ARRÊT DE LA COUR (grande chambre)

6 octobre 2020 (*)

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Fournisseurs de services de communications électroniques – Transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation – Sauvegarde de la sécurité nationale – Directive 2002/58/CE – Champ d'application – Article 1er, paragraphe 3, et article 3 – Confidentialité des communications électroniques – Protection – Article 5 et article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 11 ainsi que article 52, paragraphe 1 – Article 4, paragraphe 2, TUE »

Dans l'affaire C-623/17,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni), par décision du 18 octobre 2017, parvenue à la Cour le 31 octobre 2017, dans la procédure

Privacy International

contre

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M^me^ R. Silva de Lapuerta, vice-présidente, MM. J.-C. Bonichot, A. Arabadjiev, M^me^ A. Prechal, MM. M. Safjan, P. G. Xuereb et M^me^ L. S. Rossi, présidents de chambre, MM. J. Malenovský, L. Bay Larsen, T. von Danwitz (rapporteur), M^mes^ C. Toader, K. Jürimäe, MM. C. Lycourgos et N. Piçarra, juges,

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

greffier : M^me^ C. Strömholm, administratrice,

vu la procédure écrite et à la suite de l'audience des 9 et 10 septembre 2019,

considérant les observations présentées :

– pour Privacy International, par MM. B. Jaffey et T. de la Mare, QC, par M. D. Cashman, solicitor, ainsi que par M^e^ H. Roy, avocat,

– pour le gouvernement du Royaume-Uni, par M^mes^ Z. Lavery et D. Guðmundsdóttir ainsi que par M. S. Brandon, en qualité d'agents, assistés de MM. G. Facenna et D. Beard, QC, ainsi que de MM. C. Knight et R. Palmer, barristers,

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

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

– pour le gouvernement allemand, initialement par MM. M. Hellmann, R. Kanitz, D. Klebs et T. Henze, puis par MM. J. Möller, M. Hellmann, R. Kanitz et D. Klebs, en qualité d'agents,

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

– pour le gouvernement irlandais, par M^mes^ M. Browne et G. Hodge ainsi que par M. A. Joyce, en qualité d'agents, assistés de M. D. Fennelly, barrister,

– pour le gouvernement espagnol, initialement par M. L. Aguilera Ruiz et M^me^ M. J. García-Valdecasas Dorrego, puis par M. L. Aguilera Ruiz, en qualité d'agents,

– pour le gouvernement français, initialement par M^mes^ E. de Moustier, E. Armoët et A.-L. Desjonquères ainsi que par MM. F. Alabrune, D. Colas et D. Dubois, puis par M^mes^ E. de Moustier, E. Armoët et A.-L. Desjonquères ainsi que par MM. F. Alabrune et D. Dubois, en qualité d'agents,

– pour le gouvernement chypriote, par M^mes^ E. Symeonidou et E. Neofytou, en qualité d'agents,

– pour le gouvernement letton, initialement par M^mes^ V. Soņeca et I. Kucina, puis par M^me^ V. Soņeca, en qualité d'agents,

– pour le gouvernement hongrois, initialement par MM. G. Koós, M. Z. Fehér et G. Tornyai ainsi que par M^me^ Z. Wagner, puis par MM. G. Koós et M. Z. Fehér, en qualité d'agents,

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

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

– pour le gouvernement portugais, par MM. L. Inez Fernandes et M. Figueiredo ainsi que par M^me^ F. Aragão Homem, en qualité d'agents,

– pour le gouvernement suédois, initialement par M^mes^ A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren et A. Alriksson, puis par M^mes^ H. Shev, C. Meyer-Seitz, L. Zettergren et A. Alriksson, en qualité d'agents,

– pour le gouvernement norvégien, par MM. T. B. Leming, M. Emberland et J. Vangsnes, en qualité d'agents,

– pour la Commission européenne, initialement par MM. H. Kranenborg, M. Wasmeier et D. Nardi ainsi que M^me^ P. Costa de Oliveira, puis par MM. H. Kranenborg, M. Wasmeier et D. Nardi, en qualité d'agents,

– pour le Contrôleur européen de la protection des données, par M. T. Zerdick et M^me^ A. Buchta, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 15 janvier 2020,

rend le présent

Arrêt

1 La demande de décision préjudicielle porte sur l'interprétation de l'article 1^er^, paragraphe 3, et 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 »), lus à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7 et 8 et 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 Privacy International au Secretary of State for Foreign and Commonwealth Affairs (ministre des Affaires étrangères et du Commonwealth, Royaume-Uni), au Secretary of State for the Home Departement (ministre de l'Intérieur, Royaume-Uni), au Government Communications Headquarters (quartier général des communications, Royaume-Uni) (ci-après le « GCHQ »), au Security Service (service de sécurité, Royaume-Uni, ci-après le « MI5 ») et au Secret Intelligence Service (service secret de renseignement, Royaume-Uni, ci-après le « MI6 »), au sujet de la légalité d'une législation autorisant l'acquisition et l'utilisation par les services de sécurité et de renseignement de données relatives à des communications en masse *(bulk communications data)*.

Le cadre juridique

Le droit de l'Union

La directive 95/46

3 La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31), a été abrogée, avec effet au 25 mai 2018, par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (JO 2016, L 119, p. 1). L'article 3 de ladite directive, intitulé « Champ d'application », était libellé comme suit :

« 1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère

personnel contenues ou appelées à figurer dans un fichier.

