce :

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

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

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

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

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

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. »

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

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

l'heure de l'accès,

les personnes accédant aux données,

l'objet et la nature de l'accès.

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

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

Afin de garantir un niveau de sécurité et de qualité des données particulièrement élevé, l'Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer établit, conformément à l'article 113f, paragraphe 1, du TKG, un ensemble d'exigences qui, en vertu de l'article 113f, paragraphe 2, de celui-ci, doit être évalué en permanence et adapté le cas échéant. L'article 113g du TKG exige que des mesures de sécurité spécifiques soient intégrées dans l'exposé de la politique en matière de sécurité qui doit être présenté par le débiteur.

La StPO

L'article 100g, paragraphe 2, première phrase, de la Strafprozessordnung (code de procédure pénale, ci-après la « StPO ») est libellé comme suit :

« Si certains faits permettent de soupçonner que quelqu'un a commis, en qualité d'auteur ou de complice, l'une des infractions pénales particulièrement graves visées dans la deuxième phrase ou, dans les cas dans lesquels la tentative est punissable, a tenté de commettre une telle infraction et si l'infraction est également particulièrement grave dans le cas particulier, les données relatives au trafic, conservées 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. »

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

Les litiges au principal et la question préjudicielle

SpaceNet et Telekom Deutschland fournissent, en Allemagne, des services d'accès à Internet accessibles au public. La deuxième fournit, en outre, également en Allemagne, des services téléphoniques accessibles au public.

Ces fournisseurs de services ont contesté devant le Verwaltungsgericht Köln (tribunal administratif de Cologne, Allemagne) l'obligation qui leur est imposée par les dispositions combinées de l'article 113a, paragraphe 1, et de l'article 113b du TKG de conserver des données relatives au trafic et des données de localisation afférentes aux télécommunications de leurs clients à compter du 1er juillet 2017.

Par arrêts du 20 avril 2018, le Verwaltungsgericht Köln (tribunal administratif de Cologne) a jugé que SpaceNet et Telekom Deutschland n'étaient pas tenues de conserver les données relatives au trafic afférentes aux télécommunications, visées à l'article 113b, paragraphe 3, du TKG, des clients auxquels elles fournissent un accès à Internet et que Telekom Deutschland n'était, en outre, pas tenue de conserver les données relatives au trafic afférentes aux télécommunications, visées à l'article 113b, paragraphe 2, première et deuxième phrases, du TKG, des clients auxquels elle fournit un accès à des services de téléphonie accessibles au public. Cette juridiction a, en effet, considéré, à la lumière de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), que cette obligation de conservation était contraire au droit de l'Union.

La République fédérale d'Allemagne a formé des recours en *Revision* contre ces arrêts devant le Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne), la juridiction de renvoi.

Celle-ci estime que la question de savoir si l'obligation de conservation imposée par les dispositions combinées de l'article 113a, paragraphe 1, et de l'article 113b du TKG est contraire au droit de l'Union dépend de l'interprétation de la directive 2002/58.

À cet égard, la juridiction de renvoi relève que la Cour a déjà établi de manière définitive, dans l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), que des réglementations portant sur la conservation des données relatives au trafic et des données de localisation ainsi que sur l'accès à ces données par les autorités nationales relèvent, en principe, du champ d'application de la directive 2002/58.

Elle relève également que l'obligation de conservation en cause au principal, en ce qu'elle limite les droits découlant de l'article 5, paragraphe 1, de l'article 6, paragraphe 1, et de l'article 9, paragraphe 1, de la directive 2002/58, ne pourrait être justifiée que sur le fondement de l'article 15, paragraphe 1, de cette directive.

À cet égard, elle rappelle qu'il ressort de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

Or, selon la juridiction de renvoi, à l'instar des réglementations nationales en cause dans les affaires ayant donné lieu audit arrêt, la réglementation nationale en cause au principal n'exige aucun motif pour la conservation des données ni un quelconque lien entre les données conservées et une infraction pénale ou un risque pour la sécurité publique. En effet, cette réglementation nationale imposerait la conservation, sans motif, généralisée et non différenciée d'un point de vue personnel, temporel et géographique, de la majeure partie des données pertinentes relatives au trafic qui sont afférentes à des télécommunications.

La juridiction de renvoi considère, toutefois, qu'il n'est pas exclu que l'obligation de conservation en cause au principal puisse être justifiée en vertu de l'article 15, paragraphe 1, de la directive 2002/58.

En premier lieu, elle relève que, contrairement aux réglementations nationales en cause dans les affaires ayant donné lieu à l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), la réglementation nationale en cause au principal n'exige pas la conservation de l'ensemble des données relatives au trafic qui sont afférentes aux télécommunications de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique. Non seulement le contenu des communications serait exclu de l'obligation de conservation, mais les données relatives aux sites Internet consultés, les données des services de courrier électronique et les données qui sous-tendent les communications à caractère social ou religieux vers ou à partir de certaines lignes ne pourraient pas être conservées, ainsi qu'il ressort de l'article 113b, paragraphes 5 et 6, du TKG.

En deuxième lieu, cette juridiction indique que l'article 113b, paragraphe 1, du TKG prévoit une durée de conservation de quatre semaines pour les données de localisation et de dix semaines pour les données relatives au trafic, alors que la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54), sur laquelle les réglementations nationales en cause dans les affaires ayant donné lieu à l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), étaient fondées, prévoyait une durée de conservation comprise entre six mois et deux ans.

