СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA
EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL
CVRIA
LUXEMBOURG

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. HENRIK SAUGMANDSGAARD ØE
présentées le 3 mai 2018 [1]

Affaire C-207/16

Ministerio Fiscal

[demande de décision préjudicielle formée par l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone, Espagne)]

« Renvoi préjudiciel – Communications électroniques – Traitement des données à caractère personnel – Droit à la vie privée et droit à la protection de telles données – Directive 2002/58/CE – Article 1er et article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7 et 8 ainsi que article 52, paragraphe 1 – Données collectées dans le cadre de la fourniture de services de communications électroniques – Demande d'accès par une autorité policière à des fins d'enquête pénale – Principe de proportionnalité – Notion d'"infraction grave" susceptible de justifier une ingérence dans les droits fondamentaux – Critères de la gravité – Peine encourue – Seuil minimal »

1 Langue originale : le français.

I. Introduction

1. Le présent renvoi préjudiciel porte, en substance, sur l'interprétation de la notion d'« infractions graves » [2] au sens de la jurisprudence de la Cour issue de l'arrêt Digital Rights Ireland e.a. [3] (ci-après l'« arrêt Digital Rights ») puis de l'arrêt Tele2 Sverige et Watson e.a. [4] (ci-après l'« arrêt Tele2 »), où cette notion a été utilisée en tant que critère d'appréciation de la légitimité et de la proportionnalité d'une ingérence dans les droits consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), à savoir, respectivement, le droit au respect de la vie privée et familiale ainsi que le droit à la protection des données à caractère personnel.

2. Ce renvoi préjudiciel s'inscrit dans le cadre d'un recours exercé contre une décision de justice ayant refusé à des autorités policières la possibilité de se voir communiquer certaines données d'état civil détenues par des opérateurs de téléphonie mobile, en vue d'identifier des individus à des fins d'enquête pénale. La décision attaquée était motivée, notamment, par la considération que les faits à l'origine de cette enquête n'auraient pas été constitutifs d'une infraction grave, contrairement à ce qu'aurait exigé la réglementation espagnole applicable.

3. La juridiction de renvoi interroge la Cour, en substance, sur la façon de fixer le seuil de gravité des infractions à partir duquel il peut être justifié, au regard de la jurisprudence précitée, de porter atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la Charte, lors de l'accès, par les autorités nationales compétentes, à des données à caractère personnel ayant été conservées par des fournisseurs de services de communications électroniques.

4. Après avoir établi que la Cour est compétente pour statuer sur cette demande de décision préjudicielle et que cette dernière est recevable, j'entends

2 L'expression doit ici être entendue comme se référant aux seules infractions en matière pénale.

3 Arrêt du 8 avril 2014 (C-293/12 et C-594/12, EU:C:2014:238), dans lequel la Cour a déclaré invalide 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), au motif qu'« en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte » (point 69).

4 Arrêt du 21 décembre 2016 (C-203/15 et C-698/15, EU:C:2016:970), dans lequel la Cour a jugé que le droit de l'Union, *d'une part*, « s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique » et, *d'autre part*, « s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union » (dispositifs 1 et 2).

démontrer que l'accès à des données personnelles en des circonstances telles que celles de l'espèce entraîne une ingérence dans les droits fondamentaux susmentionnés qui ne correspond pas aux hypothèses où seule la lutte contre des infractions graves est susceptible de justifier l'atteinte portée auxdits droits, conformément à la jurisprudence précitée.

5. Dès lors que j'estime que, eu égard à l'objet particulier du litige au principal, il ne sera pas nécessaire que la Cour réponde aux questions préjudicielles dans leur libellé initial, ce n'est qu'à titre subsidiaire que je fournirai des indications sur les critères qui permettraient, éventuellement, de définir la notion d'« infractions graves » au sens de cette jurisprudence, en particulier au regard du critère de la peine encourue.

II. Le cadre juridique

A. Le droit de l'Union

6. 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) [5], telle que modifiée par la directive 2009/136/CE [6] (ci-après la « directive 2002/58 ») énonce dans son préambule :

« (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/CE [7], 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

5 JO 2002, L 201, p. 37.

6 Directive du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11).

7 Directive 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).

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 [ci-après la « CEDH »], telle qu'interprétée par la Cour européenne des droits de l'homme [ci-après la « Cour EDH »] 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 [CEDH] [8]. »

7. Aux termes de l'article 1er de la directive 2002/58, intitulé « Champ d'application et objectif » :

« 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 [...].

[...]

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. »

8. Son article 2, intitulé « Définitions », est libellé comme suit :

« 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") [9] s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

8 En particulier, dans le respect de l'article 8 de la CEDH, aux termes duquel :
« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

9 JO 2002, L 108, p. 33.

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 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 ;

[...] »

9. L’article 15 de la directive 2002/58, intitulé « Application de certaines dispositions de la directive [95/46] », prévoit, à son paragraphe 1, que « [l]es 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 ».

B. Le droit espagnol

1. La loi 25/2007

10. 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 [10] (ci-après la « loi 25/2007 »), a transposé en droit espagnol la directive 2006/24 [11], laquelle a été déclarée invalide par la Cour dans l'arrêt Digital Rights.

11. Aux termes de l'article 1er de la loi 25/2007, dans sa version applicable aux faits du litige au principal :

« 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.

[...] »

12. L'article 3 de ladite loi énumère les données que les opérateurs sont tenus de conserver. Il s'agit notamment, en vertu du paragraphe 1, sous a), point 1, ii), de cet article, des données nécessaires pour retrouver et identifier la source d'une communication, telles que, en ce qui concerne la téléphonie mobile, les nom et adresse de l'abonné ou de l'utilisateur inscrit.

2. Le code pénal

13. En vertu de l'article 13, paragraphe 1, du code pénal espagnol dans sa version applicable aux faits du litige au principal, « [s]ont des infractions graves celles que la loi punit d'une peine grave ».

14. L'article 33 dudit code est libellé comme suit :

« 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) L'emprisonnement à perpétuité révisable.

[10] BOE nº 251, du 19 octobre 2007, p. 42517.

[11] Cela ressort tant du préambule de ladite loi que de ses dispositions essentielles, dont le libellé est analogue à celui des dispositions correspondantes de la directive 2006/24.

b) L’emprisonnement pour une durée supérieure à cinq ans.

[...] »

3. Le code de procédure pénale

15. Le code de procédure pénale espagnol a été modifié 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 [12] (ci-après la « loi organique 13/2015 »).

16. Cette loi, entrée en vigueur le 6 décembre 2015, 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. Aux termes de l’article 579, paragraphe 1, du code de procédure pénale, dans sa version issue de ladite loi, « [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 maximale encourue d’au moins trois ans d’emprisonnement.

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

3) Des infractions de terrorisme. »

18. L’article 588 ter j de ce même code, intitulé « Données disponibles dans des archives automatisées des prestataires de services » énonce :

« 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.

12 BOE nº 239, du 6 octobre 2015, p. 90192.

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. »

III. Le litige au principal, les questions préjudicielles et la procédure devant la Cour

19. M. Hernández Sierra a déposé une plainte auprès de la police pour le vol avec violences de son portefeuille et de son téléphone mobile, qui serait survenu le 16 février 2015 et au cours duquel il aurait été sévèrement blessé.

20. Par requête du 27 février 2015, la police judiciaire a introduit, devant le Juzgado de Instrucción nº 3 de Tarragona (juge d'instruction nº 3 de Tarragone, Espagne, ci-après le « juge d'instruction »), une demande tendant à ce qu'il soit enjoint aux différents opérateurs de téléphonie de communiquer, d'une part, les numéros de téléphone ayant été activés, entre le 16 février et le 27 février 2015, avec le code IMEI [13] du téléphone mobile volé et, d'autre part, les données à caractère personnel des titulaires ou utilisateurs de tous les numéros de téléphone correspondant aux cartes SIM activées avec ledit code IMEI [14].