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

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

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

La directive 2002/58

4 Les considérants 2, 6, 7, 11, 22, 26 et 30 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], 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.

[...]

(22) L'interdiction du stockage des communications et des données relatives au trafic y afférentes par des personnes autres que les utilisateurs ou sans le consentement de ceux-ci ne vise pas à interdire tout stockage automatique, intermédiaire et transitoire de ces informations si ce stockage a lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques, pour autant que les informations ne soient pas stockées pour une durée plus longue que le temps nécessaire à la transmission et à la gestion du trafic et qu'au cours de la période de stockage la confidentialité des informations reste garantie. Dans la mesure où l'exige la transmission plus efficace d'informations accessibles au public à d'autres destinataires du service à leur demande, la présente directive ne fait pas obstacle à ce que ces informations soient stockées plus longtemps, à condition qu'elles soient accessibles au public en tout état de cause et sans aucune restriction et que toute donnée concernant les abonnés ou utilisateurs individuels qui les demandent soit effacée.

[...]

(26) Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales. Ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Tout autre traitement de ces données [...] ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes fournies par le fournisseur du service de communications électroniques accessible au public sur la nature des autres traitements qu'il envisage d'effectuer, ainsi que sur le droit de l'abonné de ne pas donner son consentement à ces traitements ou de retirer son consentement. Il convient également d'effacer ou de rendre anonymes les données relatives au trafic utilisées pour la commercialisation de services de communications [...]

[...]

(30) Les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires. [...] »

5 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 [TFUE], 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. »

6 Selon l'article 2 de cette directive, intitulé « Définitions » :

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

Les définitions suivantes sont aussi applicables :

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 ;

[...] »

7 L'article 3 de ladite directive, 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. »

8 Aux termes de l'article 5 de la directive 2002/58, 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. »

9 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. »

10 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. [...] »

11 L'article 15 de ladite directive, 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 règlement 2016/679

12 L'article 2 du règlement 2016/679 dispose :

« 1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;

b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ;

[...]

d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

[...] »

13 L'article 4 de ce règlement prévoit :

« Aux fins du présent règlement, on entend par :

[...]

2) "traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

[...] »

14 Aux termes de l'article 23, paragraphe 1, du même règlement :

« Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :

a) la sécurité nationale ;

b) la défense nationale ;

c) la sécurité publique ;

d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ;

f) la protection de l'indépendance de la justice et des procédures judiciaires ;

g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière ;

h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) ;

i) la protection de la personne concernée ou des droits et libertés d'autrui ;

j) l'exécution des demandes de droit civil. »

15 Selon l'article 94, paragraphe 2, du règlement 2016/679 :

« Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive [95/46] s'entendent comme faites au comité européen de la protection des données institué par le présent règlement. »

Le droit du Royaume-Uni

16 L'article 94 du Telecommunications Act 1984, dans sa version applicable aux faits au principal (ci-après la « loi de 1984 »), intitulé « Instructions dans l'intérêt de la sécurité nationale etc. », dispose :

« (1) Le ministre peut, après consultation d'une personne à laquelle s'applique le présent article, donner à cette personne des instructions de caractère général, dans la mesure de ce qui, aux yeux du ministre, est nécessaire dans l'intérêt de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni.

(2) S'il apparaît nécessaire au ministre de procéder ainsi dans l'intérêt de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni, il peut, après consultation d'une personne à laquelle s'applique le présent article, donner à cette personne des instructions lui demandant (selon les circonstances de l'espèce) d'exécuter ou de ne pas exécuter une action particulière spécifiée dans les instructions.

(2A) Le ministre ne peut donner d'instructions au titre du paragraphe (1) ou (2) que s'il estime que le comportement requis par les instructions est proportionné à l'objectif à atteindre au moyen de ce comportement.

(3) La personne à laquelle s'applique le présent article doit mettre en œuvre toutes les instructions qui lui sont données par le ministre au titre du présent article, nonobstant toute autre obligation qui lui incombe en vertu de la partie 1 ou de la partie 2, chapitre 1, du Communications Act 2003 [loi de 2003 sur les communications] et, dans le cas d'instructions données au fournisseur d'un réseau public de communications électroniques, même si lesdites instructions s'appliquent à lui au titre d'une qualité autre que celle de fournisseur d'accès à un tel réseau.

(4) Le ministre dépose auprès de chacune des chambres du Parlement une copie de toutes instructions données en vertu du présent article, sauf s'il estime que la divulgation desdites instructions serait contraire aux intérêts de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni, ou aux intérêts commerciaux d'une personne.

(5) Une personne ne doit pas divulguer, ou ne saurait être tenue de divulguer, en vertu d'une loi ou autre, de quelconques informations concernant des mesures prises conformément au présent article si le ministre lui a notifié qu'il était d'avis que la divulgation de ces informations serait contraire aux intérêts de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni, ou aux intérêts commerciaux d'une autre personne.

[...]

