ARRÊT DE LA COUR (grande chambre)

5 avril 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 – Accès aux données conservées – Contrôle juridictionnel a posteriori – Directive 2002/58/CE – Article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 11 ainsi que article 52, paragraphe 1 – Possibilité, pour une juridiction nationale, de limiter les effets dans le temps d'une déclaration d'invalidité concernant une législation nationale incompatible avec le droit de l'Union – Exclusion »

Dans l'affaire C-140/20,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par la Supreme Court (Cour suprême, Irlande), par décision du 25 mars 2020, parvenue à la Cour à la même date, dans la procédure

G.D.

contre

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. A. Arabadjiev, M^me^ A. Prechal, MM. S. Rodin, I. Jarukaitis et N. Jääskinen, présidents de chambre, MM. T. von Danwitz (rapporteur), M. Safjan, F. Biltgen, P. G. Xuereb, 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 G.D., par M. J. Dunphy, solicitor, MM. R. Kennedy et R. Farrell, SC, ainsi que par M^me^ K. McCormack, BL,

– pour le Commissioner of An Garda Síochána, le Minister for Communications, Energy and Natural Resources et l'Attorney General, par M^mes^ M. Browne, S. Purcell, C. Stone et J. Quaney ainsi que par M. A. Joyce, en qualité d'agents, assistés de MM. S. Guerin et P. Gallagher, SC, ainsi que de M. D. Fennelly et de M^me^ L. Dwyer, BL,

– pour le gouvernement belge, par MM. P. Cottin et J.-C. Halleux, en qualité d'agents, assistés de M^e^ J. Vanpraet, advocaat,

– pour le gouvernement tchèque, par MM. M. Smolek, O. Serdula et J. Vláčil, en qualité d'agents,

– pour le gouvernement danois, initialement par MM. J. Nymann-Lindegren et M. Jespersen ainsi que par M^me^ M. Wolff, puis par M^mes^ M. Wolff et V. Jørgensen, en qualité d'agents,

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

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

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

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

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

– pour le gouvernement polonais, par M. B. Majczyna et M^me^ J. Sawicka, en qualité d'agents,

– pour le gouvernement portugais, par M. L. Inez Fernandes ainsi que par M^mes^ P. Barros da Costa et I. Oliveira, en qualité d'agents,

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

– pour le gouvernement suédois, par MM. O. Simonsson et J. Lundberg ainsi que par M^mes^ H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson et H. Eklinder, en qualité d'agents,

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

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

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

rend le présent

Arrêt

1 La demande de décision préjudicielle porte 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 7, 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 »).

2 Cette demande a été présentée dans le cadre d'un litige opposant G.D. au Commissioner of An Garda Síochána (chef de la police nationale, Irlande), au Minister for Communications, Energy and Natural Ressources (ministre des communications, de l'énergie et des ressources naturelles, Irlande) et à l'Attorney General au sujet de la validité du Communications (Retention of Data) Act 2011 [loi

de 2011 sur les communications (conservation des données), ci-après la « loi de 2011 »].

Le cadre juridique

Le droit de l'Union

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

« (2) 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].

[...]

(6) 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.

(7) 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.

[...]

(11) À l'instar de la directive [95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31)], 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 [de l'Union]. 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. »

4 L'article 1er de la directive 2002/58, 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 [l'Union

européenne].

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 sur l'Union européenne, 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. »

5 Aux termes de l'article 2 de la directive 2002/58, 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 :

a) "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 ;

b) "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 ;

c) "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 ;

d) "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 ;

[...] »

6 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 [l'Union], y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification. »

7 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. »

8 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.

[...] »

9 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. [...] »

10 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 [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

Le droit irlandais

11 Ainsi qu'il ressort de la demande de décision préjudicielle, la loi de 2011 a été adoptée afin de transposer dans l'ordre juridique irlandais 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).

12 L'article 1er de la loi de 2011 définit le terme « données » comme visant « les données relatives au trafic ou les données de localisation ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur », et le terme « infraction grave » comme visant une infraction passible d'une peine d'emprisonnement d'une durée égale ou supérieure à cinq ans ou l'une des autres infractions énumérées à l'annexe 1 de cette loi.