Or, selon la juridiction de renvoi, si l'exclusion de certains moyens de communication ou de certaines catégories de données et la limitation de la durée de conservation ne suffisent pas à éliminer tout risque d'établissement d'un profil complet des personnes concernées, ce risque serait à tout le moins considérablement réduit dans le cadre de la mise en œuvre de la réglementation nationale en cause au principal.

En troisième lieu, cette réglementation comporterait des limitations strictes en ce qui concerne la protection des données conservées et l'accès à celles-ci. Ainsi, d'une part, elle garantirait une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données. D'autre part, les données conservées ne pourraient être utilisées qu'aux fins de la lutte contre les infractions graves ou aux fins de la prévention d'un risque concret pour l'intégrité physique, la vie ou la liberté d'une personne ou bien pour l'existence de l'État fédéral ou d'un Land.

En quatrième lieu, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 dans le sens d'une incompatibilité générale avec le droit de l'Union de toute conservation de données sans motif pourrait se heurter à l'obligation d'agir des États membres, découlant du droit à la sûreté consacré à l'article 6 de la Charte.

En cinquième lieu, la juridiction de renvoi estime qu'une interprétation de l'article 15 de la directive 2002/58 comme s'opposant à une conservation généralisée des données restreindrait considérablement la marge de manœuvre du législateur national dans un domaine touchant à la répression des crimes et à la sécurité publique, lequel resterait, conformément à l'article 4, paragraphe 2, TUE, de la seule responsabilité de chaque État membre.

En sixième lieu, la juridiction de renvoi estime qu'il y a lieu de tenir compte de la jurisprudence de la Cour européenne des droits de l'homme et relève que celle-ci a jugé que l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la « CEDH ») ne s'opposait pas à des dispositions nationales prévoyant l'interception massive des flux transfrontières de données, eu égard aux menaces auxquelles sont actuellement confrontés de nombreux États et aux outils technologiques sur lesquels peuvent désormais s'appuyer les terroristes et les criminels pour commettre des actes répréhensibles.

C'est dans ce contexte que le Bundesverwaltungsgericht (Cour administrative fédérale) a décidé de surseoir à statuer et de poser à la Cour la question préjudicielle suivante :

« L'article 15 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], d'une part, et de l'article 6 de [ladite Charte] ainsi que de l'article 4 [TUE], 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,

'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,

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 ? »

La procédure devant la Cour

Par décision du président de la Cour du 3 décembre 2019, les affaires C-793/19 et C-794/19 ont été jointes aux fins des phases écrite et orale de la procédure ainsi que de l'arrêt.

Par décision du président de la Cour du 14 juillet 2020, la procédure dans les affaires jointes C-793/19 et C-794/19 a été suspendue en application de l'article 55, paragraphe 1, sous b), du règlement de procédure de la Cour, jusqu'au prononcé de l'arrêt dans l'affaire La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18).

La Cour ayant rendu, le 6 octobre 2020, son arrêt dans l'affaire La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), le président de la Cour a ordonné, le 8 octobre 2020, la reprise de la procédure dans

les affaires jointes C-793/19 et C-794/19.

La juridiction de renvoi, à laquelle le greffe avait communiqué cet arrêt, a indiqué qu'elle maintenait sa demande de décision préjudicielle.

À cet égard, cette juridiction de renvoi a, tout d'abord, fait observer que l'obligation de conservation prévue par la réglementation en cause au principal concerne un nombre de données moindre et une durée de conservation moins élevée que ce que prévoyaient les réglementations nationales en cause dans les affaires ayant conduit à l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791). Ces particularités réduiraient la possibilité que les données conservées puissent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées.

Ensuite, elle a de nouveau indiqué que la réglementation nationale en cause au principal assure une protection efficace des données conservées contre les risques d'abus et d'accès illicite.

Enfin, elle a souligné que des incertitudes subsistent en ce qui concerne la question de la compatibilité avec le droit de l'Union de la conservation des adresses IP, prévue par la réglementation nationale en cause au principal, en raison d'une incohérence entre les points 155 et 168 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791). Ainsi, selon la juridiction de renvoi, une incertitude découlerait de cet arrêt quant à la question de savoir si la Cour exige, pour la conservation des adresses IP, un motif de conservation lié à l'objectif de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave ou de prévention des menaces graves contre la sécurité publique, ainsi qu'il résulterait du point 168 dudit arrêt, ou si la conservation des adresses IP est permise même en l'absence de motif concret, seule l'utilisation des données conservées étant limitée par lesdits objectifs, ainsi qu'il résulterait du point 155 du même arrêt.

Sur la question préjudicielle

Par sa question préjudicielle, la juridiction de renvoi cherche, en substance, à savoir si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe l, de la Charte et de l'article 4, paragraphe 2, TUE, doit être interprété en ce sens qu'il s'oppose à une mesure législative nationale qui, hormis certaines exceptions, impose aux fournisseurs de services de communications électroniques accessibles au public, à des fins énumérées à l'article 15, paragraphe 1, de cette directive, et notamment aux fins de la répression des infractions pénales graves ou de la prévention d'un risque concret pour la sécurité nationale, la conservation généralisée et indifférenciée de l'essentiel des données relatives au trafic et des données de localisation des utilisateurs finals de ces services, en prévoyant une durée de conservation de plusieurs semaines ainsi que des règles visant à garantir une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données.