(8) Le présent article s'applique à l'[Office of communications (OFCOM)] et à des fournisseurs de réseaux publics de communications électroniques. »

17 L'article 21, paragraphes 4 et 6, du Regulation of Investigatory Powers Act 2000 (loi de 2010 portant réglementation des pouvoirs d'enquête, ci-après la « RIPA »), dispose :

« (4) [O]n entend par "données relatives à des communications" l'une quelconque des notions suivantes :

(a) toute donnée relative au trafic comprise dans, ou annexée à, une communication (par l'expéditeur ou autrement) aux fins de tout service postal ou de système de télécommunication par le biais duquel elle est transmise ou peut être transmise ;

(b) toute information qui n'inclut aucun contenu d'une communication (excepté toute information relevant du point (a) et qui porte sur l'utilisation effectuée par toute personne :

(i) de tout service postal ou de télécommunications ; ou

(ii) en relation avec la fourniture ou l'utilisation par toute personne de tout service de télécommunications, de toute partie d'un système de télécommunication ;

(c) toute information ne relevant pas des points (a) ou (b), qui est détenue ou obtenue, en relation avec des personnes destinataires du service, par une personne fournissant un service postal ou un service de télécommunications.

[...]

(6) [L]a notion de "donnée relative au trafic", en relation avec toute communication, vise :

(a) toute donnée identifiant ou susceptible d'identifier toute personne, tout appareil ou localisation vers lesquels, ou à partir desquels, une communication est ou peut être transmise,

(b) toute donnée identifiant ou sélectionnant, ou susceptible d'identifier ou sélectionner l'appareil par lequel la communication est ou peut être transmise,

(c) toute donnée comprenant des signaux pour l'actionnement de l'appareil utilisé dans les objectifs d'un système de communication aux fins de la transmission de toute communication, et

(d) toute donnée identifiant les données comprises dans ou jointes à une communication particulière ou d'autres données en tant que données comprises dans ou jointes à une communication particulière.

[...] »

18 Les articles 65 à 69 de la RIPA fixent les règles relatives au fonctionnement et aux compétences de l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni). Conformément à l'article 65 de cette loi, des plaintes peuvent être déposées auprès de ce tribunal s'il existe une raison de penser que des données ont été obtenues de manière inappropriée.

Le litige au principal et les questions préjudicielles

19 Au début de l'année 2015, l'existence de pratiques de recueil et d'utilisation de données relatives à des communications en masse par les différents services de sécurité et de renseignement du Royaume-Uni, à savoir le GCHQ, le MI5 et le MI6, a été rendue publique, notamment dans un rapport de l'Intelligence and Security Committee of Parliament (commission du renseignement et de la sécurité du Parlement, Royaume-Uni). Le 5 juin 2015, Privacy International, organisation non gouvernementale, a saisi l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) d'un recours contre le ministre des Affaires étrangères et du Commonwealth, le ministre de l'Intérieur ainsi que ces services de sécurité et de renseignement, en contestant la légalité de ces pratiques.

20 La juridiction de renvoi a examiné la légalité desdites pratiques au regard, tout d'abord, du droit interne et des stipulations de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »), puis avec le droit de l'Union. Dans un arrêt du 17 octobre 2016, cette juridiction a constaté que les défendeurs au principal avaient reconnu que lesdits services de sécurité et de renseignement recueillaient et utilisaient, dans le cadre de leurs activités, des ensembles de données concernant des particuliers et relevant de différentes catégories *(bulk personal data),* telles que des données biographiques ou relatives à des voyages, des informations de nature financière ou commerciale, des données en rapport avec des communications et susceptibles de comporter des données sensibles, couvertes par le secret professionnel, ou encore du matériel journalistique. Ces données, obtenues par des voies diverses, le cas échéant secrètes, seraient analysées par recoupement ainsi qu'au moyen de traitements automatisés, pourraient être divulguées à d'autres personnes et autorités, et partagées avec des partenaires étrangers. Dans ce cadre, les services de sécurité et de renseignement utiliseraient également des données relatives à des communications en masse, recueillies auprès des fournisseurs de réseaux publics de communications électroniques en vertu, notamment, d'instructions ministérielles adoptées sur le fondement de l'article 94 de la loi de 1984. Le GCHQ et le MI5 procéderaient de la sorte respectivement depuis les années 2001 et 2005.

21 Ladite juridiction a estimé que ces mesures de recueil et d'utilisation de données étaient conformes au droit interne et, depuis l'année 2015, sous réserve des questions, non encore examinées, portant sur la proportionnalité desdites mesures et sur les transferts de données à des parties tierces, à l'article 8 de la CEDH. À ce dernier égard, elle a précisé que des preuves portant sur les garanties applicables lui avaient été présentées, notamment en ce qui concerne les procédures d'accès et de divulgation hors des services de sécurité et de renseignement, les modalités de conservation des données et l'existence de contrôles indépendants.

22 En ce qui concerne la légalité des mesures de recueil et d'utilisation en cause au principal au regard du droit de l'Union, la juridiction de renvoi a examiné, dans un arrêt du 8 septembre 2017, si ces mesures relevaient du champ d'application de ce droit et, dans l'affirmative, si elles étaient compatibles avec ce droit. Cette juridiction a constaté, s'agissant des données relatives aux communications en masse, que les fournisseurs de réseaux de communications électroniques étaient tenus, en vertu de l'article 94 de la loi de 1984, en cas d'instructions en ce sens émanant d'un ministre, de fournir les données collectées dans le cadre de leur activité économique relevant du droit de l'Union aux services de sécurité et de renseignement. En revanche, tel n'était pas le cas pour le recueil des autres données, obtenues par ces services sans recourir à de tels pouvoirs contraignants. Sur la base de ce constat, cette juridiction a estimé nécessaire d'interroger la Cour en vue de déterminer si un régime tel que celui résultant de cet article 94 relève du droit de l'Union et, dans l'affirmative, si et de quelle manière les exigences posées par la jurisprudence issue de l'arrêt du 21 décembre 2016, Tele2 Sverige et

Watson e.a. (C−203/15 et C−698/15, ci-après l'« arrêt Tele2 », EU:C:2016:970), s'appliquent à ce régime.