13 L'article 3, paragraphe 1, de ladite loi impose à tous les fournisseurs de services de communications électroniques de conserver les données visées à son annexe 2, partie 1, pendant une durée de deux ans ainsi que les données visées à son annexe 2, partie 2, pendant une durée d'un an.

14 L'annexe 2, partie 1, de la même loi vise, entre autres, les données relatives à la téléphonie fixe et à la téléphonie mobile permettant d'identifier la source et la destination d'une communication, de déterminer la date et l'heure du début et de la fin d'une communication, de déterminer le type de communication concerné ainsi que d'identifier le type et la localisation géographique du matériel de communication utilisé. En particulier, le point 6 de cette annexe 2, partie 1, prévoit la conservation des données nécessaires pour localiser un moyen de communication électronique mobile, ces données étant, d'une part, l'identifiant cellulaire et, d'autre part, des données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

15 L'annexe 2, partie 2, de la loi de 2011 vise les données relatives à l'accès à Internet, le courrier électronique et la téléphonie par Internet et couvre notamment les numéros d'identifiant et de téléphone, les adresses IP, ainsi que la date et l'heure du début et de la fin d'une communication. Le contenu des communications ne relève pas de ce type de données.

16 En vertu des articles 4 et 5 de la loi de 2011, les fournisseurs de services de communications

électroniques doivent prendre certaines mesures pour veiller à ce que les données soient protégées contre les accès non autorisés.

17 L'article 6 de cette loi, qui prévoit les conditions dans lesquelles une demande d'accès peut être introduite, dispose, à son paragraphe 1 :

« Un fonctionnaire de la police nationale dont le rang n'est pas inférieur à celui de commissaire divisionnaire peut demander à un fournisseur de services de lui communiquer les données conservées par ce fournisseur de services conformément à l'article 3 si ce fonctionnaire estime que les données en question sont nécessaires à des fins :

(a) de prévention, de détection, de recherche ou de poursuite d'une infraction grave,

(b) de sauvegarde de la sûreté de l'État,

(c) de préservation de la vie humaine. »

18 L'article 7 de ladite loi impose aux fournisseurs de services de communications électroniques de faire droit aux demandes visées à l'article 6 de celle-ci.

19 Au titre des mécanismes de contrôle de la décision du fonctionnaire de la police nationale mentionné à l'article 6 de la loi de 2011 figurent la procédure de réclamation prévue à l'article 10 de cette loi ainsi que la procédure devant le *designated judge* (juge désigné), au sens de l'article 12 de celle-ci, lequel est chargé d'examiner l'application des dispositions de ladite loi.

Le litige au principal et les questions préjudicielles

20 Au mois de mars 2015, G.D. a été condamné à une peine de réclusion à perpétuité pour le meurtre d'une personne qui avait disparu au mois d'août 2012 et dont la dépouille n'avait été découverte qu'au mois de septembre 2013. Dans l'appel de sa condamnation, l'intéressé a notamment reproché à la juridiction de première instance d'avoir, à tort, admis comme éléments de preuve des données relatives au trafic et des données de localisation afférentes à des appels téléphoniques, au motif que la loi de 2011, qui régissait la conservation de ces données et sur la base de laquelle les enquêteurs de la police nationale avaient eu accès auxdites données, violait les droits que lui confère le droit de l'Union. Cet appel est actuellement pendant.

21 Afin de pouvoir contester, dans le cadre de la procédure pénale, la recevabilité desdites preuves, G.D. a engagé auprès de la High Court (Haute Cour, Irlande) une procédure civile visant à constater l'invalidité de certaines dispositions de la loi de 2011. Par décision du 6 décembre 2018, cette juridiction a fait droit à l'argumentation de G.D. et considéré que l'article 6, paragraphe 1, sous a), de cette loi était incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte. L'Irlande a interjeté appel de cette décision devant la Supreme Court (Cour suprême, Irlande), la juridiction de renvoi.

22 La procédure pénale pendante devant la Court of Appeal (Cour d'appel, Irlande) a été suspendue jusqu'au prononcé de la décision de la juridiction de renvoi dans le cadre de la procédure civile au principal.