21. Par ordonnance du 5 mai 2015, le juge d'instruction a rejeté cette demande, aux motifs que la mesure exigée était peu utile pour identifier les auteurs de l'infraction et que, en tout état de cause, la loi 25/2007 limitait la communication des données conservées par les opérateurs de téléphonie aux infractions graves – à savoir, selon le code pénal espagnol [15], celles sanctionnées d'une peine de prison supérieure à cinq ans –, tandis que les faits en cause ne seraient pas constitutifs d'une infraction grave.

22. Le Ministerio Fiscal (ministère public espagnol), seule partie à la procédure, a interjeté appel contre cette ordonnance devant l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone, Espagne), en faisant valoir que la communication des données en cause aurait dû être accordée en raison de la

13 IMEI est l'abréviation de l'expression « International Mobile Equipment Identity » (identité internationale d'équipement mobile). L'IMEI est un code d'identification unique, composé d'une quinzaine de chiffres, qui est généralement inscrit à l'intérieur du compartiment batterie du téléphone mobile ainsi que sur la boîte et la facture remises lors de l'achat de l'appareil.

14 Le gouvernement espagnol indique que cette demande visait quatre compagnies de téléphonie et précisait qu'au cas où l'IMEI aurait utilisé le réseau de téléphonie de l'une de ces compagnies tandis que la gestion dudit réseau appartenait à un opérateur de réseau mobile virtuel, les données susmentionnées qui auraient été recueillies par ce dernier devaient aussi être fournies.

15 Voir les dispositions reproduites aux points 13 et 14 des présentes conclusions.

nature des faits et d'une décision du Tribunal Supremo (Cour suprême, Espagne) concernant un cas similaire [16].

23. Par ordonnance du 9 février 2016, ladite cour d'appel a ordonné, à titre de mesure provisoire adressée aux opérateurs de téléphonie, la prolongation de la conservation des données concernées par la demande litigieuse.

24. La décision de renvoi préjudiciel émanant de cette juridiction expose que, après l'adoption de la décision attaquée, le législateur espagnol a introduit, en vertu de la loi organique 13/2015 [17], deux critères alternatifs pour déterminer le degré de gravité d'une infraction. Le premier serait un critère matériel, attaché à des comportements qui correspondent à des qualifications pénales dont la nature criminelle est spécifique et grave, et qui sont particulièrement préjudiciables aux intérêts juridiques individuels et collectifs [18]. Le second serait un critère normatif formel, fondé exclusivement sur la peine prévue pour l'infraction en cause. Or, le seuil de trois ans d'emprisonnement que ce dernier prévoit pourrait englober la grande majorité des qualifications pénales. En outre, la juridiction de renvoi observe que l'intérêt qu'a l'État à protéger les citoyens et à réprimer les comportements délictueux ne saurait légitimer une atteinte disproportionnée aux droits fondamentaux des personnes.

25. Dans ce contexte, par décision du 6 avril 2016, parvenue à la Cour le 14 avril 2016, 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 [Digital Rights] en tant que normes de contrôle strict de la directive [déclarée invalide par cet arrêt], de déterminer

16 Voir arrêt de la Sala de lo Penal (chambre pénale), du 26 juillet 2010 (nº 745/2010, ES:TS:2010:4200), accessible à l'adresse Internet suivante : http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=5697924&links=&optimize=20100812&publicinterface=true.

17 Voir points 15 et suiv. des présentes conclusions. Selon la juridiction de renvoi, cette réforme est manifestement pertinente pour la demande de décision préjudicielle. Lors de l'audience, le gouvernement espagnol a indiqué que la nouvelle réglementation était applicable en l'espèce.

18 À savoir les infractions de terrorisme et celles commises dans le cadre d'une organisation criminelle.

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 de prison serait-il conforme ? »

26. La procédure devant la Cour a été suspendue, par décision du Président du 23 mai 2016, dans l'attente du prononcé de l'arrêt de la Cour dans les affaires jointes Tele2 Sverige et Watson e.a., C-203/15 et C-698/15.

27. Interrogée par la Cour après le prononcé de cet arrêt, daté du 21 décembre 2016 [19], la juridiction de renvoi a indiqué qu'elle entendait maintenir sa demande de décision préjudicielle. Elle a fait valoir que les questions préjudicielles qu'elle avait posées demeuraient pertinentes, en ce que ledit arrêt donnait certes des exemples d'infractions graves [20], mais ne définissait pas avec suffisamment de clarté le contenu matériel de la notion de gravité de l'infraction pouvant servir de critère d'appréciation de la justification d'une mesure d'ingérence. Or, cette notion induirait le risque que les conditions de la conservation des données et de l'accès à celles-ci soient fixées, au niveau national, d'une manière très large, qui ne respecterait pas les droits fondamentaux visés par l'arrêt Tele2. Ainsi, lors de l'adoption de la loi organique 13/2015, le législateur espagnol aurait, en dépit des critères énoncés dans l'arrêt Digital Rights [21], très sensiblement réduit, par rapport aux règles antérieures issues de la loi 25/2007, le seuil de gravité des infractions à l'égard desquelles sont autorisées la conservation et la communication de données personnelles.

28. À la suite de cette réponse, la procédure devant la Cour a été reprise, le 16 février 2017. Des observations écrites ont alors été déposées par les gouvernements espagnol, tchèque, estonien, irlandais, français, letton, hongrois, autrichien et du Royaume-Uni ainsi que par la Commission européenne.

29. En vue de l'audience, la Cour a posé des questions pour réponse écrite adressées au gouvernement espagnol, auxquelles celui-ci a répondu le 9 janvier 2018, ainsi que des questions pour réponse orale adressées à l'ensemble des

19 Voir note en bas de page 4 des présentes conclusions.

20 Voir point 103 de l'arrêt Tele2, où sont cités « la criminalité organisée et le terrorisme ». Je note que la même double illustration figurait aux points 24 et 51 de l'arrêt Digital Rights, en lien apparent avec le libellé des considérants 7 à 10 de la directive 2006/24, invalidée par cet arrêt.

21 La juridiction de renvoi mentionne, en particulier, le point 60 de l'arrêt Digital Rights, où la Cour relève que « la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne ».

intéressés visés à l'article 23 du statut de la Cour de justice de l'Union européenne.

30. Lors de l'audience, tenue le 29 janvier 2018, le ministère public espagnol, les gouvernements espagnol, tchèque, danois, estonien, irlandais, français, letton, polonais et du Royaume-Uni ainsi que la Commission ont présenté leurs observations orales.

IV. Analyse

A. Observations introductives

31. Avant de me livrer à un examen approfondi des questions soulevées par la présente demande de décision préjudicielle, j'estime nécessaire de présenter quelques observations concernant l'objet spécifique de celle-ci.

32. *Premièrement*, au vu des indications figurant dans la décision de renvoi et des informations complémentaires fournies par le gouvernement espagnol, je relève que le *litige au principal* présente des particularités notables, qui le différencient, en particulier, du contexte des affaires ayant donné lieu aux arrêts Digital Rights et Tele2 [22].

33. En effet, il apparaît que la requête des autorités policières ici en cause tend à obtenir *uniquement* des données permettant d'identifier les titulaires ou utilisateurs des numéros de téléphone qui sont attachés aux cartes SIM ayant été insérées dans le téléphone mobile volé [23]. En outre, il est constant que cette demande porte sur une période clairement définie et réduite dans le temps, à savoir une douzaine de jours [24].

34. Dans de telles circonstances, le nombre des personnes susceptibles d'être concernées par la mesure litigieuse est non pas illimité, mais restreint. De surcroît, ces personnes sont non pas n'importe quel détenteur d'une carte SIM, mais des individus ayant un profil bien particulier, puisqu'il s'agit de ceux ayant fait usage du téléphone volé après sa soustraction, voire l'ayant encore en leur possession, et qui peuvent donc légitimement se trouver suspectés soit d'être eux-mêmes les auteurs du délit, soit d'être en relation avec ces derniers.

22 À ce sujet, voir, notamment, notes en bas de page 3 et 4 des présentes conclusions.

