Recueil de la jurisprudence

ARRÊT DE LA COUR (première chambre)

7 septembre 2023 *

« Renvoi préjudiciel – Télécommunications – Traitement des données à caractère personnel dans le secteur des communications électroniques – Directive 2002/58/CE – Champ d'application – Article 15, paragraphe 1 – Données conservées par les fournisseurs de services de communications électroniques et mises à la disposition des autorités en charge de procédures pénales – Utilisation ultérieure de ces données lors d'une enquête portant sur une faute de service »

Dans l'affaire C-162/22,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Lietuvos vyriausiasis administracinis teismas (Cour administrative suprême de Lituanie), par décision du 24 février 2022, parvenue à la Cour le 3 mars 2022, dans la procédure engagée par

A. G.

en présence de :

Lietuvos Respublikos generalinė prokuratūra,

LA COUR (première chambre),

composée de M. A. Arabadjiev, président de chambre, MM. P. G. Xuereb (rapporteur), T. von Danwitz, A. Kumin et M^me^ I. Ziemele, juges,

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

greffier : M^me^ A. Lamote, administratrice,

vu la procédure écrite et à la suite de l'audience du 2 février 2023,

considérant les observations présentées :

– pour A. G., par M^e^ G. Danėlius, advokatas,

– pour le gouvernement lituanien, par M. S. Grigonis, M^mes^ V. Kazlauskaitė-Švenčionienė et V. Vasiliauskienė, en qualité d'agents,

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

* Langue de procédure : le lituanien.

– pour le gouvernement estonien, par M^me^ M. Kriisa, en qualité d'agent,

– pour l'Irlande, par M^me^ M. Browne, MM. A. Joyce et M. Tierney, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement français, par M. R. Bénard, en qualité d'agent,

– pour le gouvernement italien, par M^me^ G. Palmieri, en qualité d'agent, assistée de M. A. Grumetto, avvocato dello Stato,

– pour le gouvernement hongrois, par M^me^ Zs. Biró-Tóth et M. M. Z. Fehér, en qualité d'agents,

– pour la Commission européenne, par MM. S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal et F. Wilman, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 30 mars 2023,

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 »).

2 Cette demande a été présentée dans le cadre d'une procédure engagée par A. G. au sujet de la légalité de décisions du Lietuvos Respublikos generalinė prokuratūra (parquet général de la République de Lituanie, ci-après le « parquet général ») le révoquant de ses fonctions de procureur.

Le cadre juridique

Le droit de l'Union

3 L'article 1^er^ 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 la Communauté.

[...]

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, 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. »

4 L'article 5 de cette directive, intitulé « Confidentialité des communications », prévoit, à son paragraphe 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. »

5 L'article 15 de ladite directive, intitulé « Application de certaines dispositions de la directive 95/46/CE », 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/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)]. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, [TUE]. »

Le droit lituanien

La loi sur les communications électroniques

6 L'article 65, paragraphe 2, du Lietuvos Respublikos elektroninių ryšių įstatymas (loi de la République de Lituanie sur les communications électroniques), du 15 avril 2004 (Žin., 2004, nº 69-2382), dans sa version applicable aux faits au principal (ci-après la « loi sur les communications électroniques »), oblige les fournisseurs de services de communications électroniques à conserver les données visées à l'annexe 1 de cette loi et, le cas échéant, à les mettre à la disposition des autorités compétentes afin que ces dernières puissent les utiliser aux fins de la lutte contre la criminalité grave.

7 Conformément à l'annexe 1 de la loi sur les communications électroniques, les catégories de données qui doivent être conservées sont les suivantes :

« 1. Les données nécessaires pour trouver et déterminer la source d'une communication : [...] 2. Les données nécessaires pour déterminer la destination d'une communication : [...] 3. Les données nécessaires pour déterminer la date, l'heure et la durée d'une communication : [...] 4. Les données nécessaires pour déterminer le type de communication : [...] 5. Les données nécessaires pour déterminer le matériel de communication des utilisateurs ou ce que pourrait être leur matériel : [...] 6. Les données nécessaires pour localiser le matériel de communication mobile : [...] »

8 En vertu de l'article 77, paragraphe 4, de cette loi, lorsqu'il existe une décision de justice motivée ou une autre base juridique prévue par la loi, les fournisseurs de services de communications électroniques doivent rendre techniquement possible, notamment pour les organes de renseignement criminel et les organes d'instruction, selon les modalités prévues par le Lietuvos Respublikos baudžiamojo proceso kodeksas (code de procédure pénale de la République de Lituanie, ci-après le « code de procédure pénale »), le contrôle du contenu des informations acheminées par les réseaux de communications électroniques.