23 À cet égard, dans sa demande de décision préjudicielle, la juridiction de renvoi indique que, selon ledit article 94, un ministre peut donner aux fournisseurs de services de communications électroniques les instructions générales ou spécifiques qui lui semblent nécessaires dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger. Renvoyant aux définitions figurant à l'article 21, paragraphes 4 et 6, de la RIPA, cette juridiction précise que les données concernées incluent les données relatives au trafic ainsi que les informations sur les services utilisés, au sens de cette dernière disposition, seul le contenu des communications étant exclu. Ces données et ces informations permettraient, notamment, de connaître le « qui, où, quand et comment » d'une communication. Lesdites données seraient transmises aux services de sécurité et de renseignement et conservées par ces derniers aux fins de leurs activités.

24 Selon ladite juridiction, le régime en cause au principal se distingue de celui résultant du Data Retention and Investigatory Powers Act 2014 (loi de 2014 sur la conservation des données et les pouvoirs d'enquête), en cause dans l'affaire ayant conduit à l'arrêt du 21 décembre 2016, Tele2 (C−203/15 et C−698/15, EU:C:2016:970), puisque ce dernier régime prévoyait la conservation des données par les fournisseurs de services de communications électroniques et leur mise à la disposition non seulement des services de sécurité et de renseignement, dans l'intérêt de la sécurité nationale, mais également d'autres autorités publiques, en fonction de leurs besoins. Cet arrêt aurait par ailleurs concerné une enquête criminelle et non la sécurité nationale.

25 La juridiction de renvoi ajoute que les bases de données constituées par les services de sécurité et de renseignement font l'objet d'un traitement de masse et automatisé, non spécifique, visant à révéler l'existence d'éventuelles menaces inconnues. À cet effet, cette juridiction expose que les ensembles de métadonnées ainsi constitués devraient être aussi complets que possible, afin de pouvoir disposer d'une « botte de foin » pour trouver « l'aiguille » qui s'y dissimule. Concernant l'utilité du recueil de données en masse par lesdits services et des techniques de consultation de ces données, ladite juridiction se réfère en particulier aux conclusions du rapport établi le 19 août 2016 par M. David Anderson, QC, alors United Kingdom Independent Reviewer of Terrorism Legislation (contrôleur indépendant du Royaume-Uni de la législation relative au terrorisme), et qui se serait fondé, pour établir ce rapport, sur un examen effectué par une équipe de spécialistes du renseignement et sur le témoignage d'agents des services de sécurité et de renseignement.

26 La juridiction de renvoi précise également que, selon Privacy International, le régime en cause au principal est illégal au regard du droit de l'Union, tandis que les défendeurs au principal estiment que l'obligation de transmission des données prévue par ce régime, l'accès à ces données ainsi que leur utilisation ne relèvent pas des compétences de l'Union, conformément, notamment, à l'article 4, paragraphe 2, TUE, selon lequel la sécurité nationale demeure de la seule responsabilité de chaque État membre.

27 À cet égard, la juridiction de renvoi considère, sur la base de l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C−317/04 et C−318/04, EU:C:2006:346, points 56 à 59), relatif au transfert des données PNR *(Passenger Name Record)* à des fins de protection de la sécurité publique, que les activités des sociétés commerciales dans le cadre du traitement et du transfert de données aux fins de protéger la sécurité nationale ne paraissent pas relever du champ d'application du droit de l'Union. Il y aurait lieu d'examiner non pas si l'activité en cause constitue un traitement de données, mais seulement si, dans sa substance et ses effets,

l'objet d'une telle activité est de soutenir une fonction essentielle de l'État, au sens de l'article 4, paragraphe 2, TUE, à travers un cadre établi par les autorités publiques concernant la sécurité publique.

28 Dans l'hypothèse où les mesures en cause au principal relèveraient néanmoins du droit de l'Union, la juridiction de renvoi estime que les exigences figurant aux points 119 à 125 de l'arrêt du 21 décembre 2016, Tele2 (C−203/15 et C−698/15, EU:C:2016:970), apparaissent inappropriées dans le contexte de la sécurité nationale et seraient de nature à entraver la capacité des services de sécurité et de renseignement à maîtriser certaines menaces pour la sécurité nationale.