23 À mon sens, les « titulaires ou utilisateurs » visés par cette demande sont nécessairement des personnes abonnées, enregistrées ou au moins identifiables (voir aussi note en bas de page 25 des présentes conclusions), et non des individus ayant acheté une carte SIM sans laisser de traces.

24 Voir point 20 des présentes conclusions.

35. Qui plus est, les données visées correspondent non pas à tout type de « données à caractère personnel » [25] détenues par les fournisseurs de services de communications électroniques, mais seulement à celles relatives à l'identité civile des individus susmentionnés, à savoir leur prénom, leur nom et, éventuellement, leur adresse [26], données pouvant aussi être dites « de contact ». Les autres informations concernant ces individus qui pourraient se trouver dans les archives desdits fournisseurs [27] sont, à mon avis, exclues de la procédure au principal.

36. Par ailleurs, le but ici poursuivi est, à mes yeux, de récolter des renseignements qui ne sont relatifs ni à une localisation ni à des communications en tant que telles [28], mais à des personnes physiques qui sont recherchées pour avoir pu utiliser un service de communications électroniques au moyen du téléphone volé, même si ces personnes n'ont pas procédé à un appel téléphonique concret. En effet, il ressort des explications fournies à la Cour par le ministère public espagnol que les données personnelles demandées, qui sont tirées de l'association entre une carte SIM déterminée et le numéro IMEI de l'appareil volé, peuvent techniquement être obtenues grâce à une simple connexion de ce dernier avec une borne de téléphonie mobile, alors même qu'aucun appel n'aurait été passé par le détenteur de la carte au moyen du téléphone concerné, donc indépendamment de toute communication effective [29]. Il appartiendra à la juridiction de renvoi de vérifier cette assertion à caractère factuel, qui m'apparaît toutefois suffisamment plausible pour qu'il soit raisonnable de la tenir pour véridique.

25 Conformément à la définition donnée à l'article 2, sous a), de la directive 95/46, auquel renvoie l'article 2 de la directive 2002/58, la notion de « données à caractère personnel » couvre « toute information concernant une personne physique identifiée ou identifiable », étant précisé qu'« est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». La Cour a déjà relevé que « le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel se rapporte à toute information correspondant à cette définition » (voir, notamment, arrêt du 17 octobre 2013, Schwarz, C-291/12, EU:C:2013:670, point 26) et que la portée de celle-ci est très large (voir, notamment, arrêt du 20 décembre 2017, Nowak, C-434/16, EU:C:2017:994, point 33).

26 Selon le gouvernement espagnol, l'adresse des intéressés n'a pas été explicitement demandée.

27 Informations telles que, par exemple, la situation matrimoniale d'un individu, le numéro de sa carte nationale d'identité, ses coordonnées bancaires ou son éventuel abonnement téléphonique.

28 Renseignements qui pourraient porter sur les numéros afférents à des appels entrants ou sortants, ou encore sur la date, la durée ou la fréquence de communications, voire sur le contenu de celles-ci. Le gouvernement espagnol précise que, en l'espèce, les policiers ont expressément indiqué que leur demande ne visait pas à obtenir des données protégées par le secret des communications.

29 En d'autres termes, ces données pourraient être obtenues par une simple activation de l'appareil mobile en question, qu'il soit ou non ultérieurement utilisé par son titulaire ou détenteur dans un processus de communication interpersonnelle précis.

37. Eu égard à l'ensemble de ces éléments, je souligne d'emblée que le litige au principal concerne des données à caractère personnel dont la transmission est sollicitée non pas de manière généralisée et indifférenciée, mais de manière ciblée quant aux personnes et limitée quant à la durée. En outre, les données demandées apparaissent ne pas être d'une nature particulièrement sensible à première vue, bien que les droits fondamentaux consacrés aux articles 7 et 8 de la Charte soient néanmoins susceptibles d'être affectés par l'accès à des données de ce type [30].

38. *Deuxièmement*, je note qu'il ressort des motifs de la décision de renvoi que les questions préjudicielles posées dans la présente affaire ont pour caractéristique de porter non pas sur les conditions de *la conservation* de données à caractère personnel dans le secteur des communications électroniques, mais plutôt sur les modalités de *l'accès* des autorités nationales à de telles données qui ont été conservées par les fournisseurs de services opérant dans ce secteur [31].

39. La juridiction de renvoi indique notamment que, en vertu de l'article 588 ter j du code de procédure pénale, une autorisation judiciaire est requise pour que les données électroniques archivées par les prestataires de services soient transmises aux autorités compétentes afin d'être prises en compte dans le cadre d'une procédure. Le paragraphe 1 dudit article précise que la conservation de telles données peut avoir été effectuée par des prestataires soit en application de la législation pertinente, soit de leur propre initiative pour des raisons commerciales ou autres.

40. En l'occurrence, il apparaît que les données personnelles auxquelles les autorités policières demandent à avoir accès, à des fins d'enquête, ont pu être archivées par les opérateurs de téléphonie mobile en exécution d'une obligation résultant de la loi espagnole [32]. La juridiction de renvoi ne donne pas d'indications à ce sujet, étant rappelé que sa demande de décision préjudicielle est focalisée sur l'éventuel accès à des données ayant déjà été conservées et sachant que la conformité du stockage des données aux exigences du droit de l'Union n'est pas

30 Voir points 74 et suiv. des présentes conclusions.

31 Je précise qu'un accès à des données à caractère personnel, dans l'absolu, ne présente à mes yeux pas moins de risques, pour les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, qu'une conservation de telles données. Le péril pourrait même être considéré comme supérieur, en ce que l'accès à des données conservées concrétise l'usage potentiellement nuisible qui est susceptible d'être fait de celles-ci.

32 Le gouvernement espagnol indique que les prénom, nom et, éventuellement, adresse du titulaire d'une carte SIM peuvent être conservés légalement, en Espagne. Il me paraît, en effet, résulter de l'article 1er et de l'article 3, paragraphe 1, sous a), point 1, ii), de la loi 25/2007 (voir points 10 et suiv. des présentes conclusions) que les opérateurs de téléphonie mobile sont tenus de conserver les données générées ou traitées dans le cadre de leur prestation de services, notamment les nom et adresse de l'abonné ou de l'utilisateur inscrit, dans la mesure où ces données peuvent être nécessaires pour retrouver et identifier la source d'une communication. Je rappelle que des exigences équivalentes figuraient à l'article 3 et à l'article 5, paragraphe 1, sous a), point 1, ii), de la directive 2006/24, laquelle a été transposée par ladite loi.

mise en doute dans le litige au principal [33]. Dès lors, il convient à mon avis de se fonder sur la prémisse selon laquelle les données en cause dans l'affaire au principal ont été conservées conformément à la législation nationale, dans le respect des conditions fixées à l'article 15, paragraphe 1, de la directive 2002/58, ce qu'il appartient à la juridiction de renvoi uniquement de vérifier [34].

41. Je reviendrai, dans les développements qui suivent, sur les implications juridiques des constats ici dressés à titre liminaire [35].

B. Sur les exceptions de procédure soulevées par le gouvernement espagnol

42. Le gouvernement espagnol a soulevé deux catégories d'exceptions de procédure, l'une relative à la compétence de la Cour et l'autre relative à la recevabilité de la demande de décision préjudicielle, sur lesquelles la Cour devra se prononcer avant de statuer sur le fond le cas échéant.

1. Sur la compétence de la Cour au regard du champ d'application du droit de l'Union

43. Tout d'abord, je rappelle qu'il résulte d'une jurisprudence constante que les droits fondamentaux garantis dans l'ordre juridique de l'Union, et notamment ceux consacrés aux articles 7 et 8 de la Charte, ont vocation à être appliqués seulement si la situation en cause est régie par le droit de l'Union [36]. En outre, l'article 51, paragraphe 1, de la Charte prévoit que les dispositions de celle-ci s'adressent aux États membres exclusivement « lorsqu'ils mettent en œuvre le droit de l'Union », au sens de la jurisprudence de la Cour relative à cette notion [37]. Partant, lorsqu'une situation juridique n'est pas couverte par le champ d'application du droit de l'Union, la Cour n'est pas compétente pour en connaître, et les dispositions de la Charte éventuellement invoquées ne sauraient, à elles seules, fonder cette compétence [38].