Sur l'applicabilité de la directive 2002/58

S'agissant de l'argumentation de l'Irlande ainsi que des gouvernements français, néerlandais, polonais et suédois selon laquelle la réglementation nationale en cause au principal, en ce qu'elle a été adoptée notamment aux fins de la sauvegarde de la sécurité nationale, ne relève pas du champ d'application de la directive 2002/58, il suffit de rappeler 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 notamment de la protection de la sécurité nationale et de la lutte contre la criminalité, telle que celle en cause au principal, relève du champ d'application de la directive 2002/58 (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 104).

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

Rappel des principes issus de la jurisprudence de la Cour

Il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 32 ainsi que jurisprudence citée).

Il ressort des termes mêmes de l'article 15, paragraphe 1, de la directive 2002/58 que les mesures législatives que celle-ci autorise les États membres à prendre, dans les conditions qu'elle fixe, peuvent seulement viser « à limiter la portée » des droits et des obligations prévus notamment aux articles 5, 6 et 9 de la directive 2002/58 (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 33).

S'agissant du système mis en place par cette directive et dans lequel s'insère l'article 15, paragraphe 1, de celle-ci, il y a lieu de rappeler que, en vertu de l'article 5, paragraphe 1, première et deuxième phrases, de ladite directive, les États membres sont tenus de garantir, par leur 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 ont l'obligation d'interdire 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, de la même directive (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 34).

À cet égard, la Cour a déjà jugé que l'article 5, paragraphe 1, de la directive 2002/58 consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et ces données (arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 107, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 35).

Cette disposition reflète l'objectif poursuivi par le législateur de l'Union lors de l'adoption de la directive 2002/58. En effet, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil

concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM(2000) 385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu « faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée ». Ladite directive a ainsi pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, comme l'énonce le considérant 2 de la même directive, la volonté du législateur de l'Union est de garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte, relatifs, respectivement, à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 36 ainsi que jurisprudence citée).

En adoptant la directive 2002/58, le législateur de l'Union a ainsi concrétisé ces droits, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement (arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 109, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 37).

S'agissant du traitement et du stockage par les fournisseurs de services de communications électroniques des données relatives au trafic concernant les abonnés et les utilisateurs, l'article 6 de la directive 2002/58 prévoit, à son paragraphe 1, que ces données doivent être effacées ou rendues anonymes, lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, et précise, à son paragraphe 2, que les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion ne peuvent être traitées 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. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive énonce que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés.

Partant, la directive 2002/58 ne se limite pas à encadrer l'accès à de telles données par des garanties visant à prévenir les abus, mais consacre aussi, en particulier, le principe de l'interdiction de leur stockage par des tiers (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 39).

En ce que l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'adopter des mesures législatives visant à « limiter la portée » des droits et des obligations prévus notamment aux articles 5, 6 et 9 de cette directive, tels que ceux découlant des principes de confidentialité des communications et de l'interdiction du stockage des données y afférentes, rappelés au point 52 du présent arrêt, cette disposition énonce une exception à la règle générale prévue notamment à ces articles 5, 6 et 9 et doit ainsi, conformément à une jurisprudence constante, faire l'objet d'une interprétation stricte. Une telle disposition ne saurait donc justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de ladite directive, devienne la règle, sauf à vider largement cette dernière disposition de sa portée (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 40 ainsi que jurisprudence citée).

Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 41 ainsi que jurisprudence citée).

En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les mesures prises par les États membres au titre de cette disposition doivent respecter les principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et assurer le respect des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une législation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, mais également de l'article 11 de la Charte, relatif à la liberté d'expression, cette liberté constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union européenne (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, points 42 et 43 ainsi que jurisprudence citée).

Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible, si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence, ou encore si les données conservées seront ou non utilisées par la suite (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 44 ainsi que jurisprudence citée).

Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes

concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 45 ainsi que jurisprudence citée).

Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci, effets qui sont d'autant plus graves que le nombre et la variété des données conservées sont élevés. D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 46 ainsi que jurisprudence citée).

Cela étant, en ce qu'il permet aux États membres de limiter les droits et les obligations visés aux points 51 à 54 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète le fait que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais qu'ils doivent être pris en considération par rapport à leur fonction dans la société. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 48 ainsi que jurisprudence citée).

Ainsi, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, il convient de tenir compte du fait que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4, s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 49 ainsi que jurisprudence citée).

Face à ces différentes obligations positives, il convient donc de procéder à une conciliation des différents intérêts légitimes et droits en cause et d'instaurer un cadre légal permettant cette conciliation (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 50 ainsi que jurisprudence citée).

Dans ce cadre, il découle des termes mêmes de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité évoqué au point 52 du présent arrêt lorsqu'une telle mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », le considérant 11 de cette directive indiquant, à cet effet, qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi.

À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, et ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 52 ainsi que jurisprudence citée).

Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 53 ainsi que jurisprudence citée).

Pour satisfaire à l'exigence de proportionnalité, une législation nationale doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette législation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au

strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 54 ainsi que jurisprudence citée).

Ainsi, une législation nationale prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 55 ainsi que jurisprudence citée).

S'agissant des objectifs d'intérêt général susceptibles de justifier une mesure prise en vertu de l'article 15, paragraphe 1, de la directive 2002/58, il ressort de la jurisprudence de la Cour, en particulier de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), que, conformément au principe de proportionnalité, il existe une hiérarchie entre ces objectifs en fonction de leur importance respective et que l'importance de l'objectif poursuivi par une telle mesure doit être en relation avec la gravité de l'ingérence qui en résulte (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 56).

Ainsi, s'agissant de la 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, la Cour a constaté que cette disposition, lue 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 (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 58 ainsi que jurisprudence citée).