La loi sur le renseignement criminel

9 L'article 6, paragraphe 3, point 1, du Lietuvos Respublikos kriminalinės žvalgybos Įstatymas (loi de la République de Lituanie sur le renseignement criminel), du 2 octobre 2012 (Žin., 2012, nº 122-6093), dans sa version applicable aux faits au principal (ci-après la « loi sur le renseignement criminel »), dispose que, lorsque les conditions prévues par cette loi pour justifier une opération de renseignement criminel sont remplies et sur autorisation d'un membre du ministère public ou d'une juridiction, les organes de renseignement criminel ont le pouvoir, outre ceux énumérés aux paragraphes 1 et 2 du même article, d'obtenir des informations auprès des fournisseurs de services de communications électroniques.

10 L'article 8, paragraphe 1, de ladite loi prévoit qu'une enquête est menée par les organismes de renseignement en matière pénale lorsque, notamment, des informations sont disponibles sur la préparation ou la commission d'une infraction très grave, grave, ou relativement grave ou sur les personnes qui préparent, commettent ou ont commis une telle infraction. L'article 8, paragraphe 3, de la même loi précise que, si une telle enquête relève la présence d'indices d'infraction pénale, une instruction pénale est ouverte immédiatement.

11 Aux termes de l'article 19, paragraphe 1, point 5, de la loi sur le renseignement criminel, les informations provenant d'opérations de renseignement criminel peuvent être utilisées dans les cas désignés aux paragraphes 3 et 4 de cet article et dans d'autres cas prévus par la loi. En vertu du paragraphe 3 dudit article, les informations provenant d'opérations de renseignement criminel relatives à un fait présentant des caractéristiques d'infraction apparentée à la corruption peuvent être déclassifiées, avec l'accord du ministère public, et utilisées dans le cadre d'une enquête sur des fautes disciplinaires ou de service.

Le code de procédure pénale

12 L'article 154 du code de procédure pénale prévoit que, sur décision d'un juge d'instruction prononcée à la demande d'un membre du ministère public, un enquêteur peut écouter les conversations acheminées par les réseaux de communications électroniques, les faire transcrire, contrôler d'autres informations acheminées par les réseaux de communications électroniques et les enregistrer et les conserver, s'il existe, notamment, des raisons de penser que cela permettra d'obtenir des données au sujet d'une infraction très grave ou grave en cours de préparation ou de perpétration ou qui a été perpétrée, ou au sujet d'une infraction relativement grave ou d'une infraction non grave.

13 L'article 177, paragraphe 1, de ce code dispose que les données de l'instruction sont confidentielles et que, jusqu'à l'examen de l'affaire en justice, ces données ne peuvent être divulguées que sur autorisation du ministère public et seulement dans la mesure où cela est reconnu justifiable.

14 Aux fins de la mise en œuvre de l'article 177 dudit code, les Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (recommandations relatives à la transmission et l'utilisation des données issues de l'instruction à des fins autres que les poursuites ainsi qu'à la protection de ces données), approuvées par le décret n° I-279 du procureur général du 17 août 2017 (TAR, 2017, n° 2017-13413), telles que modifiées en dernier lieu par le décret n° I-211 du 25 juin 2018, s'appliquent.

15 Le point 23 de ces recommandations prévoit que, lorsqu'il reçoit une demande d'accès aux données issues de l'instruction, le procureur décide s'il y a lieu de fournir ces données. Si la décision est prise de les fournir, le procureur précise dans quelle mesure les données visées par la demande peuvent être fournies.