23 Devant la juridiction de renvoi, l'Irlande a soutenu que, aux fins de déterminer si l'ingérence dans le droit au respect de la vie privée consacré à l'article 7 de la Charte résultant de la conservation des données relatives au trafic et des données de localisation au titre de la loi de 2011 est proportionnée, il convient d'examiner les objectifs du régime mis en place par cette loi dans son ensemble. En outre, selon cet État membre, ladite loi a établi un cadre détaillé régissant l'accès aux données conservées, en vertu duquel l'unité chargée, au sein de la police nationale, de l'examen préalable des demandes d'accès jouit d'une indépendance fonctionnelle par rapport à la police nationale dans

l'exercice de sa mission et, par suite, satisfait à l'exigence d'un contrôle préalable effectué par une entité administrative indépendante. Ce système de contrôle serait complété par une procédure de réclamation et un contrôle juridictionnel. Enfin, ledit État membre fait valoir que s'il est considéré, en définitive, que la loi de 2011 est contraire au droit de l'Union, toute constatation qui en sera déduite par la juridiction de renvoi devrait uniquement valoir, du point de vue de ses effets dans le temps, pour l'avenir.

24 De son côté, G.D. a fait valoir que le régime de conservation généralisée et indifférenciée des données institué par la loi de 2011 ainsi que le régime d'accès à ces données prévu par cette loi sont incompatibles avec le droit de l'Union, tel qu'interprété en particulier par la Cour au point 120 de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970).

25 La juridiction de renvoi précise, à titre liminaire, qu'il lui appartient seulement d'apprécier si la High Court (Haute Cour) a jugé à bon droit que l'article 6, paragraphe 1, sous a), de la loi de 2011 est incompatible avec le droit de l'Union et que, en revanche, la question de la recevabilité des preuves soulevées dans le cadre du procès pénal relève de la seule compétence de la Court of Appeal (Cour d'appel), saisie de l'appel interjeté contre la décision de condamnation.

26 Dans ce contexte, la juridiction de renvoi s'interroge, tout d'abord, sur les exigences du droit de l'Union en ce qui concerne la conservation des données à des fins de lutte contre la criminalité grave. À cet égard, elle estime, en substance, que seule une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation permet de lutter, de manière effective, contre la criminalité grave, ce qu'une conservation ciblée et une conservation rapide *(quick freeze)* ne permettraient pas de faire. S'agissant de la conservation ciblée, la juridiction de renvoi s'interroge sur la possibilité de viser des groupes ou des zones géographiques déterminés aux fins de la lutte contre la criminalité grave, dans la mesure où certaines infractions graves impliqueraient rarement des circonstances connues des autorités nationales compétentes et leur permettant de soupçonner la commission d'une infraction préalablement à celle-ci. En outre, une conservation ciblée pourrait donner lieu à des discriminations. Quant à la conservation rapide, la juridiction de renvoi estime que celle-ci n'est utile que dans des situations où il existe un suspect identifiable à un stade précoce de l'enquête.

27 S'agissant, ensuite, de l'accès aux données conservées par les fournisseurs de services de communications électroniques, la juridiction de renvoi souligne que la police nationale a instauré, en son sein, un mécanisme d'autocertification des demandes d'accès adressées à ces fournisseurs. Ainsi, il ressortirait des éléments produits devant la High Court (Haute Cour) que le chef de la police nationale a décidé, à titre de mesure interne, que les demandes d'accès introduites en vertu de la loi de 2011 doivent faire l'objet d'un traitement centralisé par un seul agent de la police nationale, ayant la qualité de commissaire divisionnaire, soit le chef de la section de la sécurité et du renseignement. Si ce dernier considère que les données concernées sont nécessaires aux fins, notamment, de la prévention, de la détection, de la recherche ou de la poursuite d'une infraction grave, il peut adresser une demande d'accès aux fournisseurs de services de communications électroniques. Par ailleurs, le chef de la police nationale aurait institué, au sein de celle-ci, une unité autonome dénommée *Telecommunications Liaison Unit* (Unité de liaison en matière de télécommunications, ci-après la « TLU »), afin de fournir un appui au chef de la section de la sécurité et du renseignement dans l'exercice de ses fonctions et de servir de point de contact unique avec ces mêmes fournisseurs de services.