S'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, la Cour a relevé que, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 59 ainsi que jurisprudence citée).

En ce qui concerne l'objectif de lutte contre la criminalité grave, la Cour a jugé qu'une législation nationale prévoyant, à cette fin, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique. En effet, eu égard au caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 62 du présent arrêt, que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit, comme le prévoit le système mis en place par la directive 2002/58, l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 65 ainsi que jurisprudence citée).

En revanche, la Cour a précisé 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 à des mesures législatives prévoyant, aux fins 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 ;

une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

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 *(quick freeze)* 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 (arrêts du 6 octobre 2020, La Quadrature du

Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 67).

Sur une mesure prévoyant, pour une durée de plusieurs semaines, une conservation généralisée et indifférenciée de la majeure partie des données relatives au trafic et des données de localisation

C'est à l'aune de ces considérations de principe qu'il convient d'examiner les caractéristiques de la réglementation nationale en cause au principal, mises en exergue par la juridiction de renvoi.

En premier lieu, en ce qui concerne l'étendue des données conservées, il ressort de la décision de renvoi que, dans le cadre de la fourniture de services téléphoniques, l'obligation de conservation édictée par cette réglementation porte, notamment, sur les données nécessaires pour identifier la source d'une communication et la destination de celle-ci, 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 ainsi que, en cas d'utilisation mobile, la désignation des cellules qui ont été utilisées par l'appelant et l'appelé au début de la communication. Dans le cadre de la fourniture de services d'accès à Internet, l'obligation de conservation porte, entre autres, sur l'adresse IP attribuée à l'abonné, la date et l'heure du début et de la fin de l'utilisation d'Internet à partir de l'adresse IP attribuée et, en cas d'utilisation mobile, la désignation des cellules utilisées au début de la connexion Internet. Les données permettant de connaître la position géographique et les directions du rayonnement maximal des antennes desservant la cellule concernée sont également conservées.

Si la réglementation nationale en cause au principal exclut de l'obligation de conservation le contenu de la communication et les données relatives aux sites Internet consultés et n'impose la conservation de l'identifiant cellulaire qu'au début de la communication, il convient de faire observer qu'il en allait de même, en substance, des réglementations nationales transposant la directive 2006/24 qui étaient en cause dans les affaires ayant donné lieu à l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791). Or, en dépit de ces limitations, la Cour a jugé dans cet arrêt que les catégories de données conservées au titre de ladite directive et de ces réglementations nationales étaient susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes concernées, 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 et, en particulier, de fournir les moyens d'établir le profil de ces personnes.

Il importe de surcroît de constater que, si la réglementation en cause au principal ne couvre pas les données relatives aux sites Internet consultés, elle prévoit néanmoins la conservation des adresses IP. Or, ces adresses pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 153).

En outre, et ainsi que l'a relevé SpaceNet dans ses observations écrites, les données afférentes aux services de courrier électronique, bien qu'elles ne soient pas couvertes par l'obligation de conservation prévue par la réglementation en cause au principal, ne représentent qu'une infime partie des données en cause.

Ainsi, comme l'a relevé M. l'avocat général, en substance, au point 60 de ses conclusions, l'obligation de conservation prévue par la réglementation nationale en cause au principal s'étend à un ensemble très large de données relatives au trafic et de données de localisation, qui correspond, en substance, à ceux ayant conduit à la jurisprudence constante rappelée au point 78 du présent arrêt.

De plus, en réponse à une question posée lors de l'audience, le gouvernement allemand a précisé que seulement 1 300 entités étaient inscrites sur la liste des personnes, des autorités ou des organisations à caractère social ou religieux dont les données afférentes aux communications électroniques ne sont pas conservées en vertu de l'article 99, paragraphe 2, et de l'article 113 b, paragraphe 6, du TKG, ce qui représente manifestement une part réduite de l'ensemble des utilisateurs des services de télécommunication en Allemagne dont les données relèvent de l'obligation de conservation prévue par la réglementation nationale en cause au principal. Sont ainsi conservées, notamment, les données d'utilisateurs soumis au secret professionnel, tels que les avocats, les médecins et les journalistes.

Il ressort donc de la décision de renvoi que la conservation des données relatives au trafic et des données de localisation prévue par cette réglementation nationale concerne la quasi-totalité des personnes composant la population sans que celles-ci se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. De même, elle impose la conservation, sans motif, généralisée et non différenciée d'un point de vue personnel, temporel et géographique, de l'essentiel des données relatives au trafic et des données de localisation dont l'étendue correspond, en substance, à celle des données conservées dans les affaires ayant conduit à la jurisprudence visée au point 78 du présent arrêt.

Partant, eu égard à la jurisprudence citée au point 75 du présent arrêt, une obligation de conservation des données telle que celle en cause au principal ne peut être considérée comme étant une conservation ciblée des données, contrairement à ce que soutient le gouvernement allemand.

En deuxième lieu, en ce qui concerne la durée de conservation des données, il découle de l'article 15, paragraphe 1, deuxième phrase, de la directive 2002/58 que la durée de conservation prévue par une mesure nationale imposant une obligation de conservation généralisée et indifférenciée est, certes, un facteur pertinent, parmi d'autres, afin de déterminer si le droit de l'Union s'oppose à une telle mesure, ladite phrase exigeant que cette durée soit « limitée ».

