Recueil de la jurisprudence

ARRÊT DE LA COUR (grande chambre)

2 octobre 2018 *

« Renvoi préjudiciel – Communications électroniques – Traitement des données à caractère personnel – Directive 2002/58/CE – Articles 1er et 3 – Champ d'application – Confidentialité des communications électroniques – Protection – Articles 5 et 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7 et 8 – Données traitées dans le cadre de la fourniture de services de communications électroniques – Accès des autorités nationales aux données à des fins d'enquête – Seuil de gravité de l'infraction susceptible de justifier l'accès aux données »

Dans l'affaire C-207/16,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone, Espagne), par décision du 6 avril 2016, parvenue à la Cour le 14 avril 2016, dans la procédure engagée par

Ministerio Fiscal,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. A. Tizzano, vice-président, Mme R. Silva de Lapuerta, MM. T. von Danwitz (rapporteur), J. L. da Cruz Vilaça, C. G. Fernlund et C. Vajda, présidents de chambre, MM. E. Juhász, A. Borg Barthet, Mme C. Toader, MM. M. Safjan, D. Šváby, Mme M. Berger, MM. E. Jarašiūnas et E. Regan, juges,

avocat général : M. H. Saugmandsgaard Øe,

greffier : Mme L. Carrasco Marco, administrateur,

vu la procédure écrite et à la suite de l'audience du 29 janvier 2018,

considérant les observations présentées :

– pour le Ministerio Fiscal, par Mme E. Tejada de la Fuente,

– pour le gouvernement espagnol, par M. M. Sampol Pucurull, en qualité d'agent,

– pour le gouvernement tchèque, par MM. M. Smolek et J. Vláčil ainsi que par Mme A. Brabcová, en qualité d'agents,

– pour le gouvernement danois, par M. J. Nymann-Lindegren et Mme M. Wolff, en qualité d'agents,

– pour le gouvernement estonien, par Mme N. Grünberg, en qualité d'agent,

* Langue de procédure : l'espagnol.

– pour l'Irlande, par M^mes^ M. Browne, L. Williams et E. Creedon ainsi que par M. A. Joyce, en qualité d'agents, assistés de M^me^ E. Gibson, BL,

– pour le gouvernement français, par M. D. Colas ainsi que par M^mes^ E. de Moustier et E. Armoet, en qualité d'agents,

– pour le gouvernement letton, par M^mes^ I. Kucina et J. Davidoviča, en qualité d'agents,

– pour le gouvernement hongrois, par MM. M. Fehér et G. Koós, en qualité d'agents,

– pour le gouvernement autrichien, par M^me^ C. Pesendorfer, en qualité d'agent,

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

– pour le gouvernement du Royaume-Uni, par M. S. Brandon et M^me^ C. Brodie, en qualité d'agents, assistés de M. C. Knight, barrister, et M. G. Facenna, QC,

– pour la Commission européenne, par M^mes^ I. Martínez del Peral et P. Costa de Oliveira ainsi que par MM. R. Troosters et D. Nardi, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 3 mai 2018,

rend le présent

Arrêt

1 La demande de décision préjudicielle porte, en substance, sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive 2002/58 »), lu à la lumière des articles 7 et 8 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 recours introduit par le Ministerio Fiscal (ministère public, Espagne) contre la décision du Juzgado de Instrucción n° 3 de Tarragona (juge d'instruction n° 3 de Tarragone, ci-après le « juge d'instruction ») portant refus d'autoriser l'accès de la police judiciaire à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques.

Le cadre juridique

Le droit de l'Union

La directive 95/46

3 Aux termes de l'article 2, sous b), 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), il convient, aux

fins de cette dernière, d'entendre par « traitement de données à caractère personnel », « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

4 L'article 3 de cette directive, intitulé « Champ d'application », prévoit :

« 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 du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

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

La directive 2002/58

5 Les considérants 2, 11, 15 et 21 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].

[...]

(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 communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, 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.

[...]

(15) Une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. [...]

[...]

(21) Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, y compris de leur contenu et de toute donnée afférente à ces communications. La législation nationale de certains États membres interdit uniquement l'accès non autorisé intentionnel aux communications. »

6 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 la Communauté.

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

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité 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. »

7 Aux termes de l'article 2 de la directive 2002/58, intitulé « Définitions » :

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

Les définitions suivantes sont aussi applicables :

[...]

b) "données relatives au trafic" : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques et 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 de l’abonné ou utilisateur identifiable qui la reçoit ;

[...] »

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

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

9 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. [...]