28 La juridiction de renvoi ajoute que, pendant la période concernée par l'enquête pénale ouverte contre G.D., toutes les demandes d'accès devaient être approuvées en premier lieu par un commissaire ou un inspecteur faisant fonction de commissaire, avant d'être envoyées à la TLU en vue de leur traitement, et que les enquêteurs étaient invités à assortir leurs demandes d'accès de détails suffisants pour qu'une décision éclairée puisse être prise. En outre, la TLU et le chef de la section de la sécurité et du renseignement étaient tenus d'examiner la légalité, la nécessité et la proportionnalité des demandes d'accès, en tenant compte du fait que ce chef pouvait être appelé à

répondre de sa décision devant un juge désigné par la High Court (Haute Cour). Par ailleurs, la TLU serait subordonnée au contrôle du Data Protection Commissioner (commissaire à la protection des données, Irlande).

29 Enfin, la juridiction de renvoi s'interroge sur la portée et les effets dans le temps d'une éventuelle constatation de non-conformité de la loi de 2011 avec le droit de l'Union. À cet égard, elle précise qu'une telle constatation ne pourrait valoir que pour l'avenir, au motif que les données utilisées comme preuves dans la procédure pénale contre G.D. ont fait l'objet d'une conservation et d'un accès à la fin de l'année 2013, à savoir à une période où l'Irlande était tenue d'appliquer les dispositions de la loi de 2011 transposant la directive 2006/24. Selon l'Irlande, une telle solution serait également appropriée dans la mesure où, à défaut, la recherche et la poursuite des infractions graves en Irlande, ainsi que la situation de personnes déjà jugées et condamnées, pourraient se trouver sérieusement affectées.

30 C'est dans ces circonstances que la Supreme Court (Cour suprême) a décidé de surseoir à statuer et de soumettre à la Cour les questions préjudicielles suivantes :

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

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

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

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

5) Si une juridiction nationale est tenue de conclure qu'une mesure nationale est contraire aux dispositions de l'article 15 de la directive 2002/58, interprétées à la lumière de la Charte, est-elle fondée à limiter les effets dans le temps d'une telle constatation si elle estime que ne pas limiter ses effets entraînerait « le chaos et un préjudice grave pour l'intérêt général » [conformément à l'approche adoptée, par exemple, dans le jugement R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs [2018] EWHC 975, point 46] ?

6) Une juridiction nationale invitée à constater l'incompatibilité de la législation nationale avec l'article 15 de la directive 2002/58 ou à écarter l'application de cette législation ou bien à déclarer que l'application d'une telle législation a violé les droits d'une personne physique,

que ce soit dans le cadre d'une procédure engagée afin de faciliter la présentation d'un argument relatif à l'admissibilité des preuves dans une procédure pénale ou dans un autre cadre, peut-elle être autorisée à refuser de faire droit à cette demande en ce qui concerne les données conservées en application de la disposition nationale adoptée en vertu de l'obligation, prévue à l'article 288 TFUE, de transposer fidèlement en droit national les dispositions d'une directive ou à limiter une telle constatation à la période postérieure à la déclaration de l'invalidité de la directive 2006/24 par [l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238)] ? »

Sur les questions préjudicielles

Sur les première, deuxième et quatrième questions

31 Par ses première, deuxième et quatrième questions, qu'il convient d'examiner ensemble, 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 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 législation nationale prévoyant une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation à des fins de lutte contre la criminalité grave.

32 Il convient de rappeler, à titre liminaire, qu'il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (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 105 ainsi que jurisprudence citée).

33 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.

34 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.

35 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 (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 107).

36 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 (voir, en ce sens, arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 83, ainsi que 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 106).

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

38 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.

39 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.

40 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 35 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 (voir, en ce sens, arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 89, ainsi que 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 111).

41 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 112 ainsi que jurisprudence citée).

42 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, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (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 113 ainsi que jurisprudence citée).

43 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (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 114 ainsi que jurisprudence citée).

44 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 (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, points 115 et 116 ainsi que jurisprudence citée).

45 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 117 ainsi que jurisprudence citée).

46 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 (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, points 118 et 119 ainsi que jurisprudence citée).