29 Dans ces conditions, l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« Dans des circonstances où :

a) les capacités des [services de sécurité et de renseignement] pour utiliser les [données relatives à des communications en masse] qui leur sont fournies sont essentielles pour la protection de la sécurité nationale du Royaume-Uni, notamment dans les domaines du contre-terrorisme, du contre-espionnage et de la lutte contre la prolifération ;

b) une caractéristique fondamentale de l'utilisation des [données relatives à des communications en masse] par les [services de sécurité et de renseignement] est la découverte de menaces pour la sécurité nationale inconnues jusque-là au moyen de techniques de masse non ciblées qui exigent le regroupement des données relatives à des communications en masse en un endroit unique. Son utilité principale repose sur l'identification et l'établissement du profil rapide des cibles ainsi que sur la fourniture d'une base d'action au vu d'une menace imminente ;

c) le fournisseur d'un réseau de communications électroniques n'est pas tenu de conserver par la suite les [données relatives à des communications en masse] (au-delà de la période requise par l'activité commerciale ordinaire) qui sont conservées par l'État seul (les [services de sécurité et de renseignement]) ;

d) la juridiction nationale a jugé (sous réserve de certaines questions réservées) que les garanties entourant l'utilisation des [données relatives à des communications en masse] par les [services de sécurité et de renseignement] sont conformes aux exigences de la CEDH, et

e) la juridiction nationale a jugé que l'imposition des exigences spécifiées aux points 119 à 125 de l'arrêt [du 21 décembre 2016, Tele2 (C−203/15 et C−698/15, EU:C:2016:970)], si ces dernières étaient applicables, ferait échec aux mesures prises par les services de sécurité et de renseignement pour protéger la sécurité nationale et mettrait par là même en péril la sécurité nationale du Royaume Uni ;

1) Au vu de l'article 4 TUE et de l'article 1er, paragraphe 3, de la directive [2002/58], une exigence figurant dans des instructions données par le ministre à un fournisseur d'un réseau de communications électroniques selon lesquelles il doit fournir les données relatives à des communications en masse aux services de sécurité et de renseignement d'un État membre, relève-t-elle du champ d'application du droit de l'Union et de la directive [2002/58] ?

2) En cas de réponse affirmative à la première question, les exigences [applicables aux données relatives à des communications conservées, spécifiées aux points 119 à 125 de l'arrêt du 21 décembre 2016, Tele2 (C−203/15 et C−698/15, EU:C:2016:970)] ou toute autre exigence en plus de celles imposées par la CEDH, s'appliquent-elles à de telles instructions du ministre ? Si tel est le cas, comment et dans quelle mesure ces exigences s'appliquent-elles, eu égard à la nécessité essentielle pour les [services de sécurité et de renseignement] d'utiliser l'acquisition de masse et les techniques de traitement automatisé pour protéger la sécurité nationale et eu égard à la mesure dans laquelle de telles capacités, si elles sont conformes à la CEDH, pourraient être fondamentalement entravées par l'imposition de telles exigences ? »

Sur les questions préjudicielles

Sur la première question

30 Par sa première question, la juridiction de renvoi demande, en substance, si l'article 1er, paragraphe 3, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE, doit être interprété en ce sens que relève du champ d'application de cette directive une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale.

31 À cet égard, Privacy International avance, en substance, que, eu égard aux enseignements découlant de la jurisprudence de la Cour quant au champ d'application de la directive 2002/58, tant le recueil des données par les services de sécurité et de renseignement auprès de ces fournisseurs, en vertu de l'article 94 de la loi de 1984, que leur utilisation par lesdits services relèvent du champ d'application de cette directive, que lesdites données soient recueillies au moyen d'une transmission effectuée en temps différé ou qu'elles le soient en temps réel. En particulier, le fait que l'objectif de protection de la sécurité nationale est expressément énuméré à l'article 15, paragraphe 1, de ladite directive n'aurait pas pour conséquence l'inapplicabilité de cette dernière à de telles situations, et l'article 4, paragraphe 2, TUE n'affecterait pas cette appréciation.

32 En revanche, les gouvernements du Royaume-Uni, tchèque et estonien, l'Irlande ainsi que les gouvernements français, chypriote, hongrois, polonais et suédois font, en substance, valoir que la directive 2002/58 ne trouve pas à s'appliquer à la réglementation nationale en cause au principal, dans la mesure où celle-ci a pour finalité la sauvegarde de la sécurité nationale. Les activités des services de sécurité et de renseignement relèveraient des fonctions essentielles des États membres, tenant au maintien de l'ordre public ainsi qu'à la sauvegarde de la sécurité intérieure et de l'intégrité territoriale et, par suite, seraient de la seule compétence de ces derniers, comme en témoignerait notamment l'article 4, paragraphe 2, troisième phrase, TUE.

33 Selon ces gouvernements, la directive 2002/58 ne saurait dès lors être interprétée en ce sens que des mesures nationales visant la sauvegarde de la sécurité nationale relèvent de son champ d'application. L'article 1er, paragraphe 3, de cette directive délimiterait ce champ d'application et en exclurait, à l'instar de ce que prévoyait déjà l'article 3, paragraphe 2, premier tiret, de la directive 95/46, les activités concernant la sécurité publique, la défense et la sûreté de l'État. Ces dispositions refléteraient la répartition des compétences prévues à l'article 4, paragraphe 2, TUE et seraient privées d'effet utile si des mesures relevant du domaine de la sécurité nationale devaient respecter les exigences de la directive 2002/58. Par ailleurs, la jurisprudence

de la Cour issue de l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C−317/04 et C−318/04, EU:C:2006:346), portant sur l'article 3, paragraphe 2, premier tiret, de la directive 95/46, serait transposable à l'article 1er, paragraphe 3, de la directive 2002/58.

34 À cet égard, il a lieu d'indiquer que, aux termes de son article 1er, paragraphe 1, la directive 2002/58 prévoit, notamment, l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et des 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.