Or, en l'occurrence, il est vrai que ces durées, qui s'élèvent, selon l'article 113b, paragraphe 1, du TKG, à quatre semaines pour les données de localisation et à dix semaines pour les autres données, sont sensiblement plus courtes que celles prévues par les réglementations nationales imposant une obligation de conservation généralisée et indifférenciée examinées par la Cour dans ses arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a.

(C-203/15 et C-698/15, EU:C:2016:970), du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258).

Toutefois, ainsi qu'il ressort de la jurisprudence citée au point 61 du présent arrêt, la gravité de l'ingérence découle du risque, notamment eu égard à leur nombre et à leur variété, que les données conservées, prises dans leur ensemble, permettent de tirer des conclusions très précises concernant la vie privée de la ou des personnes dont les données ont été conservées et, en particulier, fournissent les moyens d'établir le profil de la ou des personnes concernées, qui est une information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

Partant, la conservation des données relatives au trafic ou des 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 de conservation, de la quantité ou de la nature des données conservées, lorsque ledit ensemble de données est susceptible de permettre de tirer des conclusions très précises concernant la vie privée de la ou des personnes concernées [voir, en ce qui concerne l'accès à de telles données, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 39].

À cet égard, même la conservation d'une quantité limitée de données relatives au trafic ou de données de localisation ou la conservation de ces données sur une courte période sont susceptibles de fournir des informations très précises sur la vie privée d'un utilisateur d'un moyen de communication électronique. En outre, la quantité des données disponibles et les informations très précises sur la vie privée de la personne concernée en découlant ne peuvent être appréciées qu'après la consultation desdites données. Or, l'ingérence résultant de la conservation desdites données intervient nécessairement avant que les données et les informations en découlant puissent être consultées. Ainsi, l'appréciation de la gravité de l'ingérence que constitue la conservation s'effectue nécessairement en fonction du risque généralement afférent à la catégorie de données conservées pour la vie privée des personnes concernées, sans qu'il importe, par ailleurs, de savoir si les informations relatives à la vie privée en découlant présentent ou non, concrètement, un caractère sensible [voir, en ce sens, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 40].

En l'occurrence, ainsi qu'il ressort du point 77 du présent arrêt et qu'il a été confirmé lors de l'audience, un ensemble de données relatives au trafic et de données de localisation conservées pendant, respectivement, dix semaines et quatre semaines peut permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données sont 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, et, en particulier, d'établir un profil desdites personnes.

En troisième lieu, en ce qui concerne les garanties prévues par la réglementation nationale en cause au principal, visant à protéger les données conservées contre les risques d'abus et contre tout accès illicite, il convient de relever que la conservation de ces données et l'accès à celles-ci constituent, ainsi qu'il ressort de la jurisprudence rappelée au point 60 du présent arrêt, des ingérences distinctes dans les droits fondamentaux garantis aux articles 7 et 11 de la Charte, nécessitant une justification distincte, au titre de l'article 52, paragraphe 1, de celle-ci. Il en découle qu'une législation nationale assurant le plein respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 en matière d'accès aux données conservées ne saurait, par nature, être susceptible ni de limiter ni même de remédier à l'ingérence grave, qui résulterait de la conservation généralisée de ces données prévue par cette législation nationale, dans les droits garantis aux articles 5 et 6 de cette directive et par les droits fondamentaux dont ces articles constituent la concrétisation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 47).

En quatrième et dernier lieu, en ce qui concerne l'argument de la Commission européenne selon lequel la criminalité particulièrement grave pourrait être assimilée à une menace pour la sécurité nationale, la Cour a déjà jugé que l'objectif de préservation de la sécurité nationale correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, par la prévention et la répression des activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que des activités de terrorisme (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 61 ainsi que jurisprudence citée).

À la différence de la criminalité, même particulièrement grave, une menace pour la sécurité nationale doit être réelle et actuelle ou, à tout le moins, prévisible, ce qui suppose la survenance de circonstances suffisamment concrètes, pour pouvoir justifier une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, pendant une durée limitée. Une telle menace se distingue donc, par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent, du risque général et permanent qu'est celui de survenance de tensions ou de troubles, même graves, à la sécurité publique ou celui d'infractions pénales graves (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 62 ainsi que jurisprudence citée).

Ainsi, la criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale. En effet, une telle assimilation serait susceptible d'introduire une catégorie intermédiaire entre la sécurité nationale et la sécurité publique, aux fins d'appliquer à la seconde les exigences inhérentes à la première (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 63).

Sur les mesures prévoyant une conservation ciblée, une conservation rapide ou une conservation des adresses IP

Plusieurs gouvernements, dont le gouvernement français, soulignent que seule une conservation généralisée et indifférenciée permet la réalisation efficace des objectifs visés par les mesures de conservation, le gouvernement allemand précisant, en substance, qu'une telle conclusion n'est pas infirmée par le fait que les États membres peuvent avoir recours aux mesures de conservation ciblée et de conservation rapide visées au point 75 du présent arrêt.

À cet égard, il convient de relever, en premier lieu, que l'efficacité de poursuites pénales dépend généralement non pas d'un seul instrument d'enquête, mais de tous les instruments d'enquête dont disposent les autorités nationales compétentes à ces fins (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 69).

En deuxième lieu, 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, tel qu'interprété par la jurisprudence rappelée au point 75 du présent arrêt, permet aux États membres d'adopter, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, non seulement des mesures instituant une conservation ciblée et une conservation rapide, mais également des mesures prévoyant une conservation généralisée et indifférenciée, d'une part, des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques et, d'autre part, des adresses IP attribuées à la source d'une connexion (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 70).