47 à cet égard, il y a lieu de souligner que la conservation de ces données et l'accès à celles-ci constituent, ainsi qu'il ressort de la jurisprudence rappelée au point 44 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.

48 Cela étant, en ce qu'il permet aux États membres de limiter les droits et les obligations visés aux points 34 à 37 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 120 à 122 ainsi que jurisprudence citée).

49 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 126 ainsi que jurisprudence citée).

50 Face à ces différentes obligations positives, il convient donc de procéder à une conciliation des différents intérêts légitimes et droits en cause. En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différents intérêts

légitimes et droits à protéger (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 127 et 128 ainsi que jurisprudence citée).

51 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 35 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 (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 129).

52 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 130 ainsi que jurisprudence citée).

53 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 131 ainsi que jurisprudence citée).

54 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 132 ainsi que jurisprudence citée).

55 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. En particulier, s'agissant de la lutte contre la criminalité grave, les données dont la conservation est prévue doivent être de nature à contribuer à la prévention, à la détection ou à la poursuite d'infractions graves (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 59, ainsi que 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 133).

56 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.

57 À cet égard, la Cour a jugé que l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, selon lequel la sauvegarde de la sécurité nationale reste de la seule responsabilité de chaque État membre, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs (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, points 135 et 136).

58 C'est pour ce motif que la Cour a constaté 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 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 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).

59 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 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 140 ainsi que jurisprudence citée).

60 Au cours de l'audience, la Commission européenne a soutenu que la criminalité particulièrement grave pourrait être assimilée à une menace pour la sécurité nationale.

61 Or, 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 notamment des activités de terrorisme (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 135).

62 Il convient, en outre, de relever que, 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 (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, points 136 et 137).

63 Ainsi, la criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale. En effet, comme M. l'avocat général l'a relevé aux points 49 et 50 de ses conclusions, 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.

64 Il s'ensuit également que la circonstance, mentionnée dans la deuxième question préjudicielle, que les données relatives au trafic et les données de localisation ont légalement fait l'objet d'une conservation aux fins de la sauvegarde de la sécurité nationale est sans incidence sur la licéité de leur conservation aux fins de la lutte contre la criminalité grave.

65 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, compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 46 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 (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, points 141 et 142 ainsi que jurisprudence citée).

66 En outre, la Cour a souligné qu'une législation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi. Une telle législation concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. En particulier, comme l'a déjà jugé la Cour, une telle législation n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave (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 143 et 144 ainsi que jurisprudence citée).

67 En revanche, au point 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), 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.

68 Dans la présente demande de décision préjudicielle, laquelle est parvenue à la Cour avant le prononcé des 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), et du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), la juridiction de renvoi a toutefois estimé que seule une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation permettrait de lutter, de manière effective, contre la criminalité grave. Lors de l'audience du 13 septembre 2021, il a été soutenu, notamment par l'Irlande et le gouvernement français, qu'une telle conclusion n'était pas infirmée par le fait que les États membres peuvent avoir recours aux mesures visées au point précédent.

69 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.

70 En deuxième lieu, il y a lieu de souligner 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, tel qu'interprété par la jurisprudence rappelée au point 67 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.

71 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.

72 Or, ainsi qu'il ressort de la jurisprudence résumée au point 67 du présent arrêt, 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.

73 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 50 à 53 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), 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 (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, points 153 et 154).

74 Partant, la Cour a jugé qu'une telle 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 de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données visées aux points 155 et 156 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).

75 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, les indications figurant dans la demande de décision préjudicielle font apparaître une compréhension plus étroite de la portée de ces mesures que celle retenue par la jurisprudence rappelée au point 67 du présent arrêt. En effet, si, conformément à ce qui a été rappelé au point 40 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 ni 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.

76 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 (arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 111, ainsi que 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 148).

77 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 (voir, en ce sens, arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 110, ainsi que 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 149).

78 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.

79 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 (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 150 ainsi que jurisprudence citée).

80 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.

81 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.

82 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 76 à 81 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 (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 151).

83 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 biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

84 En tout état de cause, ainsi que l'avocat général Campos Sánchez-Bordona l'a relevé au point 50 de ses conclusions dans les affaires jointes SpaceNet et Telekom Deutschland (C-793/19 et C-794/19, EU:C:2021:939), 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.