44. En l'occurrence, les questions posées par la juridiction de renvoi visent uniquement les articles 7 et 8 de la Charte ainsi que « les principes fondamentaux

33 Circonstance qui avait également été relevée par la Cour dans l'arrêt du 29 janvier 2008, Promusicae (C-275/06, EU:C:2008:54, point 45 in fine).

34 En ce sens, arrêt du 19 avril 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219, point 37).

35 En particulier, s'agissant de la compétence de la Cour et s'agissant de la réponse à la première question préjudicielle, voir respectivement points 43 et suiv. ainsi que points 70 et suiv. des présentes conclusions.

36 Voir, notamment, arrêt du 16 mai 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, point 49 et jurisprudence citée).

37 Voir, notamment, arrêt du 6 octobre 2016, Paoletti e.a. (C-218/15, EU:C:2016:748, points 14 et suiv.).

38 Voir, notamment, arrêt du 1er décembre 2016, Daouidi (C-395/15, EU:C:2016:917, point 63).

du droit de l'Union appliqués par la Cour dans son arrêt [Digital Rights] ». Cependant, cette juridiction estime que les directives applicables en matière de protection des données à caractère personnel, telles que la directive 95/46 et la directive 2002/58, établissent le lien de rattachement exigé, en vertu de l'article 51, paragraphe 1, de la Charte, entre l'affaire au principal et le droit de l'Union.

45. À cet égard, j'observe, *en premier lieu*, que le gouvernement espagnol soutient, à titre principal, que la Cour n'est pas dotée de la compétence requise pour statuer sur le présent renvoi préjudiciel, au motif que ce dernier ne concerne pas l'application du droit de l'Union. Il fait valoir, notamment, que le litige au principal serait *exclu du champ d'application du droit de l'Union*, dès lors qu'il concerne un accès de la police à des données soumis à une décision de justice dans le cadre d'une enquête, ce qui constituerait une activité de l'État en matière pénale [39] et relèverait donc des exceptions prévues à l'article 1er, paragraphe 3, de la directive 2002/58, de même qu'à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 [40]. Lors de l'audience, le gouvernement du Royaume-Uni a indiqué qu'il partageait ce point de vue du gouvernement espagnol.

46. Toutefois, j'estime que la directive 2002/58 est applicable à l'égard de mesures nationales telles que celles en cause au principal. En effet, la Cour a déjà jugé, dans l'arrêt Tele2, que les législations nationales relatives à la conservation de données à des fins de lutte contre la criminalité sont couvertes par le champ d'application de cette directive, non seulement en ce qu'elles définissent les obligations pesant à ce titre sur les fournisseurs de services de communications électroniques, mais aussi en ce qu'elles régissent l'accès des autorités nationales aux données conservées dans ce cadre [41]. À l'instar de la Commission, je suis d'avis que les considérations énoncées dans cet arrêt sont transposables aux règles nationales applicables en l'espèce, à savoir celles issues de la loi 25/2007 lue en combinaison avec le code de procédure pénale espagnol tel que modifié par la loi organique 13/2015 [42], et donc transposables à l'objet du litige au principal.

47. J'ajoute qu'il convient de ne pas confondre, d'une part, les données à caractère personnel traitées *directement* dans le cadre des activités – de nature

39 Selon le gouvernement espagnol, il s'agirait là d'un exercice du droit de punir (ius puniendi) par les autorités de l'État. À ce sujet, voir conclusions de l'avocat général Campos Sánchez-Bordona dans l'affaire Breyer (C-582/14, EU:C:2016:339, points 86 à 92).

40 Les principes énoncés à ces dispositions sont aussi mentionnés au considérant 11 de la directive 2002/58, renvoyant à son article 15, paragraphe 1 (voir points 6 et 7 des présentes conclusions).

41 Voir points 72 à 81 de l'arrêt Tele2. À ce sujet, voir aussi mes conclusions dans les affaires jointes Tele2 Sverige e.a. (C-203/15 et C-698/15, EU:C:2016:572, points 88 à 97 et point 124).

42 Voir, en particulier, l'article 1er, paragraphe 1, de la loi 25/2007 et l'article 579, paragraphe 1, du code de procédure pénale, reproduits aux points 11 et 17 des présentes conclusions, ainsi que, sur l'obligation légale pesant sur lesdits fournisseurs, point 40 des présentes conclusions.

régalienne [43] – de l'État en un domaine relevant du droit pénal [44] et, d'autre part, celles traitées dans le cadre des activités – de nature commerciale – d'un prestataire de services de communications électroniques qui sont *ensuite* utilisées par les autorités étatiques compétentes [45]. Par ailleurs, je note que la Cour a été récemment saisie d'une demande de décision préjudicielle portant, en particulier, sur l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58 dans le contexte d'une utilisation, par les services de sécurité et de renseignement d'un État membre, de données devant leur être transmises en masse par de tels prestataires [46], problématique qu'il n'y aura selon moi pas lieu de trancher dans la présente affaire [47].

48. *En second lieu*, j'observe que d'autres interrogations ont été émises au sujet du *champ d'application de la directive 2002/58*, dont dépend la compétence de la Cour dans la présente affaire, eu égard au *type de données en cause au principal*.

49. Comme je l'ai déjà indiqué [48], il ressort des éléments versés au dossier que la demande d'accès litigieuse tend à obtenir des informations sur l'identité des titulaires ou utilisateurs des numéros de téléphone correspondant aux cartes SIM ayant été activées au moyen du téléphone mobile volé, afin de retrouver les personnes ayant détenu cet appareil, et non des renseignements sur les appels éventuellement passés à partir de celui-ci.

50. En d'autres termes, même si un plus large éventail de données à caractère personnel aurait potentiellement pu être concerné au regard de la réglementation

43 Étant précisé que les activités dites « régaliennes » de l'État se rapportent aux fonctions réservées à l'État ou à ses démembrements, qu'il ne saurait déléguer à des entités privées, en particulier, celles liées à la justice, à la police et à l'armée.

44 Telles que les données traitées par les autorités policières ou judiciaires en vue de rechercher des auteurs d'infractions (par exemple, les données collectées et analysées lors d'une interception de conversations téléphoniques opérée par des policiers sur réquisition d'un juge d'instruction).

45 Telles que les données relatives aux coordonnées des utilisateurs d'un service de téléphonie qui sont exploitées à l'occasion d'une enquête pénale, comme dans le litige au principal.

46 Voir la décision de renvoi relative à l'affaire pendante Privacy International (C-623/17), qui évoque, notamment, les arrêts du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346, points 56 à 59), ainsi que du 10 février 2009, Irlande/Parlement et Conseil (C-301/06, EU:C:2009:68, points 88 et 91), dont il ressortirait que le traitement des données relatives aux passagers aériens faisant l'objet de ce premier arrêt était requis non par la réalisation d'une prestation de services, mais par la sauvegarde de la sécurité publique, et était dès lors exclu du champ d'application de la directive 95/46.

47 Étant donné que, d'une part, le litige au principal porte ici sur une transmission de données non pas massive mais ciblée et que, d'autre part, les considérations adoptées par la Cour dans l'arrêt Tele2 peuvent à mon avis être transposées en l'espèce, comme je l'ai indiqué au point 46 des présentes conclusions.

48 Voir points 33 et suiv. des présentes conclusions.

espagnole [49], le présent litige au principal porte sur des données qui sont relatives uniquement à l'identité d'« utilisateurs », au sens de l'article 2, second alinéa, sous a), de la directive 2002/58, et non à une quelconque « localisation » [50], au sens dudit article 2, second alinéa, sous c), ni à des « communications » en tant que telles, au sens de ce même article 2, second alinéa, sous d) [51].

51. Selon le ministère public espagnol, les gouvernements espagnol, danois, irlandais, letton et du Royaume-Uni ainsi que la Commission, des informations telles que celles ici en cause, pour autant qu'elles sont prises en compte isolément, c'est-à-dire indépendamment des communications effectuées le cas échéant, ne devraient, en principe, pas être couvertes non plus par la notion de « données relatives au trafic », au sens dudit article 2, second alinéa, sous b), lequel définit ces dernières comme étant « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » [52].