Le litige au principal et la question préjudicielle

16 Le parquet général a ouvert une enquête administrative contre le requérant au principal, qui exerçait à cette époque les fonctions de procureur auprès d'un parquet lituanien, au motif qu'il existait des indices selon lesquels celui-ci avait, dans le cadre d'une instruction qu'il dirigeait, illégalement fourni des informations pertinentes pour cette instruction au suspect et à son avocat.

17 Dans son rapport sur cette enquête, la commission du parquet général a constaté que le requérant au principal avait effectivement commis une faute de service.

18 Selon ce rapport, cette faute de service était démontrée par les éléments recueillis lors de l'enquête administrative. En particulier, les informations obtenues lors des opérations de renseignement criminel et les données collectées lors de deux instructions pénales auraient confirmé l'existence de communications téléphoniques entre le requérant au principal et l'avocat du suspect dans le cadre de l'instruction visant ce dernier que le requérant au principal dirigeait. Ledit rapport a relevé en outre qu'une ordonnance judiciaire avait autorisé l'interception et l'enregistrement du contenu des informations acheminées par des réseaux de communications électroniques concernant l'avocat en cause et qu'une autre ordonnance judiciaire avait autorisé la même mesure concernant le requérant au principal.

19 Sur le fondement du même rapport, le parquet général a adopté deux décrets par lesquels il a, d'une part, infligé au requérant au principal une sanction consistant en la révocation de ses fonctions et, d'autre part, révoqué ce dernier de ses fonctions.

20 Le requérant au principal a saisi le Vilniaus apygardos administracinis teismas (tribunal administratif régional de Vilnius, Lituanie) d'un recours tendant, notamment, à l'annulation de ces deux décrets.

21 Par jugement du 16 juillet 2021, cette juridiction a rejeté le recours du requérant au principal, au motif, notamment, que les opérations de renseignement criminel effectuées en l'occurrence étaient légales et que les informations rassemblées conformément aux dispositions de la loi sur le renseignement criminel avaient été utilisées légalement pour apprécier l'existence d'une faute de service éventuellement commise par le requérant au principal.

22 Le requérant au principal a saisi en appel le Lietuvos vyriausiasis administracinis teismas (Cour administrative suprême de Lituanie), la juridiction de renvoi, en faisant valoir que l'accès par les organes de renseignement, dans le cadre d'une opération de renseignement criminel, aux données relatives au trafic et au contenu même des communications électroniques constituait une atteinte aux droits fondamentaux d'une telle gravité que, compte tenu des dispositions de la directive 2002/58 et de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), cet accès ne pouvait être octroyé qu'aux fins de la lutte contre des infractions graves. Or, l'article 19, paragraphe 3, de la loi sur le renseignement criminel prévoirait que de telles données peuvent être utilisées pour enquêter non seulement sur des infractions graves, mais aussi sur des fautes disciplinaires ou des fautes de service s'apparentant à des actes de corruption.

23 Selon la juridiction de renvoi, les questions soulevées par le requérant au principal portent sur deux éléments, à savoir, d'une part, l'accès aux données conservées par les fournisseurs de services de communications électroniques à des fins autres que la lutte contre les infractions graves et la prévention des menaces graves contre la sécurité publique et, d'autre part, cet accès étant obtenu, l'utilisation de ces données pour enquêter sur des fautes de service apparentées à la corruption.

24 Cette juridiction rappelle qu'il ressort de la jurisprudence de la Cour, notamment de l'arrêt du 6 octobre 2020, Privacy International (C-623/17, EU:C:2020:790, point 39), que, d'une part, l'article 15, paragraphe 1, de la directive 2002/58, lu en combinaison avec l'article 3 de celle-ci, doit être interprété en ce sens que relèvent du champ d'application de cette directive non seulement une mesure législative qui impose aux fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation, mais également une mesure législative leur imposant d'accorder aux autorités nationales compétentes l'accès à ces données. D'autre part, il découlerait de cette jurisprudence, notamment de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152, points 33 et 35), que, en ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite des infractions pénales, conformément au principe de proportionnalité, seule la lutte contre la criminalité grave et la prévention de 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, qu'elle soit généralisée et indifférenciée ou ciblée.