85 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 la base des articles 5, 6 et 9 de la directive 2002/58 ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de 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 (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, points 160 et 161).

86 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 50 à 53 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 (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 163).

87 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).

88 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 55 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 (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 165).

89 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.

90 Une telle conservation rapide peut, selon la jurisprudence de la Cour rappelée au point 88 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).

91 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.

92 S'agissant de la variété des mesures de conservation des données relatives au trafic et des données de localisation visées au point 67 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.

93 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.

94 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.

95 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 49 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.

96 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.

97 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.

98 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 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 la directive 2002/58, ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation (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, points 165 et 166).

99 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 53, 56, 57 et 59 du présent arrêt.

100 En outre et surtout, conformément à la jurisprudence rappelée au point 65 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 58 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 65.

101 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux première, deuxième et quatrième questions que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, 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, 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 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 la troisième question

102 Par sa troisième question, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8, 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombe à un fonctionnaire de police, assisté par une unité instituée au sein de la police jouissant d'un certain degré d'autonomie dans l'exercice de sa mission et dont les décisions peuvent faire ultérieurement l'objet d'un contrôle juridictionnel.

103 À titre liminaire, il convient de rappeler que, s'il appartient au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données dont ils disposent, une législation nationale doit, pour satisfaire à l'exigence de proportionnalité, telle que rappelée au point 54 du présent arrêt, prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de 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 [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 48 et jurisprudence citée].

104 En particulier, une législation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées, adoptée au titre de l'article 15, paragraphe 1, de la directive 2002/58, ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette législation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 49 et jurisprudence citée].

105 Ainsi, dès lors qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, la législation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause. À cet égard, un tel accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes peut également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 50 et jurisprudence citée].

106 Aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 51 et jurisprudence citée].

107 Ce contrôle préalable requiert notamment que la juridiction ou l'entité administrative indépendante chargée de l'effectuer dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts légitimes et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 52].

108 Lorsque ce contrôle est effectué non par une juridiction, mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure. Ainsi, l'exigence d'indépendance à laquelle doit satisfaire l'entité chargée d'exercer le contrôle préalable impose que celle-ci ait la qualité de tiers par rapport à l'autorité qui demande l'accès aux données, de sorte que ladite entité soit en mesure d'exercer ce contrôle de manière objective et impartiale, en étant protégée de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que l'autorité chargée de ce contrôle préalable, d'une part, ne

soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité à l'égard des parties à la procédure pénale [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, points 53 et 54].

109 Ainsi, la Cour a notamment considéré qu'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique ne peut se voir reconnaître la qualité de tiers par rapport aux intérêts légitimes en cause, dès lors qu'il a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale. Par conséquent, un tel ministère public n'est pas en mesure d'effectuer le contrôle préalable des demandes d'accès aux données conservées [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, points 55 et 57].

110 Enfin, le contrôle indépendant requis conformément à l'article 15, paragraphe 1, de la directive 2002/58 doit intervenir préalablement à tout accès aux données concernées, sauf en cas d'urgence dûment justifiée, auquel cas ledit contrôle doit intervenir dans de brefs délais. En effet, un contrôle ultérieur ne permettrait pas de répondre à l'objectif du contrôle préalable, qui consiste à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire [voir, en ce sens, 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 189, ainsi que du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 58].

111 En l'occurrence, il ressort, tout d'abord, de la demande de décision préjudicielle que la loi de 2011 attribue à un fonctionnaire de police, dont le rang n'est pas inférieur à celui de commissaire divisionnaire, la compétence pour exercer le contrôle préalable des demandes d'accès aux données émanant des services d'enquête de police et pour solliciter des fournisseurs de services de communications électroniques qu'ils lui communiquent les données qu'ils conservent. Dans la mesure où ce fonctionnaire ne revêt pas la qualité de tiers par rapport à ces services, il ne remplit pas les exigences d'indépendance et d'impartialité rappelées au point 108 du présent arrêt, nonobstant la circonstance qu'il est assisté dans cette mission par une unité de la police, en l'occurrence la TLU, bénéficiant d'un certain degré d'autonomie dans l'exercice de sa mission.