[...]

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. [...] »

10 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.

[...] »

11 L'article 15 de ladite directive, intitulé « Application de certaines dispositions de la directive [95/46] », prévoit, à son paragraphe 1 :

« Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive [95/46]. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

Le droit espagnol

La loi 25/2007

12 L'article 1er de la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (loi 25/2007 concernant la conservation des données relatives aux communications électroniques et aux réseaux publics de communications), du 18 octobre 2007 (BOE nº 251, du 19 octobre 2007, p. 42517), dispose :

« 1. La présente loi a pour objet de réglementer l'obligation des opérateurs de conserver les données générées ou traitées dans le cadre de la prestation de services de communications électroniques ou de réseaux publics de communication, ainsi que l'obligation de communiquer ces données aux agents habilités à chaque fois que cela leur est demandé au moyen de l'autorisation judiciaire nécessaire, aux fins de détection, d'enquête et de jugement d'infractions graves prévues dans le code pénal ou dans les lois pénales spéciales.

2. La présente loi s'applique aux données relatives au trafic et aux données de localisation concernant tant les personnes physiques que morales, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré.

[...] »

Le code pénal

13 L'article 13, paragraphe 1, de la Ley Orgánica 10/1995 del Código Penal (code pénal), du 23 novembre 1995 (BOE nº 281, du 24 novembre 1995, p. 33987), est libellé comme suit :

« Sont des infractions graves celles que la loi punit d'une peine grave. »

14 L'article 33 dudit code prévoit :

« 1. En fonction de leur nature et de leur durée, les peines sont classées en graves, moins graves et légères.

2. Sont des peines graves :

a) la prison à perpétuité révisable.

b) l'emprisonnement pour une durée supérieure à cinq ans.

[...] »

Le code de procédure pénale

15 Après la date des faits au principal, la Ley de Enjuiciamiento Criminal (code de procédure pénale) a été modifiée par la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (loi organique 13/2015 portant modification du code de procédure pénale en vue du renforcement des garanties procédurales et de la réglementation des mesures d'enquête technologique), du 5 octobre 2015 (BOE nº 239, du 6 octobre 2015, p. 90192).

16 Cette loi est entrée en vigueur le 6 décembre 2015. Elle incorpore, dans le code de procédure pénale, le domaine de l'accès aux données concernant les communications téléphoniques et télématiques qui ont été conservées par les fournisseurs de services de communications électroniques.

17 L'article 579, paragraphe 1, du code de procédure pénale, dans sa version issue de la loi organique 13/2015, dispose :

« 1. Le juge peut autoriser l'interception de la correspondance privée, postale et télégraphique, y compris des fax, des Burofax et des mandats postaux internationaux, que le suspect envoie ou reçoit, ainsi que l'ouverture et l'analyse de celle-ci s'il existe des indices permettant de penser que cela permettra de découvrir ou de vérifier un fait ou un facteur pertinent pour l'affaire, dès lors que l'enquête a pour objet l'une des infractions suivantes :

1°) Des infractions intentionnelles punies d'une peine de prison maximale d'au moins trois ans ;

2°) Des infractions commises dans le cadre d'une organisation criminelle.

3°) Des infractions de terrorisme.

[...] »

18 L'article 588 ter j dudit code prévoit :

« 1. Les données électroniques conservées par les prestataires de services ou par les personnes qui fournissent la communication en application de la législation relative à la conservation de données relatives aux communications électroniques, ou de leur propre initiative pour des raisons commerciales ou autres, et qui sont liées à des processus de communication, ne pourront être communiquées afin d'être prises en compte dans le cadre de la procédure que sur autorisation judiciaire.

2. Lorsque la connaissance de ces données s'avère indispensable pour l'enquête, il convient de demander au juge compétent d'autoriser l'accès aux informations qui se trouvent dans les archives automatisées des prestataires de services, notamment pour une recherche croisée ou intelligente de données, dès lors que sont précisées la nature des données dont il est nécessaire de prendre connaissance et les raisons justifiant leur communication. »

La procédure au principal et les questions préjudicielles

19 M. Hernandez Sierra a déposé une plainte auprès de la police pour vol avec violence, survenu le 16 février 2015, au cours duquel il a été blessé et son portefeuille ainsi que son téléphone mobile lui ont été dérobés.