52. Certes, il semble que les données d'identification ici demandées par les autorités policières ne portent pas sur le « trafic » de communications proprement dit, dans la mesure où il apparaît que ces données peuvent être obtenues nonobstant une éventuelle absence totale d'appels passés avec l'appareil volé, et donc même si aucune communication interpersonnelle n'a été acheminée par un opérateur de téléphonie mobile, pendant la période ciblée [53].

53. Néanmoins, je considère qu'un litige tel que celui au principal relève du champ d'application de la directive 2002/58, dès lors que le traitement des informations associées aux cartes SIM et à leurs titulaires, visées en l'espèce, est nécessaire, d'un point de vue commercial, à la fourniture des services de communications électroniques [54], à tout le moins aux fins de facturer le service qui est fourni [55] quels que soient les appels effectués ou non dans le cadre de cette prestation.

49 Voir, notamment, article 1er, paragraphe 2, de la loi 25/2007 et article 579, paragraphe 1, du code de procédure pénale.

50 En effet, la demande des autorités policières tend à trouver non pas la position géographique de l'appareil volé ou des personnes l'ayant détenu, mais seulement l'identité de ces dernières.

51 Dispositions dudit article 2 reproduites au point 8 des présentes conclusions.

52 Données relatives au trafic qui sont régies par l'article 6 de la directive 2002/58.

53 Voir point 36 des présentes conclusions.

54 Service de communications électroniques défini à l'article 2, sous c), de la directive 2002/21 (laquelle fixe le cadre réglementaire commun en la matière), comme étant « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques [...] ».

55 Le fait que le traitement de données peut être nécessaire à la facturation du service, en particulier s'agissant des abonnés, est évoqué dans plusieurs dispositions de la directive 2002/58

54. En effet, eu égard à l'article 1er, paragraphe 1, et à l'article 3 de la directive 2002/58 [56], je partage l'opinion émise, en particulier, par la Commission, selon laquelle cette directive a vocation à régir, de façon globale, le traitement des données à caractère personnel opéré dans le cadre de la fourniture de services de communications électroniques, de sorte que son champ d'application inclut les données relatives à l'identité d'utilisateurs de tels services, comme celles ici en cause, et non pas seulement celles afférentes à une communication précise. Compte tenu aussi des objectifs de protection visés par ladite directive, qui consistent principalement en la sauvegarde de droits fondamentaux garantis par la Charte [57], j'estime donc que la notion de « communication », au sens de cet instrument, doit être entendue dans son acception large et que le principe de confidentialité des communications prévu par cet instrument [58] est bien en jeu en l'espèce.

55. Je suis aussi d'avis que cette interprétation est corroborée par un précédent arrêt de la Cour, dans lequel celle-ci a déjà admis que le champ d'application de la directive 2002/58 couvrait un litige portant sur la transmission des noms et adresses d'utilisateurs d'un service de communication électronique [59]. J'ajoute que l'article 12 de ladite directive, qui est relatif aux annuaires d'abonnés, vise, à mes yeux, certainement des données de cette nature [60] et que son considérant 15 reflète aussi une conception souple de la notion de « communication », en y incluant notamment « une adresse, fournie par celui qui émet la communication » [61].

56. De surcroît, une telle approche est cohérente avec la jurisprudence de la Cour EDH en la matière [62], étant rappelé que le préambule de la directive 2002/58

[notamment, considérants 26, 27 et 29 ; article 2, second alinéa, sous g), ainsi que article 6, paragraphes 2 et 5]. À ce sujet, voir aussi point 86 de l'arrêt Tele2 et jurisprudence citée.

56 Dispositions visant respectivement, de manière générale, le « traitement des données à caractère personnel dans le secteur des communications électroniques » et le « traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques ».

57 Voir considérants 2, 7 et 11 ainsi que article 1er, paragraphe 1, et article 15, paragraphe 3, de la directive 2002/58.

58 Voir considérant 21 ainsi que article 1er, paragraphe 1, et article 5, lequel régit spécifiquement la confidentialité des communications, de la directive 2002/58.

59 Voir arrêt du 29 janvier 2008, Promusicae (C-275/06, EU:C:2008:54, points 29 à 31 et 45).

60 Sur l'interprétation de cet article 12, voir, notamment, arrêt du 15 mars 2017, Tele2 (Netherlands) e.a. (C-536/15, EU:C:2017:214, points 33 et suiv. ainsi que jurisprudence citée).

61 Aux termes dudit considérant 15, « [u]ne 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 [...] ».

62 La notion de données relatives à la vie privée d'un individu au sens de l'article 8 de la CEDH (reproduit à la note en bas de page 8 des présentes conclusions) est interprétée par la Cour EDH de façon extensive (voir, notamment, Cour EDH, 13 février 2018, Ivashchenko c. Russie,

souligne que celle-ci entend garantir la confidentialité des communications et le droit des utilisateurs à une vie privée en conformité avec la CEDH telle qu'interprétée par ladite juridiction [63], même si ce dernier instrument n'est pas formellement intégré à l'ordre juridique de l'Union [64].

57. Par conséquent, j'estime qu'un litige tel que celui au principal relève du champ d'application matériel de la directive 2002/58 et que l'exception d'incompétence soulevée par le gouvernement espagnol doit donc être rejetée.

58. Afin d'être exhaustif, je précise cependant que, dans l'hypothèse où la directive 2002/58 ne serait pas reconnue applicable en un tel cas de figure, la directive 95/46, évoquée tant par la juridiction de renvoi que par le gouvernement espagnol, ne saurait fonder la compétence de la Cour pour statuer dans la présente affaire.

59. En effet, ainsi que la Commission l'indique, la directive 95/46 constitue, certes, l'instrument de portée générale en matière de traitement des données à caractère personnel [65], mais les questions posées par la juridiction de renvoi seraient, à mon avis, dépourvues de pertinence si elles étaient examinées sous ce seul angle, étant donné qu'elles ont pour objet de déterminer le seuil à partir duquel des infractions peuvent être qualifiées de « graves » au sens de la jurisprudence issue des arrêts Digital Rights et Tele2, lesquels ne portaient pas sur l'interprétation de ladite directive [66].

2. Sur la recevabilité de la demande de décision préjudicielle

60. Le gouvernement espagnol prétend à titre subsidiaire, dans l'hypothèse où la Cour jugerait qu'elle est compétente pour répondre aux questions posées, que la demande de décision préjudicielle devrait être déclarée irrecevable, et ce pour deux motifs.

CE:ECHR:2018:0213JUD006106410, §§ 63 et suiv.), comme cela a déjà été relevé (voir arrêt du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 59 ainsi que jurisprudence de la Cour EDH citée).

63 Voir considérants 3, 11 et 24 de la directive 2002/58.

64 Voir, notamment, arrêt Tele2 (point 120, où une analogie avec la jurisprudence de la Cour EDH est faite, ainsi que points 126 et suiv., rappelant la situation de l'Union vis-à-vis de la CEDH).

65 Tandis que la directive 2002/58 régit le secteur particulier des communications électroniques (voir, notamment, ses considérants 4 et 10 ainsi que son article 1er, paragraphes 1 et 2).

66 Je rappelle que la notion d'« infractions graves » a été introduite, en tant que critère limitatif de l'action des États membres, par la directive 2006/24 sur la conservation de données, laquelle a été déclarée invalide par l'arrêt Digital Rights, puis a été utilisée par la Cour dans l'arrêt Tele2, pour interpréter des dispositions de la directive 2002/58, dans le contexte de réglementations nationales relatives à la conservation de données et à l'accès à celles-ci (voir aussi notes en bas de page 3 et 4 des présentes conclusions). Il en résulte, selon moi, que si la directive 2002/58 était déclarée inapplicable en l'espèce, il n'y aurait pas lieu de procéder à l'interprétation de ladite notion, qui est sollicitée par la juridiction de renvoi.