À cet égard, il est constant que la conservation des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques est susceptible de contribuer à la lutte contre la criminalité grave, pour autant que ces données permettent d'identifier les personnes ayant utilisé de tels moyens dans le contexte de la préparation ou de la commission d'un acte relevant de la criminalité grave (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 71).

Or, la directive 2002/58 ne s'oppose pas, aux fins de la lutte contre la criminalité en général, à la conservation généralisée des données relatives à l'identité civile. Dans ces conditions, il y a lieu de préciser que ni cette directive ni aucun autre acte du droit de l'Union ne s'opposent à une législation nationale, ayant pour objet la lutte contre la criminalité grave, en vertu de laquelle l'acquisition d'un moyen de communication électronique, tel qu'une carte SIM prépayée, est subordonnée à la vérification de documents officiels établissant l'identité de l'acheteur et à l'enregistrement, par le vendeur, des informations en résultant, le vendeur étant le cas échéant tenu de donner accès à ces informations aux autorités nationales compétentes (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 72).

En outre, il y a lieu de rappeler que la conservation généralisée des adresses IP de la source de la connexion constitue une ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte dès lors que ces adresses IP peuvent permettre de tirer des conclusions précises sur la vie privée de l'utilisateur du moyen de communication électronique concerné et peut avoir des effets dissuasifs sur l'exercice de la liberté d'expression garantie à l'article 11 de celle-ci. Toutefois, s'agissant d'une telle conservation, la Cour a constaté qu'il y a lieu, aux fins de la conciliation nécessaire des droits et des intérêts légitimes en cause exigée par la jurisprudence visée aux points 65 à 68 du présent arrêt, de tenir compte du fait que, dans le cas d'une infraction commise en ligne et, en particulier, dans le cas de l'acquisition, de la diffusion, de la transmission ou de la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous c), de la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision–cadre 2004/68/JAI du Conseil (JO 2011, L 335, p. 1, et rectificatif JO 2012, L 18, p. 7), l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 73).

Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, au sens de la jurisprudence citée au point 70 du présent arrêt, avec les objectifs poursuivis et que les internautes disposent, conformément à ce qui a été constaté au point 54 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 155).

Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 156).

Ainsi, contrairement à ce que la juridiction de renvoi a souligné, il n'existe pas de tension entre les points 155 et 168 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791). En effet, ainsi que l'a relevé en substance M. l'avocat général aux points 81 et 82 de ses conclusions, il ressort clairement de ce point 155, lu en combinaison avec le point 156 et le point 168 de cet arrêt, que 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 la conservation généralisée des adresses IP attribuées

à la source d'une connexion, indépendamment du point de savoir si les personnes concernées sont susceptibles de présenter un lien, à tout le moins indirect, avec les objectifs poursuivis.

En troisième lieu, en ce qui concerne les mesures législatives prévoyant une conservation ciblée et une conservation rapide des données relatives au trafic et des données de localisation, certaines considérations exposées par des États membres à l'encontre de telles mesures font apparaître une compréhension plus étroite de la portée de ces mesures que celle retenue par la jurisprudence mentionnée au point 75 du présent arrêt. En effet, si, conformément à ce qui a été rappelé au point 57 du présent arrêt, ces mesures de conservation doivent présenter un caractère dérogatoire dans le système mis en place par la directive 2002/58, celle-ci, lue à la lumière des droits fondamentaux consacrés aux articles 7, 8 et 11 ainsi qu'à l'article 52, paragraphe 1, de la Charte, ne subordonne pas la possibilité d'émettre une injonction imposant une conservation ciblée à la condition que soient connus, à l'avance, les lieux susceptibles d'être la scène d'un acte de criminalité grave ou les personnes suspectées d'être impliquées dans un tel acte. De même, ladite directive n'exige pas que l'injonction imposant une conservation rapide soit limitée à des suspects identifiés préalablement à une telle injonction (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 75).

S'agissant, premièrement, de la conservation ciblée, la Cour a jugé que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une législation nationale fondée sur des éléments objectifs, permettant de viser, d'une part, les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 76 ainsi que jurisprudence citée).

La Cour a précisé, à cet égard, que, si ces éléments objectifs peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs et non discriminatoires, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 77).

Les États membres ont ainsi notamment la faculté de prendre des mesures de conservation visant des personnes faisant, au titre d'une telle identification, l'objet d'une enquête ou d'autres mesures de surveillance actuelles ou d'une inscription dans le casier judiciaire national mentionnant une condamnation antérieure pour des actes de criminalité grave pouvant impliquer un risque élevé de récidive. Or, lorsqu'une telle identification est fondée sur des éléments objectifs et non discriminatoires, définis par le droit national, la conservation ciblée visant des personnes ainsi identifiées est justifiée (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 78).

D'autre part, une mesure de conservation ciblée des données relatives au trafic et des données de localisation peut, selon le choix du législateur national et dans le respect strict du principe de proportionnalité, également être fondée sur un critère géographique, lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave. Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou encore des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 79 ainsi que jurisprudence citée).