20 Le 27 février 2015, la police judiciaire a saisi le juge d'instruction d'une demande tendant à ordonner à divers fournisseurs de services de communications électroniques la transmission des numéros de téléphone activés, entre le 16 février et le 27 février 2015, avec le code relatif à l'identité internationale d'équipement mobile (ci-après le « code IMEI ») du téléphone mobile volé ainsi que les données à caractère personnel relatives à l'identité civile des titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code, telles que leurs nom, prénom et, le cas échéant, adresse.

21 Par ordonnance du 5 mai 2015, le juge d'instruction a rejeté cette demande. D'une part, il a jugé que la mesure exigée n'était pas utile aux fins de l'identification des auteurs de l'infraction. D'autre part, il a refusé d'accueillir la demande au motif que la loi 25/2007 limitait la transmission des données conservées par les fournisseurs des services de communications électroniques aux infractions graves. Conformément au code pénal, les infractions graves seraient punies de peines privatives de liberté supérieures à cinq ans, tandis que les faits en cause au principal ne paraissaient pas être constitutifs d'une telle infraction.

22 Le ministère public a interjeté appel de cette ordonnance devant la juridiction de renvoi, considérant que la communication des données en cause aurait dû être accordée en raison de la nature des faits et en vertu d'un arrêt du Tribunal Supremo (Cour suprême, Espagne), du 26 juillet 2010, concernant un cas similaire.

23 La juridiction de renvoi expose que, postérieurement à ladite ordonnance, le législateur espagnol a modifié le code de procédure pénale par l'adoption de la loi organique 13/2015. Cette loi, qui serait pertinente pour le sort du recours au principal, aurait introduit deux critères alternatifs nouveaux afin de déterminer le degré de gravité d'une infraction. Il s'agirait, d'une part, d'un critère matériel identifié par des comportements correspondant à des qualifications pénales dont la nature criminelle est spécifique et grave et qui sont particulièrement préjudiciables aux intérêts juridiques individuels et collectifs. D'autre part, le législateur national aurait eu recours à un critère normatif formel, fondé sur la peine prévue pour l'infraction en cause. Le seuil de trois ans d'emprisonnement qu'il prévoit désormais couvrirait, toutefois, la grande majorité des infractions. En outre, la juridiction de renvoi considère que l'intérêt de l'État à réprimer les comportements délictuels ne peut justifier des ingérences disproportionnées dans les droits fondamentaux consacrés par la Charte.

24 À cet égard, ladite juridiction estime que, dans la procédure au principal, les directives 95/46 et 2002/58 établissent le lien de rattachement avec la Charte. La réglementation nationale en cause au principal relèverait donc, conformément à l'article 51, paragraphe 1, de la Charte, du champ d'application de celle-ci, malgré l'invalidation de la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54), par l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238).

25 Dans cet arrêt, la Cour aurait reconnu que la conservation et la communication des données relatives au trafic constituent des ingérences particulièrement graves dans les droits garantis par les articles 7 et 8 de la Charte et aurait identifié les critères d'appréciation du respect du principe de proportionnalité, dont la gravité des infractions justifiant la conservation de ces données et l'accès à celles-ci à des fins d'enquête.

26 C'est dans ces conditions que l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) Est-il possible de déterminer la gravité suffisante des infractions, en tant que critère justifiant l'atteinte aux droits fondamentaux reconnus aux articles 7 et 8 de la [Charte], uniquement en prenant en considération la peine dont peut être punie l'infraction faisant l'objet d'une enquête ou est-il nécessaire, en outre, d'identifier dans le comportement délictueux un caractère préjudiciable particulier pour des intérêts juridiques individuels ou collectifs ?

2) Le cas échéant, s'il était conforme aux principes fondamentaux de l'Union appliqués par la Cour dans son arrêt [du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238] en tant que normes de contrôle strict de la directive [2002/58], de déterminer la gravité de l'infraction uniquement en fonction de la peine susceptible d'être infligée, quel devrait être le niveau minimal de cette peine ? Un niveau fixé de manière générale à un minimum de trois ans serait-il conforme ? »

La procédure devant la Cour

27 Par décision du président de la Cour du 23 mai 2016, la procédure devant la Cour a été suspendue jusqu'au prononcé de l'arrêt dans les affaires jointes Tele2 Sverige et Watson e.a., C-203/15 et C-698/15 (arrêt du 21 décembre 2016, EU:C:2016:970, ci-après l'« arrêt Tele2 Sverige et Watson e.a. »). À la suite du prononcé de cet arrêt, la juridiction de renvoi a été interrogée sur le point de savoir si elle souhaitait maintenir ou retirer sa demande de décision préjudicielle. En réponse, la juridiction de renvoi a, par lettre du 30 janvier 2017, parvenue à la Cour le 14 février 2017, fait savoir qu'elle considérait que cet arrêt ne lui permettait pas d'apprécier, avec suffisamment de certitude, la réglementation nationale en cause au principal au regard du droit de l'Union. Par suite, la procédure devant la Cour a été reprise le 16 février 2017.