61. *En premier lieu*, ce gouvernement allègue que la juridiction de renvoi *n'identifierait pas de façon claire le cadre normatif de l'Union* sur lequel la Cour doit se prononcer.

62. À ce sujet, il rappelle la jurisprudence constante selon laquelle, dans le cadre de la coopération instituée par l'article 267 TFUE, la Cour ne peut refuser de statuer sur des questions préjudicielles, lesquelles bénéficient d'une présomption de pertinence, que s'il apparaît de manière manifeste que l'interprétation ou l'appréciation de validité d'une règle de l'Union sollicitée 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 [67].

63. Cependant, je considère que, en l'occurrence, le grief formulé par le gouvernement espagnol n'est pas bien fondé. En effet, au vu des indications données par la juridiction de renvoi, j'estime que celle-ci a procédé à une identification suffisante des dispositions du droit de l'Union qui sont pertinentes selon elle. Je rappelle, d'une part, que les questions posées visent en particulier les articles 7 et 8 de la Charte, d'autre part, que cette juridiction expose que les directives 95/46 et 2002/58 constituent le lien de rattachement qui est nécessaire entre la réglementation nationale applicable au principal et le droit de l'Union [68] et, enfin, que la directive 2002/58 tend, comme l'énonce son considérant 2, à garantir, en particulier, le plein respect des droits énoncés aux articles 7 et 8 de la Charte [69].

64. J'ajoute qu'il est indifférent que l'un des éléments de la réglementation espagnole évoqués dans la décision de renvoi, à savoir la loi 25/2007, ait eu pour objet de transposer la directive 2006/24, laquelle a été abrogée à la suite de son invalidation par l'arrêt Digital Rights [70]. Comme la juridiction de renvoi l'indique à juste titre, il serait inexact de considérer que les questions préjudicielles ici soumises à la Cour se trouvent dénuées de pertinence en raison de ladite invalidation. À ce sujet, il suffit de constater que la matière concernée par ces questions, à savoir la protection des données à caractère personnel, relève du domaine de compétence de l'Union et que le litige au principal est couvert par le champ d'application d'un acte du droit de l'Union, à savoir la directive 2002/58 [71], que la directive 2006/24 invalidée avait vocation à modifier.

67 Voir, notamment, arrêts du 16 juin 2015, Gauweiler e.a. (C-62/14, EU:C:2015:400, points 24 et 25), ainsi que du 22 février 2018, Porras Guisado (C-103/16, EU:C:2018:99, point 34).

68 Voir aussi point 44 des présentes conclusions.

69 Voir, également, arrêt Tele2 (point 82).

70 Voir aussi point 10 des présentes conclusions. Je note que la situation était similaire dans l'une des affaires ayant donné lieu à l'arrêt Tele2 (voir points 15 et 63).

71 À ce dernier égard, voir points 45 et suiv. des présentes conclusions.

65. Il peut d'ailleurs être observé que les parties ayant soumis des observations à la Cour partent très majoritairement du principe que la présente demande de décision préjudicielle doit être examinée au regard de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, ainsi que sur la base des enseignements découlant des arrêts Digital Rights et Tele2. Tel est également mon avis, étant précisé que l'expression « infractions pénales », et non « infractions graves », figure dans la directive 2002/58, uniquement audit article 15, paragraphe 1 [72].

66. *En second lieu*, le gouvernement espagnol soutient que *l'article 7 de la Charte*, qui constituerait l'élément central de la présente demande de décision préjudicielle, *ne serait pas pertinent*, aux motifs que la mesure d'enquête sollicitée dans l'affaire au principal ne viserait pas l'interception de communications et ne pourrait donc pas affecter la confidentialité des communications, de sorte que les questions posées seraient hypothétiques.

67. Pour ma part, j'estime que l'article 7 de la Charte est bien pertinent dans la présente affaire et que la demande de décision préjudicielle est, dès lors, dénuée de caractère hypothétique. S'il est vrai que, en l'espèce, il n'existe pas de risque de violation du droit au secret des communications, eu égard à l'objet de la mesure en cause au principal [73], il n'en demeure pas moins qu'une mesure de ce type est susceptible de porter atteinte au droit au respect de la vie privée qui est garanti par ladite disposition, même si cette atteinte est selon moi de faible ampleur [74].

68. En effet, ainsi que la Cour l'a déjà jugé de façon constante, la communication de données à caractère personnel à un tiers, telle qu'une autorité publique, constitue une ingérence dans le droit fondamental consacré à l'article 7 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées. Il en va de même de la conservation des données à caractère personnel, notamment par les fournisseurs de services de communications électroniques, ainsi que de l'accès auxdites données en vue de leur utilisation par les autorités publiques [75].

69. Partant, je suis d'avis que l'exception d'irrecevabilité soulevée par le gouvernement espagnol doit être rejetée et qu'il convient donc de se prononcer sur le fond de la demande de décision préjudicielle.

72 Voir aussi point 71 des présentes conclusions.

73 Voir points 36 et 52 des présentes conclusions

74 Sur l'absence de gravité de l'ingérence causée en l'espèce, voir points 74 et suiv. des présentes conclusions.

75 Voir, notamment, arrêt Digital Rights (points 26 et suiv.) ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 124 et jurisprudence citée).

C. Sur les éléments requis pour devoir caractériser la gravité suffisante d'une infraction justifiant une ingérence dans les droits fondamentaux visés (première question)

70. Par sa première question, la juridiction de renvoi interroge la Cour, en substance, sur les éléments à prendre en compte afin d'établir que des infractions pénales sont d'une gravité suffisante pour justifier qu'il soit porté atteinte aux droits fondamentaux garantis par les articles 7 et 8 de la Charte, dans le cadre de la conservation de données à caractère personnel et de l'accès à celles-ci, conformément à la jurisprudence issue de l'arrêt Digital Rights, suivi de l'arrêt Tele2.

71. À ce sujet, je rappelle que la notion d'« infractions graves » a été employée par la Cour dans l'arrêt Digital Rights [76], parfois en combinaison avec la notion de « criminalité grave » [77], en tant que critère de vérification de la finalité et de la proportionnalité de l'ingérence dans les droits fondamentaux susmentionnés qui était entraînée par des dispositions du droit de l'Union relatives aux données à caractère personnel, à savoir celles de la directive 2006/24. Je précise que cette notion, qui ne figure pas dans la directive 2002/58 [78], était utilisée dans la directive 2006/24 [79], dont l'invalidité faisait l'objet dudit arrêt. La Cour a par la suite fait usage de ces deux notions dans l'arrêt Tele2 [80], en tant que même critère d'appréciation, mais concernant cette fois la conformité au droit de l'Union [81] de dispositions adoptées par des États membres.

72. Plus précisément, la première question préjudicielle invite la Cour à dire si, aux fins d'apprécier l'existence d'une « infraction grave » susceptible de justifier une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte exercée à l'égard de données à caractère personnel, il faut prendre en considération uniquement la peine encourue pour l'infraction litigieuse ou bien, au surplus, le caractère particulièrement préjudiciable du comportement délictueux à l'égard des intérêts juridiques individuels ou collectifs en jeu.

76 Voir points 24, 41, 49 et 57 à 61 de l'arrêt Digital Rights.

77 Voir points 41, 42 51 et 59 de l'arrêt Digital Rights.

78 Étant rappelé que seule l'expression « infractions pénales » figure dans la directive 2002/58, à son article 15, paragraphe 1, première phrase.

79 En substance, au considérant 9 de la directive 2006/24 ainsi que, littéralement, au considérant 21 et à l'article 1er, paragraphe 1, de celle-ci.

80 Voir, s'agissant de la notion d'« infractions graves », points 105, 106 et 119 ainsi que, s'agissant de la notion de « criminalité grave », points 102, 103, 108, 110, 111, 114, 115, 118, 125 et 134 de l'arrêt Tele2.

81 À savoir, l'article 15, paragraphe 1, de la directive 2002/58, en vertu duquel les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'elle est nécessaire, appropriée et proportionnée, au sein d'une société démocratique, au regard des objectifs que cette disposition énonce.