25 Toutefois, la Cour ne se serait pas encore prononcée sur l'incidence de l'utilisation ultérieure des données en question sur l'ingérence dans les droits fondamentaux. Dans ces circonstances, la juridiction de renvoi se demande si une telle utilisation ultérieure doit également être considérée comme constituant une ingérence d'une telle gravité dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à la justifier, ce qui exclurait la possibilité d'utiliser ces données dans des enquêtes concernant des fautes de service apparentées à la corruption.

26 Dans ces conditions, le Lietuvos vyriausiasis administracinis teismas (Cour administrative suprême de Lituanie) a décidé de surseoir à statuer et de poser à la Cour la question préjudicielle suivante :

« L'article 15, paragraphe 1, de la directive [2002/58], lu en combinaison avec les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la [Charte], doit-il être interprété en ce sens qu'il interdit aux autorités publiques compétentes d'utiliser des données, conservées par les fournisseurs de services de communications électroniques, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique, dans des enquêtes relatives à des fautes de service apparentées à la corruption, indépendamment du point de savoir si l'accès à ces données a été accordé dans le cas d'espèce à des fins de lutte contre la criminalité grave et de prévention de menaces graves contre la sécurité publique ? »

Sur la question préjudicielle

27 Par sa 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 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à ce que des données à caractère personnel relatives à des communications électroniques qui ont été conservées, en application d'une mesure législative prise au titre de cette disposition, par les fournisseurs de services de communications électroniques et qui ont par la suite été mises à la disposition, en application de cette mesure, des autorités compétentes à des fins de la lutte contre la criminalité grave puissent être utilisées dans le cadre d'enquêtes relatives à des fautes de service apparentées à la corruption.

28 À titre liminaire, il importe de relever qu'il ressort de la décision de renvoi que, si le dossier administratif afférent à la procédure aboutissant aux décrets en cause au principal, visés au point 19 du présent arrêt, comprenait également des informations qui avaient été recueillies par les autorités compétentes grâce à l'interception et à l'enregistrement de communications électroniques qui avaient été autorisés, aux fins de poursuites pénales, par deux ordonnances judiciaires, il n'en reste pas moins que la juridiction de renvoi s'interroge non pas sur l'utilisation de données à caractère personnel qui ont été obtenues sans l'intervention des fournisseurs de services de communications électroniques, mais sur l'utilisation ultérieure de données à caractère personnel qui ont été conservées par de tels fournisseurs sur le fondement d'une mesure législative de l'État membre leur imposant une telle obligation de conservation, au titre de l'article 15, paragraphe 1, de la directive 2002/58.

29 À cet égard, il ressort des indications figurant dans la demande de décision préjudicielle que les données visées par la question posée sont celles retenues en vertu de l'article 65, paragraphe 2, de la loi sur les communications électroniques, lu en combinaison avec l'annexe 1 de cette loi, qui

impose aux fournisseurs de services de communications électroniques une obligation de conserver, de manière généralisée et indifférenciée, les données relatives au trafic et les données de localisation afférentes à de telles communications aux fins de la lutte contre la criminalité grave.

30 S'agissant des conditions dans lesquelles ces données peuvent être utilisées lors d'une procédure administrative relative à des fautes de service apparentées à la corruption, il y a tout d'abord lieu de rappeler qu'un accès auxdites données ne peut être octroyé, en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, que pour autant que les mêmes données aient été conservées par ces fournisseurs d'une manière conforme à cette disposition [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 29 et jurisprudence citée]. Ensuite, une utilisation ultérieure des données relatives au trafic et des données de localisation afférentes à de telles communications aux fins de la lutte contre la criminalité grave n'est possible qu'à la condition, d'une part, que la conservation de ces données par les fournisseurs de services de communications électroniques était conforme à l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété par la jurisprudence de la Cour, et, d'autre part, que l'accès auxdites données octroyé aux autorités compétentes était lui aussi conforme à cette disposition.

31 À cet égard, la Cour a déjà jugé que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, 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 (arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland, C-793/19 et C-794/19, EU:C:2022:702, points 74 et 131 ainsi que jurisprudence citée). En revanche, elle a précisé que cet 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 (arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland, C-793/19 et C-794/19, EU:C:2022:702, point 75 et jurisprudence citée).