Sur les questions préjudicielles

28 Le gouvernement espagnol excipe, d'une part, de l'incompétence de la Cour pour répondre à la demande de décision préjudicielle et, d'autre part, de l'irrecevabilité de cette demande.

Sur la compétence de la Cour

29 Dans ses observations écrites soumises à la Cour, le gouvernement espagnol a exprimé l'avis, auquel s'est rallié le gouvernement du Royaume-Uni lors de l'audience, selon lequel la Cour n'est pas compétente pour répondre à la demande de décision préjudicielle au motif que l'affaire au principal est, conformément à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 et à l'article 1er, paragraphe 3, de la directive 2002/58, exclue du champ d'application de ces deux directives. Cette affaire ne relèverait donc pas du champ d'application du droit de l'Union, de telle sorte que la Charte, conformément à son article 51, paragraphe 1, ne serait pas applicable.

30 Selon le gouvernement espagnol, la Cour a, certes, jugé, dans l'arrêt Tele2 Sverige et Watson e.a., qu'une mesure législative qui régit l'accès des autorités nationales aux données conservées par les fournisseurs de services de communications électroniques relève du champ d'application de la directive 2002/58. Toutefois, en l'occurrence, il s'agirait d'une demande d'accès d'une autorité publique, en vertu d'une décision judiciaire dans le cadre d'une procédure d'instruction pénale, à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques. Le gouvernement espagnol en conclut que cette demande d'accès s'inscrit dans l'exercice, par les autorités

nationales, du ius puniendi, de telle sorte qu'elle constitue une activité de l'État relative à des domaines du droit pénal relevant de l'exception prévue à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 et à l'article 1er, paragraphe 3, de la directive 2002/58.

31 Afin d'apprécier cette exception d'incompétence, il convient de relever que l'article 1er de la directive 2002/58 dispose, à son paragraphe 1, que cette directive prévoit l'harmonisation des dispositions nationales nécessaires pour, notamment, 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. Conformément à son article 1er, paragraphe 2, ladite directive précise et complète la directive 95/46 aux fins énoncées audit paragraphe 1.

32 L'article 1er, paragraphe 3, de la directive 2002/58 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 de l'État dans le domaine pénal et celles 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 (arrêt Tele2 Sverige et Watson e.a., point 69 et jurisprudence citée). Les activités qui y sont 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 (voir, par analogie, en ce qui concerne l'article 3, paragraphe 2, premier tiret, de la directive 95/46, arrêt du 10 juillet 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, point 38 et jurisprudence citée).

33 Quant à l'article 3 de la directive 2002/58, il 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 Tele2 Sverige et Watson e.a., point 70).

34 S'agissant de l'article 15, paragraphe 1, de la directive 2002/58, la Cour a déjà jugé que les mesures législatives visées à cette disposition relèvent du champ d'application de cette directive, même si elles se rapportent à des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers, et même si 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 directive 2002/58. En effet, l'article 15, paragraphe 1, de cette directive présuppose nécessairement que les mesures nationales qui y sont visées relèvent du champ d'application de ladite directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit. En outre, les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 régissent, aux fins mentionnées à cette disposition, l'activité des fournisseurs de services de communications électroniques (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., points 72 à 74).

35 La Cour a conclu que ledit article 15, paragraphe 1, lu en combinaison avec l'article 3 de la directive 2002/58, 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 portant sur l'accès des autorités nationales aux données conservées par ces fournisseurs (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., points 75 et 76).

36 En effet, la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie par l'article 5, paragraphe 1, de la directive 2002/58, s'applique aux mesures prises par toutes les personnes autres que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques. Comme le confirme le considérant 21 de cette directive,

celle-ci vise à empêcher « tout accès » non autorisé aux communications, y compris à « toute donnée afférente à ces communications », afin de protéger la confidentialité des communications électroniques (arrêt Tele2 Sverige et Watson e.a., point 77).