73. Toutefois, à l'instar de la Commission, j'estime que, avant de se prononcer sur cette question, il convient d'examiner si l'ingérence en cause dans un litige tel que celui au principal présente un degré de gravité suffisamment élevé pour qu'il soit exigé, en vertu du droit de l'Union, que cette ingérence soit justifiée par la lutte contre une infraction à caractère grave afin de pouvoir être admise. En effet, il m'apparaît que si tel n'est pas le cas, la Cour devrait procéder à une interprétation des dispositions pertinentes du droit de l'Union, non pas en s'en tenant à celle qui est sollicitée par la juridiction de renvoi, mais après avoir reformulé la première question posée [82] autant que nécessaire au regard des circonstances du litige au principal [83].

1. Sur la prise en compte de l'absence de gravité de l'ingérence litigieuse

74. *Tout d'abord*, il y a lieu d'établir que des opérations telles que celles en cause au principal sont bien susceptibles de porter atteinte aux droits fondamentaux garantis par les articles 7 et 8 de la Charte, et donc de *constituer une ingérence* dans ces droits, au sens de la jurisprudence issue des arrêts Digital Rights et Tele2.

75. Certes, comme les gouvernements espagnol et danois l'ont évoqué dans leur plaidoirie [84] et comme je l'ai déjà indiqué [85], les données auxquelles les autorités chargées de l'enquête pénale en cause souhaitent avoir accès semblent revêtir un caractère moins sensible que certaines autres catégories de données personnelles [86], sachant que la demande en cause apparaît porter sur les seuls prénom, nom et, éventuellement, adresse des individus ciblés par cette enquête, en tant qu'utilisateurs de numéros de téléphone activés depuis le téléphone mobile volé faisant l'objet de celle-ci.

82 Étant observé que la seconde question préjudicielle n'est soumise qu'à titre subsidiaire.

83 Il ressort d'une jurisprudence constante qu'afin de fournir une réponse utile à la juridiction de renvoi, qui lui permette de trancher le litige dont celle-ci est saisie, il incombe, le cas échéant, à la Cour de reformuler les questions qui lui sont soumises (voir, notamment, arrêt du 22 février 2018, SAKSA, C-185/17, EU:C:2018:108, point 28).

84 Le gouvernement espagnol a souligné que les données faisant l'objet du litige au principal ne permettent pas d'établir, par exemple, le profil de la personne concernée.

85 Voir points 35 à 37 des présentes conclusions.

86 Je rappelle que la directive 95/46 prévoit, à son article 8, des règles particulières pour le traitement des « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle ». Sur la notion de données à caractère sensible et leur traitement, voir *Manuel de droit européen en matière de protection des données*, élaboré sous l'égide de l'Agence des droits fondamentaux de l'Union européenne et du Conseil de l'Europe, 2014, version actualisée accessible à l'adresse Internet suivante : https://www.coe.int/fr/web/data-protection/home, p. 46 et suiv. ainsi que p. 94 et suiv.

76. Cependant, j'estime que pour déterminer si des données à caractère personnel doivent être couvertes par la protection prévue par le droit de l'Union, et en particulier par la directive 2002/58 [87], il est indifférent de savoir si les informations visées par la demande de conservation ou de communication sont d'une sensibilité particulière ou non. En effet, ainsi que cela a été relevé dans le cadre des premiers travaux législatifs en la matière, « selon la finalité de son utilisation toute donnée relative à une personne, même apparemment inoffensive, peut avoir un caractère sensible (comme une simple adresse postale par exemple) » [88]. De surcroît, la Cour a déjà jugé que, aux fins de caractériser *l'existence d'une ingérence* dans le droit fondamental consacré à l'article 7 de la Charte, « 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 » [89].

77. Par ailleurs, je rappelle que la communication de données à caractère personnel à un tiers, même une autorité publique telle qu'un service de police judiciaire, constitue une ingérence dans le droit fondamental garanti à l'article 7 de la Charte [90], y compris si ces informations sont transmises à des fins d'enquête pénale, situation d'ailleurs expressément visée à l'article 15, paragraphe 1, de la directive 2002/58 [91]. J'ajoute qu'une opération de ce type peut aussi porter atteinte au droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'elle induit un traitement de données à caractère personnel [92].

78. Dès lors, je considère qu'il y a lieu de constater qu'une mesure telle que celle en cause au principal est constitutive d'une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

79. *Cependant*, j'estime que, dans les circonstances de l'espèce, il manque un élément essentiel ayant été retenu par la Cour pour exiger, au stade de la

87 Le caractère sensible de certaines données est mentionné uniquement au considérant 25 de la directive 2002/58, sans qu'il puisse en être déduit qu'il s'agirait d'une exigence générale.

88 Voir communication de la Commission, du 13 septembre 1990, relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté et à la sécurité des systèmes d'information [COM(90) 314 final, p. 20].

89 Voir avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 124 et jurisprudence citée). La Cour EDH s'est aussi prononcée en ce sens (voir Cour EDH, 16 février 2000, Amann c. Suisse, CE:ECHR:2000:0216JUD002779895, §§ 68 à 70).

90 Voir point 68 des présentes conclusions. Voir, également, Cour EDH, 8 février 2018, Ben Faiza c. France (CE:ECHR:2018:0208JUD003144612, §§ 66 à 68), au sujet d'une réquisition judiciaire visant la communication d'informations relatives à l'usage fait d'un téléphone.

91 Dans les termes suivants : « assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ».

92 Voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 126 et jurisprudence citée).

justification d'une telle ingérence, qu'il existe une « infraction grave » – notion dont la définition est demandée par la juridiction de renvoi –, aux fins de pouvoir déroger au principe de confidentialité des communications électroniques. L'élément qui *fait défaut*, selon moi, en l'espèce, pour qu'il soit répondu à la première question préjudicielle dans les termes employés par cette juridiction est celui de *la gravité de l'ingérence litigieuse*, facteur qui, s'il était présent, induirait la nécessité d'une justification renforcée.

80. À cet égard, je relève que, dans l'arrêt Digital Rights, la Cour a mis en exergue la vaste ampleur et le caractère particulièrement grave de l'ingérence qui était produite par la réglementation en cause, en relevant notamment que « la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves » [93].

81. De façon similaire, dans l'arrêt Tele2, la Cour a dit pour droit que « [l]'article 15, paragraphe 1, de la directive 2002/58 [...] s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique » [94]. Un lien de corrélation a été fait également dans cet arrêt entre, d'une part, la particulière « gravité de l'ingérence » ainsi constatée et, d'autre part, la nécessité de justifier une atteinte d'une telle portée, envers les droits fondamentaux garantis par les articles 7 et 8 de la Charte, en se fondant sur un motif d'intérêt général aussi primordial que celui de la « lutte contre la criminalité grave » [95].

82. Cette mise en relation entre la gravité de l'ingérence constatée et la gravité du motif permettant de justifier celle-ci a été opérée en adéquation avec le principe de proportionnalité [96]. De surcroît, il m'apparaît que la Cour EDH a

93 Point 57 de l'arrêt Digital Rights. Sur la particulière gravité de l'ingérence en cause, voir aussi points 37, 39, 47, 48, 60 et 65 de cet arrêt.

94 Dispositif 1 de l'arrêt Tele2.

95 Aux termes du point 102 de l'arrêt Tele2, « *[e]u égard à la gravité de l'ingérence* dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, *la conservation* de données relatives au trafic et de données de localisation, *seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure* (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 60 [où figurait la formule « *au regard de l'ampleur et de la gravité de l'ingérence* »]) » (souligné par mes soins). Le point 115 de l'arrêt Tele2 reprend ce raisonnement s'agissant de *l'accès* à de telles données. Sur la particulière gravité de l'ingérence en cause, voir aussi points 97 et 100 de cet arrêt.