112 Ensuite, s'il est vrai que la loi de 2011 prévoit des mécanismes de contrôle a posteriori de la décision du fonctionnaire de police compétent sous la forme d'une procédure de réclamation et d'une procédure devant un juge chargé de vérifier l'application des dispositions de ladite loi, il ressort de la jurisprudence rappelée au point 110 du présent arrêt qu'un contrôle exercé a posteriori ne saurait se substituer à l'exigence, rappelée au point 106 du présent arrêt, de contrôle indépendant et, sauf cas d'urgence dûment justifiée, préalable.

113 Enfin, la loi de 2011 ne prévoit pas de critères objectifs définissant précisément les conditions et les circonstances dans lesquelles doit être accordé aux autorités nationales l'accès aux données, le fonctionnaire de police chargé du traitement des demandes d'accès aux données conservées étant seul compétent, ainsi que l'a confirmé l'Irlande au cours de l'audience, pour apprécier les soupçons pesant sur les personnes concernées et la nécessité d'un accès aux données relatives à ces dernières.

114 Par conséquent, il convient de répondre à la troisième question que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8, 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une législation nationale en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées par les fournisseurs de services de communications électroniques, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombe à un fonctionnaire de police, assisté par une unité instituée au sein de la police jouissant d'un certain degré d'autonomie dans l'exercice de sa mission et dont les décisions peuvent faire ultérieurement l'objet d'un contrôle juridictionnel.

Sur les cinquième et sixième questions

115 Par ses cinquième et sixième questions, qu'il convient d'examiner ensemble, la juridiction de renvoi cherche, en substance, à savoir si le droit de l'Union doit être interprété en ce sens qu'une juridiction nationale peut limiter dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de la Charte.

116 Il ressort des informations fournies par la juridiction de renvoi que la législation nationale en cause au principal, à savoir la loi de 2011, a été adoptée aux fins de transposer en droit national la directive 2006/24, qui a ensuite été déclarée invalide par la Cour dans son arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238).

117 En outre, la juridiction de renvoi relève que, si l'examen de la recevabilité des éléments de preuve fondés sur des données conservées en vertu de la loi de 2011 et invoqués à l'égard de G.D. dans le cadre de la procédure pénale incombe au juge pénal, c'est néanmoins à elle, dans le cadre de la procédure civile, qu'il appartient de statuer sur la validité des dispositions en cause de cette loi et sur les effets dans le temps d'un constat d'invalidité de celles-ci. Ainsi, si la seule question qui se pose devant la juridiction de renvoi est celle de la validité des dispositions de la loi de 2011, ladite juridiction estime toutefois nécessaire d'interroger la Cour quant à l'incidence d'un éventuel constat d'invalidité sur l'admissibilité des éléments de preuve obtenus au moyen de la conservation généralisée et indifférenciée des données que cette loi a permise.

118 À titre liminaire, il convient de rappeler que le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes dispositions du droit de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces dispositions sur le territoire desdits États. En vertu de ce principe, à défaut de pouvoir procéder à une interprétation de la législation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel [voir, en ce sens, arrêts du 15 juillet 1964, Costa, 6/64, EU:C:1964:66, p. 1159 et 1160 ; du 19 novembre 2019, A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême), C-585/18, C-624/18 et C-625/18, EU:C:2019:982, points 157, 158 et 160, ainsi que 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 214 et 215].

119 Seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée. Il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (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 216 et 217 ainsi que jurisprudence citée).

120 Certes, la Cour a considéré, dans une affaire concernant la légalité de mesures adoptées en méconnaissance de l'obligation, édictée par le droit de l'Union, d'effectuer une évaluation préalable des incidences d'un projet sur l'environnement et sur un site protégé, qu'une juridiction nationale peut, si le droit interne le permet, exceptionnellement maintenir les effets de telles mesures lorsque ce maintien est justifié par des considérations impérieuses liées à la nécessité d'écarter une menace réelle et grave de rupture de l'approvisionnement en électricité de l'État membre concerné, à

laquelle il ne pourrait être fait face par d'autres moyens et alternatives, notamment dans le cadre du marché intérieur, ledit maintien ne pouvant couvrir que le laps de temps strictement nécessaire pour remédier à cette illégalité (voir, en ce sens, arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, points 175, 176, 179 et 181).