37 Il convient d'ajouter que des mesures législatives imposant aux fournisseurs de services de communications électroniques de conserver des données à caractère personnel ou d'accorder aux autorités nationales compétentes l'accès à ces données, impliquent nécessairement un traitement, par ces fournisseurs, desdites données (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., points 75 et 78). De telles mesures, en ce qu'elles régissent les activités desdits fournisseurs, ne sauraient donc être assimilées à des activités propres aux États, visées à l'article 1er, paragraphe 3, de la directive 2002/58.

38 En l'occurrence, ainsi qu'il ressort de la décision de renvoi, la demande en cause au principal, par laquelle la police judiciaire sollicite une autorisation judiciaire afin d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour fondement la loi 25/2007, lue en combinaison avec le code de procédure pénale, dans sa version applicable aux faits au principal, qui régit l'accès des autorités publiques à de telles données. Cette réglementation est de nature à permettre à la police judiciaire, en cas d'octroi de l'autorisation judiciaire sollicitée sur le fondement de celle-ci, d'exiger des fournisseurs de services de communications électroniques qu'ils mettent à sa disposition des données à caractère personnel et que, ce faisant, ils procèdent, eu égard à la définition figurant à l'article 2, sous b), de la directive 95/46, applicable dans le contexte de la directive 2002/58 en vertu de l'article 2, premier alinéa, de cette dernière, à un « traitement » de telles données, au sens de ces deux directives. Ladite réglementation régit donc des activités des fournisseurs de services de communications électroniques et relève, par conséquent, du champ d'application de la directive 2002/58.

39 Dans ces conditions, la circonstance soulevée par le gouvernement espagnol selon laquelle cette demande d'accès intervient dans le cadre d'une procédure d'instruction pénale ne saurait rendre la directive 2002/58 inapplicable à l'affaire au principal en vertu de l'article 1er, paragraphe 3, de celle-ci.

40 Il est également sans incidence à cet égard que la demande d'accès en cause au principal vise, ainsi qu'il ressort de la réponse écrite du gouvernement espagnol à une question posée par la Cour et comme l'ont confirmé tant ce gouvernement que le ministère public lors de l'audience, à permettre l'accès aux seuls numéros de téléphone correspondant aux cartes SIM activées avec le code IMEI du téléphone mobile volé ainsi qu'aux données relatives à l'identité civile des titulaires de ces cartes, telles que leurs nom, prénom et, le cas échéant, adresse, à l'exclusion des données relatives aux communications effectuées avec lesdites cartes SIM et des données de localisation concernant le téléphone mobile volé.

41 En effet, comme l'a relevé M. l'avocat général au point 54 de ses conclusions, la directive 2002/58 régit, en vertu de son article 1er, paragraphe 1, et de son article 3, tout traitement de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques. En outre, conformément à l'article 2, second alinéa, sous b), de cette directive, la notion de « données relatives au trafic » couvre « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques et sa facturation ».

42 À ce dernier égard, s'agissant plus particulièrement des données relatives à l'identité civile des titulaires de cartes SIM, il ressort du considérant 15 de la directive 2002/58 que les données relatives au trafic peuvent, notamment, inclure le nom et l'adresse de la personne qui émet une communication ou qui utilise une connexion pour effectuer une communication. Les données relatives à l'identité civile des titulaires de cartes SIM peuvent, en outre, s'avérer nécessaires pour la facturation des services de communications électroniques fournis et font donc partie des données relatives au trafic, telles que définies à l'article 2, second alinéa, sous b), de cette directive. Ces données relèvent par conséquent du champ d'application de la directive 2002/58.

43 Partant, la Cour est compétente pour répondre à la question posée par la juridiction de renvoi.

Sur la recevabilité

44 Le gouvernement espagnol avance que la demande de décision préjudicielle est irrecevable au motif qu'elle n'identifie pas clairement les dispositions du droit de l'Union sur lesquelles la Cour est invitée à se prononcer. Qui plus est, la demande de la police judiciaire en cause au principal porterait non pas sur l'interception des communications effectuées au moyen des cartes SIM activées avec le code IMEI du téléphone mobile volé, mais sur une mise en relation de ces cartes et de leurs titulaires, de telle sorte que la confidentialité des communications ne serait pas affectée. L'article 7 de la Charte visé par les questions préjudicielles serait donc dénué de pertinence dans le contexte de la présente affaire.