35 L'article 1er, paragraphe 3, de cette directive exclut du champ d'application de celle-ci les « activités de l'État » dans les domaines qui y sont visés, parmi lesquelles figurent les activités dans le domaine pénal ainsi que celles concernant la sécurité publique, la défense et 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. Les activités ainsi mentionnées à titre d'exemples sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (arrêt du 2 octobre 2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, point 32 et jurisprudence citée).

36 En outre, l'article 3 de la directive 2002/58 énonce que cette 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 (ci-après les « services de communications électroniques »). Partant, ladite directive doit être regardée comme régissant les activités des fournisseurs de tels services (arrêt du 2 octobre 2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, point 33 et jurisprudence citée).

37 Dans ce cadre, l'article 15, paragraphe 1, de la directive 2002/58 autorise les États membres à adopter, dans le respect des conditions qu'il prévoit, 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 [cette] directive » (arrêt du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, point 71).

38 Or, l'article 15, paragraphe 1, de la directive 2002/58 présuppose nécessairement que les mesures législatives nationales qui y sont visées relèvent du champ d'application de celle-ci, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit. En outre, de telles mesures régissent, aux fins mentionnées à cette disposition, l'activité des fournisseurs de services de communications électroniques (arrêt du 2 octobre 2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, point 34 et jurisprudence citée).

39 C'est notamment au regard de ces considérations que la Cour a jugé que 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. En effet, de telles mesures législatives impliquent obligatoirement un traitement, par lesdits fournisseurs, desdites données et ne sauraient, en ce qu'elles régissent les activités de ces mêmes fournisseurs, être assimilées à des activités propres aux États, visées à l'article 1er,

paragraphe 3, de ladite directive (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C−207/16, EU:C:2018:788, points 35 et 37 ainsi que jurisprudence citée).

40 En ce qui concerne une mesure législative telle que l'article 94 de la loi de 1984, sur le fondement duquel l'autorité compétente peut donner aux fournisseurs de services de communications électroniques l'instruction de communiquer par transmission des données en masse aux services de sécurité et de renseignement, il convient de relever que, en vertu de la définition figurant à l'article 4, point 2, du règlement 2016/679, laquelle est, conformément à l'article 2 de la directive 2002/58, lu en combinaison avec l'article 94, paragraphe 2, dudit règlement, applicable, la notion de « traitement de données à caractère personnel » désigne « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel telles que la collecte, [...], la conservation, [...], la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition [...] ».

41 Il s'ensuit qu'une communication de données à caractère personnel par transmission est, de même qu'une conservation de données ou que toute autre forme de mise à disposition, constitutive d'un traitement, au sens de l'article 3 de la directive 2002/58, et, par suite, relève du champ d'application de cette directive (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C−275/06, EU:C:2008:54, point 45).

42 En outre, eu égard aux considérations figurant au point 38 du présent arrêt et à l'économie générale de la directive 2002/58, une interprétation de cette directive selon laquelle les mesures législatives visées à son article 15, paragraphe 1, seraient exclues du champ d'application de ladite directive du fait que les finalités auxquelles de telles mesures doivent répondre recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de la même directive, priverait cet article 15, paragraphe 1, de tout effet utile (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, points 72 et 73).

43 La notion d'« activités » figurant à l'article 1er, paragraphe 3, de la directive 2002/58 ne saurait donc, comme l'a relevé en substance M. l'avocat général au point 75 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C−511/18 et C−512/18, EU:C:2020:6), auxquelles il renvoie au point 24 de ses conclusions dans la présente affaire, être interprétée comme couvrant les mesures législatives visées à l'article 15, paragraphe 1, de cette directive.

44 Les dispositions de l'article 4, paragraphe 2, TUE, auxquelles se sont référés les gouvernements mentionnés au point 32 du présent arrêt, ne sauraient infirmer cette conclusion. En effet, conformément à la jurisprudence constante de la Cour, bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit [voir, en ce sens, arrêts du 4 juin 2013, ZZ, C−300/11, EU:C:2013:363, point 38 et jurisprudence citée ; du 20 mars 2018, Commission/Autriche (Imprimerie d'État), C−187/16, EU:C:2018:194, points 75 et 76, ainsi que du 2 avril 2020, Commission/Pologne, Hongrie et République tchèque (Mécanisme temporaire de relocalisation de demandeurs de protection internationale), C−715/17, C−718/17 et C−719/17, EU:C:2020:257, points 143 et 170].

45 Il est vrai que, dans l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C−317/04 et C−318/04, EU:C:2006:346, points 56 à 59), la Cour a jugé que le transfert de données à caractère personnel par des compagnies aériennes à des autorités publiques d'un État tiers à

des fins de prévention ainsi que de lutte contre le terrorisme et d'autres crimes graves ne relevait pas, en vertu de l'article 3, paragraphe 2, premier tiret, de la directive 95/46, du champ d'application de cette directive, puisqu'un tel transfert s'insérait dans un cadre institué par les pouvoirs publics visant la sécurité publique.