Il convient de souligner que, selon cette jurisprudence, les autorités nationales compétentes peuvent prendre, pour les zones visées au point précédent, une mesure de conservation ciblée fondée sur un critère géographique, tel que notamment le taux moyen de criminalité dans une zone géographique, sans qu'elles disposent nécessairement d'indices concrets portant sur la préparation ou la commission, dans les zones concernées, d'actes de criminalité grave. Dans la mesure où une conservation ciblée fondée sur un tel critère est susceptible de toucher, en fonction des infractions pénales graves visées et de la situation propre aux États membres respectifs, à la fois des lieux caractérisés par un nombre élevé d'actes de criminalité grave et des lieux particulièrement exposés à la commission de tels actes, elle n'est, en principe, pas davantage de nature à donner lieu à des discriminations, le critère tiré du taux moyen de criminalité grave ne présentant, en soi, aucun lien avec des éléments potentiellement discriminatoires (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 80).

En outre et surtout, une mesure de conservation ciblée visant des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages, permet aux autorités compétentes de recueillir des données relatives au trafic et, notamment, des données de localisation de toutes les personnes utilisant, à un moment donné, un moyen de communication électronique dans l'un de ces lieux. Ainsi, une telle mesure de conservation ciblée est susceptible de permettre auxdites autorités d'obtenir, par l'accès aux données ainsi conservées, des informations sur la présence de ces personnes dans les lieux ou les zones géographiques visés par cette mesure ainsi que sur leurs déplacements entre ou à l'intérieur de ceux-ci et d'en tirer, aux fins de la lutte contre la criminalité grave, des conclusions sur leur présence et leur activité dans ces lieux ou ces zones géographiques à un moment donné au cours de la période de conservation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 81).

Il convient encore de relever que les zones géographiques visées par une telle conservation ciblée peuvent et, le cas échéant, doivent être modifiées en fonction de l'évolution des conditions ayant justifié leur sélection, permettant ainsi notamment de réagir aux évolutions de la lutte contre la criminalité grave. En effet, la Cour a déjà

jugé que la durée des mesures de conservation ciblée, décrites aux points 105 à 110 du présent arrêt, ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation (arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 151, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 82).

S'agissant de la possibilité de prévoir des critères distinctifs autres qu'un critère personnel ou géographique pour mettre en œuvre une conservation ciblée des données relatives au trafic et des données de localisation, il ne saurait être exclu que d'autres critères, objectifs et non discriminatoires, puissent entrer en ligne de compte afin d'assurer que la portée d'une conservation ciblée soit limitée au strict nécessaire et d'établir un lien, au moins indirect, entre les actes de criminalité grave et les personnes dont les données sont conservées. Cela étant, l'article 15, paragraphe 1, de la directive 2002/58 visant des mesures législatives des États membres, c'est à ces derniers et non à la Cour qu'il incombe d'identifier de tels critères, étant entendu qu'il ne saurait être question de réinstaurer, par ce moyen, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 83).

En tout état de cause, ainsi que M. l'avocat général l'a relevé au point 50 de ses conclusions, l'existence éventuelle de difficultés pour définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne saurait justifier que des États membres, en faisant de l'exception une règle, prévoient une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 84).

S'agissant, deuxièmement, de la conservation rapide des données relatives au trafic et des données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur le fondement des articles 5, 6 et 9 de la directive 2002/58 ou sur celui des mesures législatives prises en vertu de l'article 15, paragraphe 1, de cette directive, il convient de rappeler que de telles données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant ladite directive, leur traitement et leur stockage. Néanmoins, la Cour a jugé que, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 85).

Dans une telle situation, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts légitimes en cause visée aux points 65 à 68 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent (arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 163, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 86).

Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seules la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence, à la condition que cette mesure ainsi que l'accès aux données ainsi conservées respectent les limites du strict nécessaire, telles qu'énoncées aux points 164 à 167 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 87).

La Cour a précisé qu'une mesure de conservation de cette nature ne doit pas être limitée aux données des personnes identifiées préalablement comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné ou des personnes concrètement soupçonnées d'avoir commis un acte de criminalité grave ou une atteinte à la sécurité nationale. En effet, selon la Cour, tout en respectant le cadre dressé par l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, et compte tenu des considérations figurant au point 70 du présent arrêt, une telle mesure peut, selon le choix du législateur national et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel (arrêts du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 165, ainsi que du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 88).

Ainsi, une mesure législative peut autoriser le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation rapide des données relatives au trafic et des données de localisation, notamment, des personnes avec lesquelles, antérieurement à la survenance d'une menace grave pour la sécurité publique ou à la commission d'un acte de criminalité grave, une victime a été en contact en

utilisant ses moyens de communications électroniques (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 89).

Une telle conservation rapide peut, selon la jurisprudence de la Cour rappelée au point 117 du présent arrêt et dans les mêmes conditions que celles visées à ce point, également être étendue à des zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. Il convient de préciser que peuvent encore faire l'objet d'une telle mesure les données relatives au trafic et les données de localisation afférentes au lieu où une personne, potentiellement victime d'un acte de criminalité grave, a disparu, à la condition que cette mesure ainsi que l'accès aux données ainsi conservées respectent les limites du strict nécessaire aux fins de la lutte contre la criminalité grave ou de la sauvegarde de la sécurité nationale, telles qu'énoncées aux points 164 à 167 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 90).

Par ailleurs, il importe de préciser que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à ce que les autorités nationales compétentes ordonnent une mesure de conservation rapide dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique ou sur un éventuel acte de criminalité grave, à savoir à partir du moment auquel ces autorités peuvent, selon les dispositions pertinentes du droit national, ouvrir une telle enquête (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 91).