45 Conformément à la jurisprudence constante de la Cour, il appartient au seul juge national, qui est saisi du litige et qui doit assumer la responsabilité de la décision juridictionnelle à intervenir, d'apprécier, au regard des particularités de l'affaire, tant la nécessité d'une décision préjudicielle pour être en mesure de rendre son jugement que la pertinence des questions qu'il pose à la Cour. En conséquence, dès lors que les questions posées portent sur l'interprétation du droit de l'Union, la Cour est, en principe, tenue de statuer. Le refus de la Cour de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que s'il apparaît de manière manifeste que l'interprétation sollicitée du droit de l'Union n'a aucun rapport avec la réalité ou l'objet du litige au principal, lorsque le problème est de nature hypothétique ou encore lorsque la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées (arrêt du 10 juillet 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, point 31 et jurisprudence citée).

46 En l'occurrence, la décision de renvoi contient les éléments de fait et de droit suffisants tant pour l'identification des dispositions du droit de l'Union visées par les questions préjudicielles que pour la compréhension de la portée de ces questions. En particulier, il ressort de la décision de renvoi que les questions préjudicielles visent à permettre à la juridiction de renvoi d'apprécier la question de savoir si et dans quelle mesure la réglementation nationale, sur laquelle est fondée la demande de la police judiciaire en cause au principal, poursuit un objectif qui est susceptible de justifier une atteinte aux droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Or, selon les indications de cette même juridiction, cette réglementation nationale relève du champ d'application de la directive 2002/58, si bien que la Charte est applicable à l'affaire au principal. Les questions préjudicielles présentent ainsi un rapport direct avec l'objet de la procédure au principal et ne sauraient dès lors être considérées comme étant hypothétiques.

47 Dans ces conditions, les questions préjudicielles sont recevables.

Sur le fond

48 Par ses deux questions, qu'il convient d'examiner conjointement, 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 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui présente une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave et, dans l'affirmative, à l'aune de quels critères la gravité de l'infraction en cause doit être appréciée.

49 À cet égard, il ressort de la décision de renvoi que, comme l'a relevé en substance M. l'avocat général au point 38 de ses conclusions, la demande de décision préjudicielle ne vise pas à déterminer si les données à caractère personnel en cause au principal ont été conservées par les fournisseurs de services de communications électroniques dans le respect des conditions visées à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte. Cette demande porte, ainsi qu'il ressort du point 46 du présent arrêt, uniquement sur la question de savoir si et dans quelle mesure l'objectif poursuivi par la réglementation en cause au principal est susceptible de justifier l'accès d'autorités publiques, telles que la police judiciaire, à de telles données, sans que les autres conditions d'accès résultant de cet article 15, paragraphe 1, fassent l'objet de cette demande.

50 En particulier, cette juridiction s'interroge sur les éléments à prendre en compte afin d'apprécier si les infractions au regard desquelles des autorités policières peuvent être autorisées, à des fins d'enquête, à accéder à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, sont d'une gravité suffisante pour justifier l'ingérence que comporte un tel accès dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, tels qu'interprétés par la Cour dans ses arrêts du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238), et Tele2 Sverige et Watson e.a.

51 Quant à l'existence d'une ingérence dans ces droits fondamentaux, il y a lieu de rappeler que, comme l'a relevé M. l'avocat général aux points 76 et 77 de ses conclusions, l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de « grave » et sans qu'il importe 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 ladite ingérence. Un tel accès constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel [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].

52 En ce qui concerne les objectifs susceptibles de justifier une réglementation nationale, telle que celle en cause au principal, régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, il convient de rappeler que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., points 90 et 115).

53 Or, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, il y a lieu d'observer que le libellé de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les « infractions pénales » en général.

54 À cet égard, la Cour a, certes, jugé que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., point 99).

55 La Cour a toutefois motivé cette interprétation par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., point 115).

56 En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ».

57 En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général.

58 Il convient donc, avant tout, de déterminer si, en l'occurrence, en fonction des circonstances de l'espèce, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire aux données en cause au principal comporterait doit être considérée comme étant « grave ».

59 À cet égard, la demande en cause au principal par laquelle la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. Ainsi qu'il a été relevé au point 40 du présent arrêt, cette demande vise l'accès aux seuls numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne portent pas, comme l'ont confirmé tant le gouvernement espagnol que le ministère public lors de l'audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.

60 Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.

61 Dans ces conditions, l'accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d'ingérence « grave » dans les droits fondamentaux des personnes dont les données sont concernées.

62 Ainsi qu'il ressort des points 53 à 57 du présent arrêt, l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58, sans qu'il soit nécessaire que ces infractions soient qualifiées de « graves ».

63 Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

Sur les dépens

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

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

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la charte des droits fondamentaux, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

Signatures