32 En ce qui concerne les objectifs susceptibles de justifier l'utilisation, par les autorités publiques, des données conservées par les fournisseurs de services de communications électroniques en application d'une mesure conforme à ces dispositions, il y a lieu de rappeler que l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, 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. 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 l'un de ces motifs (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 110).

33 Or, l'article 15, paragraphe 1, de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes, et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de ladite directive, devienne la règle, sauf à vider largement cette dernière disposition de sa portée (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 40).

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

35 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 que, conformément au principe de proportionnalité, il existe une hiérarchie entre ces objectifs en fonction de leur importance respective et que l'importance de l'objectif poursuivi par une telle mesure doit être en relation avec la gravité de l'ingérence qui en résulte (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 56).

36 À cet égard, 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 (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 57 ainsi que jurisprudence citée).

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

38 Il ressort de cette jurisprudence que, si la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont d'une importance moindre, dans la hiérarchie des objectifs d'intérêt général, que la sauvegarde de la sécurité nationale (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 99), leur importance dépasse toutefois celle de la lutte contre des infractions pénales en général et de la prévention de menaces non graves contre la sécurité publique.

39 Dans ce contexte, il importe néanmoins de rappeler que, ainsi qu'il ressort également du point 31 du présent arrêt, 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).

40 En outre, la Cour a déjà jugé que 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 cette directive, ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 98 ainsi que jurisprudence citée).

41 Or, ces considérations s'appliquent mutatis mutandis à une utilisation ultérieure des données relatives au trafic et à des données de localisation conservées par des fournisseurs de services de communications électroniques en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 aux fins de la lutte contre la criminalité grave. En effet, de telles données ne sauraient, après avoir été conservées et mises à la disposition des autorités compétentes aux fins de la lutte contre la criminalité grave, être transmises à d'autres autorités et utilisées afin de réaliser des objectifs, tels que, comme en l'occurrence, la lutte contre des fautes de service apparentées à la corruption, qui sont d'une importance moindre, dans la hiérarchie des objectifs d'intérêt général, que celui de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique. En effet, autoriser, dans une telle situation, un accès

aux données conservées et leur utilisation irait à l'encontre de cette hiérarchie des objectifs d'intérêt général rappelée aux points 33, 35 à 37 et 40 du présent arrêt (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 99).

42 S'agissant de l'argument soulevé par le gouvernement tchèque et par l'Irlande dans leurs observations écrites, selon lequel une procédure disciplinaire relative à des fautes de service apparentées à la corruption pourrait se rattacher à la sauvegarde de la sécurité publique, il suffit de relever que, dans sa décision de renvoi, la juridiction de renvoi n'a pas fait état d'une menace grave contre la sécurité publique.

43 Par ailleurs, s'il est vrai que les enquêtes administratives portant sur des fautes disciplinaires ou sur des fautes de service s'apparentant à des actes de corruption peuvent jouer un rôle important dans la lutte contre de tels actes, une mesure législative prévoyant de telles enquêtes ne répond pas effectivement et strictement à l'objectif de poursuite et de sanction des infractions pénales, visé à l'article 15, paragraphe 1, première phrase, de la directive 2002/58, qui ne vise que des poursuites pénales.

44 Eu égard à ce qui précède, il y a lieu de répondre à la question posée 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 ce que des données à caractère personnel relatives à des communications électroniques qui ont été conservées, en application d'une mesure législative prise au titre de cette disposition, par les fournisseurs de services de communications électroniques et qui ont par la suite été mises à la disposition, en application de cette mesure, des autorités compétentes à des fins de la lutte contre la criminalité grave puissent être utilisées dans le cadre d'enquêtes relatives à des fautes de service apparentées à la corruption.

Sur les dépens

45 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 (première chambre) dit pour droit :

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

doit être interprété en ce sens que :

il s'oppose à ce que des données à caractère personnel relatives à des communications électroniques qui ont été conservées, en application d'une mesure législative prise au titre de cette disposition, par les fournisseurs de services de communications électroniques et qui ont par la suite été mises à la disposition, en application de cette mesure, des autorités

compétentes à des fins de la lutte contre la criminalité grave puissent être utilisées dans le cadre d'enquêtes relatives à des fautes de service apparentées à la corruption.

Signatures