S'agissant encore de la variété des mesures de conservation des données relatives au trafic et des données de localisation visées au point 75 du présent arrêt, il importe de préciser que ces différentes mesures peuvent, selon le choix du législateur national et tout en respectant les limites du strict nécessaire, trouver à s'appliquer conjointement. Dans ces conditions, 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, tel qu'interprété par la jurisprudence issue de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), ne s'oppose pas à une combinaison de ces mesures (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 92).

En quatrième et dernier lieu, il importe de souligner que la proportionnalité des mesures adoptées en vertu de l'article 15, paragraphe 1, de la directive 2002/58 requiert, selon la jurisprudence constante de la Cour telle que récapitulée dans l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), le respect non seulement des exigences d'aptitude et de nécessité, mais également de celle ayant trait au caractère proportionné de ces mesures par rapport à l'objectif poursuivi (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 93).

Dans ce contexte, il y a lieu de rappeler que, au point 51 de son arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238), la Cour a jugé que, si la lutte contre la criminalité grave est d'une importance primordiale pour garantir la sécurité publique et si son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, telle que celle instaurée par la directive 2006/24, soit considérée comme nécessaire (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 94).

Dans le même ordre d'idées, la Cour a précisé, au point 145 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), que même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé au point 64 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une législation nationale prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 95).

Par ailleurs, les arrêts de la Cour EDH du 25 mai 2021, Big Brother Watch e.a. c. Royaume-Uni (CE:ECHR:2021:0525JUD 005817013), et du 25 mai 2021, Centrum för Rättvisa c. Suède (CE:ECHR:2021:0525JUD 003525208), invoqués par certains gouvernements lors de l'audience pour soutenir que la CEDH ne s'oppose pas à des réglementations nationales prévoyant, en substance, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, ne sauraient remettre en cause l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 découlant des développements qui précèdent. En effet, étaient en cause dans ces arrêts des interceptions de masse de données afférentes à des communications internationales. Ainsi, et comme la Commission l'a relevé lors de l'audience, la Cour européenne des droits de l'homme ne s'est pas prononcée, dans lesdits arrêts, sur la conformité avec la CEDH d'une conservation généralisée et indifférenciée de données relatives au trafic et de données de localisation sur le territoire national ni même d'une interception de grande ampleur de ces données aux fins de la prévention, de la détection et de la recherche d'infractions pénales graves. En tout état de cause, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne, de telle sorte que c'est seulement en tant que seuil de protection minimale qu'il y a lieu de tenir compte des droits correspondants de la CEDH en vue d'interpréter la Charte (arrêt du 17 décembre 2020, Centraal Israëlitisch Consistorie van België e.a., C-336/19, EU:C:2020:1031, point 56).

Sur l'accès aux données ayant été conservées de manière généralisée et indifférenciée

Lors de l'audience, le gouvernement danois a soutenu que les autorités nationales compétentes devraient pouvoir accéder, aux fins de la lutte contre la criminalité grave, aux données relatives au trafic et aux données de

localisation qui ont été conservées de manière généralisée et indifférenciée, conformément à la jurisprudence issue de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 135 à 139), pour faire face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible.

Il convient de relever d'emblée que le fait d'autoriser l'accès, aux fins de la lutte contre la criminalité grave, à des données relatives au trafic et à des données de localisation qui ont été conservées de manière généralisée et indifférenciée ferait dépendre cet accès de circonstances étrangères à cet objectif, en fonction de l'existence ou non, dans l'État membre concerné, d'une menace grave pour la sécurité nationale telle que visée au point précédent, alors que, au regard du seul objectif de lutte contre la criminalité grave devant justifier la conservation de ces données et l'accès à celles-ci, rien ne justifierait une différence de traitement, en particulier entre les États membres (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 97).

Ainsi que la Cour l'a déjà jugé, l'accès à des données relatives au trafic et à des données de localisation conservées par des fournisseurs de services de communications électroniques en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, qui doit s'effectuer dans le plein respect des conditions résultant de la jurisprudence ayant interprété cette directive, ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 98).

Or, l'argumentation du gouvernement danois vise une situation dans laquelle l'objectif de la demande d'accès envisagée, à savoir la lutte contre la criminalité grave, est d'une importance moindre, dans la hiérarchie des objectifs d'intérêt général, que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale. Autoriser, dans une telle situation, un accès aux données conservées irait à l'encontre de cette hiérarchie des objectifs d'intérêt général rappelée au point précédent ainsi qu'aux points 68, 71, 72 et 73 du présent arrêt (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 99).

En outre et surtout, conformément à la jurisprudence rappelée au point 74 du présent arrêt, les données relatives au trafic et les données de localisation ne peuvent pas faire l'objet d'une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave et, partant, un accès à ces données ne saurait être justifié à ces mêmes fins. Or, lorsque ces données ont exceptionnellement été conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale contre une menace qui s'avère réelle et actuelle ou prévisible, dans les conditions visées au point 71 du présent arrêt, les autorités nationales compétentes en matière d'enquêtes pénales ne sauraient accéder auxdites données dans le cadre de poursuites pénales, sous peine de priver de tout effet utile l'interdiction de procéder à une telle conservation aux fins de la lutte contre la criminalité grave, rappelée audit point 74 (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 100).

Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la question préjudicielle que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à des mesures législatives nationales prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, 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, doit être interprété en ce sens qu'il ne s'oppose pas à des mesures législatives nationales :

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.

Sur les dépens

La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne,

doit être interprété en ce sens que :

il s'oppose à des mesures législatives nationales prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation ;

il ne s'oppose pas à des mesures législatives nationales :

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.

Signatures

---

* Langue de procédure : l'allemand.