46 Toutefois, eu égard aux considérations figurant aux points 36, 38 et 39 du présent arrêt, cette jurisprudence n'est pas transposable à l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58. En effet, comme l'a relevé, en substance, M. l'avocat général aux points 70 à 72 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C−511/18 et C−512/18, EU:C:2020:6), l'article 3, paragraphe 2, premier tiret, de la directive 95/46, auquel se rapporte ladite jurisprudence, excluait du champ d'application de cette dernière directive, de manière générale, les « traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État », sans opérer de distinction en fonction de l'auteur du traitement de données concerné. En revanche, dans le cadre de l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58, une telle distinction s'avère nécessaire. En effet, ainsi qu'il ressort des points 37 à 39 et 42 du présent arrêt, l'ensemble des traitements de données à caractère personnel effectués par les fournisseurs de services de communications électroniques relève du champ d'application de ladite directive, en ce compris les traitements qui découlent d'obligations qui leur sont imposées par les pouvoirs publics, alors que ces derniers traitements pouvaient, le cas échéant, relever du champ d'application de l'exception prévue à l'article 3, paragraphe 2, premier tiret, de la directive 95/46, compte tenu de la formulation plus large de cette disposition, visant l'ensemble des traitements, quel qu'en soit l'auteur, ayant pour objet la sécurité publique, la défense ou la sûreté de l'État.

47 Par ailleurs, il y a lieu de relever que la directive 95/46, en cause dans l'affaire ayant conduit à l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C−317/04 et C−318/04, EU:C:2006:346), a été, en vertu de l'article 94, paragraphe 1, du règlement 2016/679, abrogée et remplacée par celui-ci, avec effet au 25 mai 2018. Or, si ledit règlement précise, à son article 2, paragraphe 2, sous d), qu'il ne s'applique pas aux traitements effectués « par les autorités compétentes » à des fins, notamment, de prévention et de détection des infractions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, il ressort de l'article 23, paragraphe 1, sous d) et h), du même règlement que les traitements de données à caractère personnel effectués à ces mêmes fins par des particuliers relèvent du champ d'application de celui-ci. Il s'ensuit que l'interprétation de l'article 1er, paragraphe 3, de l'article 3 et de l'article 15, paragraphe 1, de la directive 2002/58 qui précède est cohérente avec la délimitation du champ d'application du règlement 2016/679 que cette directive complète et précise.

48 En revanche, lorsque les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, sans imposer des obligations de traitement aux fournisseurs de services de telles communications, la protection des données des personnes concernées relève non pas de la directive 2002/58 mais du seul droit national, sous réserve de l'application de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89), de telle sorte que les mesures en cause doivent respecter notamment le droit national de rang constitutionnel et les exigences de la CEDH.

49 Au regard des considérations qui précèdent, il convient de répondre à la première question que l'article 1er, paragraphe 3, l'article 3 et l'article 15, paragraphe 1, de la directive 2002/58, lus à la lumière de l'article 4, paragraphe 2, TUE, doivent être interprétés en ce sens que relève du champ d'application de cette directive une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale.

Sur la seconde question

50 Par sa seconde question, la juridiction de renvoi cherche, en substance, à savoir si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

51 À titre liminaire, il convient de rappeler que, selon les indications figurant dans la demande de décision préjudicielle, l'article 94 de la loi de 1984 autorise le ministre à imposer aux fournisseurs de services de communications électroniques, par voie d'instructions, lorsqu'il l'estime nécessaire dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger, de transmettre aux services de sécurité et de renseignement les données relatives aux communications en masse, ces données incluant les données relatives au trafic et les données de localisation ainsi que des informations sur les services utilisés, au sens de l'article 21, paragraphes 4 et 6, de la RIPA. Cette dernière disposition couvre, entre autres, les données nécessaires pour identifier la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, le numéro de téléphone de l'appelant et le numéro appelé, les adresses IP de la source et du destinataire de la communication ainsi que les adresses des sites Internet visités.

52 Une telle communication par transmission des données concerne l'ensemble des utilisateurs des moyens de communications électroniques, sans qu'il soit précisé si cette transmission doit intervenir en temps réel ou de manière différée. Une fois transmises, ces données sont, selon les indications figurant dans la demande de décision préjudicielle, conservées par les services de sécurité et de renseignement et demeurent à la disposition de ces derniers aux fins de leurs activités, à l'instar des autres bases de données que ces services détiennent. En particulier, les données ainsi recueillies, qui sont soumises à des traitements et à des analyses de masse et automatisés, peuvent être recoupées avec d'autres bases de données comportant différentes catégories de données à caractère personnel en masse ou être divulguées hors de ces services et à des États tiers. Enfin, ces opérations ne sont pas subordonnées à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante et ne donnent lieu à aucune information des personnes concernées.

53 La directive 2002/58 a 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, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, 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 ».

54 À cet effet, l'article 5, paragraphe 1, de la directive 2002/58 dispose que « 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 ». Cette même disposition souligne également que, « [e]n particulier, [les États membres] 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 », et précise que « [ce] paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité. »

55 Ainsi, cet article 5, paragraphe 1, 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. Eu égard au caractère général de son libellé, cette disposition couvre nécessairement toute opération permettant à des tiers de prendre connaissance des communications et des données y afférentes à des fins autres que l'acheminement d'une communication.

56 L'interdiction d'intercepter les communications et les données y afférentes figurant à l'article 5, paragraphe 1, de la directive 2002/58 englobe donc toute forme de mise à disposition par les fournisseurs de services de communications électroniques de données relatives au trafic et de données de localisation à des autorités publiques, tels des services de sécurité et de renseignement, ainsi que la conservation desdites données par ces autorités, quelle que soit l'utilisation ultérieure qui est faite de celles-ci.