121 Cependant, contrairement à l'omission d'une obligation procédurale, telle que l'évaluation préalable des incidences d'un projet, qui s'inscrit dans le domaine spécifique de la protection de l'environnement, une méconnaissance de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle mentionnée au point précédent (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 219).

122 En effet, le maintien des effets d'une législation nationale telle que la loi de 2011 signifierait que cette législation continue à imposer aux fournisseurs de services de communications électroniques des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées (voir, par analogie, 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 219).

123 Partant, la juridiction de renvoi ne saurait limiter dans le temps les effets d'une déclaration d'invalidité lui incombant, en vertu du droit national, quant à la législation nationale en cause au principal (voir, par analogie, 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 220).

124 À cet égard, ainsi que M. l'avocat général l'a relevé en substance au point 75 de ses conclusions, la circonstance que cette législation nationale a été adoptée aux fins de transposer la directive 2006/24 dans le droit national est dénuée de pertinence dès lors que, en raison de l'invalidation par la Cour de cette directive, invalidation dont les effets remontent à la date de son entrée en vigueur (voir, en ce sens, arrêt du 8 février 1996, FMC e.a., C-212/94, EU:C:1996:40, point 55), la validité de cette législation nationale doit être appréciée par la juridiction de renvoi à la lumière de la directive 2002/58 et de la Charte, telles qu'interprétées par la Cour.

125 S'agissant, plus particulièrement, de l'interprétation de la directive 2002/58 et de la Charte retenue par la Cour notamment dans ses arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), et du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), il convient de rappeler que, selon une jurisprudence constante, l'interprétation que la Cour donne d'une règle du droit de l'Union, dans l'exercice de la compétence que lui confère l'article 267 TFUE, éclaire et précise la signification et la portée de cette règle, telle qu'elle doit ou aurait dû être comprise et appliquée depuis le moment de son entrée en vigueur. Il s'ensuit que la règle ainsi interprétée peut et doit être appliquée par le juge à des rapports juridiques nés et constitués avant le prononcé de l'arrêt statuant sur la demande d'interprétation si, par ailleurs, les conditions permettant de porter devant les juridictions compétentes un litige relatif à l'application de ladite règle se trouvent réunies (arrêt du 16 septembre 2020, Romenergo et Aris Capital, C-339/19, EU:C:2020:709, point 47 ainsi que jurisprudence citée).

126 À cet égard, il convient encore de préciser qu'une limitation dans le temps des effets de l'interprétation retenue n'a pas été opérée dans les arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), et du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), de sorte que, conformément à la jurisprudence rappelée au point 119 du présent arrêt, elle ne saurait intervenir dans un arrêt de la Cour postérieur à ceux-ci.

127 Enfin, s'agissant de l'incidence du constat de l'éventuelle incompatibilité de la loi de 2011 avec la directive 2002/58, lue à la lumière de la Charte, sur la recevabilité des preuves soulevées contre

G.D. dans le cadre de la procédure pénale, il suffit de renvoyer à la jurisprudence de la Cour y afférente, en particulier aux principes rappelés aux points 41 à 44 de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), (C-746/18, EU:C:2021:152), dont il découle que cette recevabilité relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité.

128 Eu égard aux considérations qui précèdent, il convient de répondre aux cinquième et sixième questions que le droit de l'Union doit être interprété en ce sens qu'il s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de la Charte. L'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect, notamment, des principes d'équivalence et d'effectivité.

Sur les dépens

129 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 :

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

2) **L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8, 11 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une législation nationale en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées par les fournisseurs de services de communications électroniques, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombe à un fonctionnaire de police, assisté par une unité instituée au sein de la police jouissant d'un certain degré d'autonomie dans l'exercice de sa mission et dont les décisions peuvent faire ultérieurement l'objet d'un contrôle juridictionnel.**

3) **Le droit de l'Union doit être interprété en ce sens qu'il s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de la charte des droits fondamentaux. L'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect, notamment, des principes d'équivalence et d'effectivité.**

Signatures

---

* Langue de procédure : l'anglais.