57 Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C−511/18, C−512/18 et C−520/18, point 109).

58 Toutefois, 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.

59 Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 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, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, points 89 et 104, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C−511/18, C−512/18 et C−520/18, point 111).

60 En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et 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 réglementation 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 (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, points 25 et 70, ainsi que du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

61 Ces mêmes questions se posent également pour d'autres types de traitement de données, tels que leur transmission à des personnes autres que les utilisateurs ou l'accès à ces données en vue de leur utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 122 et 123 ainsi que jurisprudence citée].

62 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 (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C−274/99 P, EU:C:2001:127, point 39, et du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, point 93 et jurisprudence citée).

63 Toutefois, les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C−311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

64 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.

65 Il convient d'ajouter que l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence

dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné (arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C−311/18, EU:C:2020:559, point 175 ainsi que jurisprudence citée).

66 En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi.

67 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, ce en effectuant une pondération équilibrée entre l'objectif et les intérêts et droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C−73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C−92/09 et C−93/09, EU:C:2010:662, points 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights Ireland e.a., C−293/12 et C−594/12, EU:C:2014:238, point 52 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

68 Pour satisfaire à l'exigence de proportionnalité, une réglementation 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 réglementation 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 [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, points 54 et 55, ainsi que du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, point 117 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

69 S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause au principal, satisfait aux exigences 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, il convient de relever que la transmission des données relatives au trafic et des données de localisation à des personnes autres que les utilisateurs, telles que des services de sécurité et de renseignement, déroge au principe de confidentialité. Dès lors que cette opération est effectuée, comme en l'occurrence, de manière généralisée et indifférenciée, elle a pour effet de faire de la dérogation à l'obligation de principe de garantir la confidentialité des données la règle, alors que le système mis en place par la directive 2002/58 exige qu'une telle dérogation demeure l'exception.

70 En outre, conformément à la jurisprudence constante de la Cour, la transmission des données relatives au trafic et des données de localisation à un tiers constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure qui est faite de ces données. À cet égard, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée, et arrêt du 6 octobre 2020, La Quadrature du Net e.a., C−511/18, C−512/18 et C−520/18, points 115 et 116].

71 L'ingérence que comporte la transmission des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement dans le droit consacré à l'article 7 de la Charte doit être considérée comme étant particulièrement grave, compte tenu notamment du caractère sensible des informations que peuvent fournir ces données et, notamment, de la possibilité d'établir à partir de celles-ci le profil des personnes concernées, une telle information étant tout aussi sensible que le contenu même des communications. En outre, elle est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C−293/12 et C−594/12, EU:C:2014:238, points 27 et 37, ainsi que du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, points 99 et 100).

72 Il convient de relever encore qu'une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible, à elle seule, 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 la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés (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 28 ; du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, point 101, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C−511/18, C−512/18 et C−520/18, point 118).

73 Enfin, 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 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.

74 S'agissant des objectifs susceptibles de justifier de telles ingérences, plus particulièrement de l'objectif de sauvegarde de la sécurité nationale, en cause au principal, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C−511/18,

C−512/18 et C−520/18, point 135).

75 Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, 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. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, mêmes graves, à 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 6 octobre 2020, La Quadrature du Net e.a., C−511/18, C−512/18 et C−520/18, point 136).

76 Toutefois, pour satisfaire à l'exigence de proportionnalité rappelée au point 67 du présent arrêt, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, une réglementation nationale comportant une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte doit respecter les exigences résultant de la jurisprudence citée aux points 65, 67 et 68 du présent arrêt.

77 En particulier, s'agissant de l'accès d'une autorité à des données à caractère personnel, une réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 192 et jurisprudence citée].

78 Ainsi, et dès lors qu'un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, une réglementation nationale régissant l'accès aux données relatives au trafic et aux données de localisation 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 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, point 119 et jurisprudence citée).

79 Ces exigences s'appliquent, a fortiori, à une mesure législative, telle que celle en cause au principal, sur le fondement de laquelle l'autorité nationale compétente peut imposer aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement. En effet, une telle transmission a pour effet de mettre ces données à la disposition des autorités publiques [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 212].

80 Dès lors que la transmission des données relatives au trafic et des données de localisation a lieu de manière généralisée et indifférenciée, elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement pourrait avoir un lien, même indirect ou lointain, avec l'objectif de sauvegarde de la sécurité nationale et, en particulier, sans que soit établie une relation entre les données dont la transmission est prévue et une menace pour la sécurité nationale (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, points 57 et 58, ainsi que du 21 décembre 2016, Tele2, C−203/15 et C−698/15, EU:C:2016:970, point 105). Eu égard au fait que la transmission de telles données aux autorités publiques équivaut, conformément à ce qui a été constaté au point 79 du présent arrêt, à un accès, il convient de considérer qu'une réglementation permettant une transmission généralisée et indifférenciée des données aux autorités publiques, implique un accès général.

81 Il en résulte qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte.

82 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la seconde question que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

Sur les dépens

83 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celles-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 1er, paragraphe 3, l'article 3 et 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, lus à la lumière de l'article 4, paragraphe 2, TUE, doivent être interprétés en ce sens que relève du champ d'application de cette directive une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale.**

2) **L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et 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 une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de**

la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

Signatures

---

* Langue de procédure : l'anglais.