96 Ainsi, le point 115 de l'arrêt Tele2 met en exergue que « *dès lors que l'objectif poursuivi par [une réglementation nationale dérogeant au principe de confidentialité des communications électroniques] doit être en relation avec la gravité de l'ingérence* dans les droits fondamentaux qu'entraîne cet accès, il s'ensuit que, en matière de prévention, de recherche, de détection et de

établi, dans sa jurisprudence relative à l'article 8 de la CEDH [97], un lien de corrélation équivalant à celui qui ressort, à mon sens, des arrêts Digital Rights et Tele2.

83. Or, comme je l'ai évoqué ci-dessus [98] et comme l'ont souligné plus spécialement les gouvernements français et du Royaume-Uni ainsi que la Commission, la nature de l'ingérence en cause dans le présent litige au principal est, à plusieurs titres, distincte de celles ayant été envisagées par la Cour dans ces deux précédents arrêts. L'examen de la conformité au droit de l'Union d'une mesure telle que celle ici concernée doit, dès lors, être effectué de manière différente.

84. En l'espèce, il ne s'agit pas d'une mesure relative à une obligation de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation de n'importe quel abonné ou utilisateur inscrit qui concernerait tous les moyens de communication électronique. Il s'agit d'une mesure ciblée qui tend à une possibilité d'accès, par des autorités compétentes et pour les besoins d'une enquête pénale, à des données détenues à des fins commerciales par des prestataires de services et qui porte uniquement sur l'identité (nom, prénom et éventuellement adresse) d'une catégorie restreinte d'abonnés ou utilisateurs d'un moyen de communication spécifique, à savoir ceux dont le numéro de téléphone a été activé depuis le téléphone mobile dont le vol fait l'objet de l'enquête, et ce durant une période limitée, à savoir une douzaine de jours [99].

85. J'ajoute que les effets potentiellement nuisibles, pour les personnes visées par la demande d'accès en cause, sont à la fois modérés et encadrés. En effet, ayant vocation à être utilisées dans le cadre singulier d'une mesure d'investigation, les données demandées ne sont pas destinées à être divulguées au

poursuite d'infractions pénales, *seule la lutte contre la criminalité grave est susceptible de justifier un tel accès* aux données conservées » (souligné par mes soins).

97 En effet, cette juridiction a itérativement souligné la nécessité de *mettre en balance*, d'une part, l'intérêt d'un État à protéger sa *sécurité nationale* au moyen de mesures affectant des données personnelles et, d'autre part, la *gravité de l'atteinte* portée au droit d'un individu au respect de sa vie privée, deux facteurs dont dépendent la marge d'appréciation de l'État, en particulier lorsque ce dernier entend prévenir ou poursuivre des *infractions pénales graves* (voir Cour EDH, 26 mars 1987, Leander c. Suède, CE:ECHR:1987:0326JUD000924881, § 59 ; Cour EDH, 26 juin 2006, Weber et Saravia c. Allemagne, CE:ECHR:2006:0629DEC005493400, §§ 106, 125 et 126, ainsi que Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, §§ 232 et 244).

98 Voir points 32 et suiv. des présentes conclusions.

99 Je note que, dans l'avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, notamment points 194 et 207 à 209), la Cour a aussi évalué le caractère nécessaire des ingérences que comportait l'accord envisagé en examinant les modalités d'utilisation et de conservation des données qui y étaient prévues, spécialement, sous l'angle du contexte particulier de ces mesures, de leur spécification et de leur durée.

grand public [100]. De surcroît, la faculté d'accès offerte aux autorités policières est entourée de garanties procédurales en vertu du droit espagnol, puisqu'elle donne lieu à un contrôle juridictionnel, qui a d'ailleurs conduit à un rejet de la requête policière dans le litige au principal.

86. L'ingérence dans les droits fondamentaux susmentionnés qui est entraînée par la communication de ces données d'identité civile, à mes yeux, ne revêt pas un caractère de particulière gravité [101], dès lors que des données d'une telle nature et d'une portée si limitée ne permettent pas, à elles seules, d'obtenir des renseignements variés et/ou précis sur les personnes concernées [102] et n'affectent donc pas directement et fortement l'intimité de leur vie privée dans ces circonstances particulières [103].

87. *Partant*, à l'instar de la Commission, j'estime que, afin de fournir à la juridiction de renvoi les indications pertinentes pour trancher le litige dont celle-ci est saisie, il y a lieu de *reformuler* la première question préjudicielle de sorte que la réponse à venir de la Cour porte sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 au regard de circonstances telles que celles de l'espèce, à savoir en présence d'une ingérence dans les droits fondamentaux susmentionnés qui est dénuée d'une particulière gravité et fondée sur la lutte contre un type d'infractions pénales dont le caractère grave est mis en doute.

88. À cet égard, je rappelle que, dès lors que les objectifs susceptibles de justifier une réglementation nationale dérogeant au principe de confidentialité des communications électroniques sont énumérés de façon exhaustive à l'article 15, paragraphe 1, de la directive 2002/58, l'accès aux données conservées doit répondre effectivement et strictement à l'un desdits objectifs [104]. Parmi ces

100 Comme cela pourrait être le cas, par exemple, de l'identité de personnes qui serait publiée dans un article de presse ou sur un site Internet.

101 En ce sens, voir la convention sur la cybercriminalité conclue sous l'égide du Conseil de l'Europe, à Budapest le 23 novembre 2001, et signée par tous les États membres de l'Union (accessible à l'adresse Internet suivante : https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?_coeconventions_WAR_coeconventionsportlet_languageId=fr_FR), dont l'article 18 impose l'adoption de mesures législatives permettant aux autorités compétentes d'ordonner à un fournisseur de services de leur communiquer les données relatives aux abonnés, telles que « l'identité, l'adresse [...] et le numéro de téléphone », qui sont en sa possession.

102 Ainsi que le gouvernement danois l'a relevé à juste titre, lorsque la police obtient, comme en l'espèce, des renseignements sur le nom et l'adresse du propriétaire d'une carte SIM utilisée dans le cadre d'un délit, ce n'est pas fondamentalement différent, par exemple, de l'obtention d'informations concernant le propriétaire d'un véhicule utilisé pour commettre une infraction.

103 Contrairement aux informations particulièrement intrusives, notamment quant au traçage des communications et au profil des personnes concernées, qui étaient en jeu dans les affaires ayant donné lieu à l'arrêt Digital Rights (voir points 26 à 29 et 37) et à l'arrêt Tele2 (voir points 97 à 100).

104 Voir, notamment, points 90 et 115 de l'arrêt Tele2.

derniers, figure l'objectif d'intérêt général d'« assurer la prévention, la recherche, la détection et la poursuite d'*infractions pénales* » [105], sans autre précision quant à la nature de celles-ci.

89. Il ressort de la terminologie ainsi employée qu'il n'est pas impératif que les infractions légitimant la mesure restrictive en cause, en vertu dudit article 15, paragraphe 1, puissent être qualifiées de « graves » au sens de la jurisprudence issue des arrêts Digital Rights et Tele2. À mon avis, c'est uniquement lorsque l'ingérence subie est d'une particulière gravité, comme dans les affaires ayant donné lieu auxdits arrêts, que les infractions susceptibles de justifier une telle ingérence doivent elles-mêmes être d'une particulière gravité. En revanche, dans le cas d'une ingérence non grave, il y a lieu de revenir au principe de base résultant du libellé de cette disposition, à savoir que tout type d'« infractions pénales » est susceptible de justifier une telle ingérence.

90. Il convient, selon moi, de veiller à ne pas adopter une conception trop large des exigences posées par la Cour dans ces deux arrêts, afin de ne pas entraver, en tout cas pas excessivement, la possibilité des États membres de déroger au régime établi par la directive 2002/58, qui leur est octroyée par l'article 15, paragraphe 1, de celle-ci, dans les cas où les intrusions dans la vie privée en cause ont à la fois une finalité légitime et une portée réduite, telles que celles pouvant être entraînées en l'espèce par la requête du service de police judiciaire. Plus concrètement, je suis d'avis que le droit de l'Union ne s'oppose pas à ce que des autorités compétentes puissent avoir accès aux données d'identification, détenues par des fournisseurs de services de communications électroniques, qui permettent de retrouver les auteurs supposés d'une infraction pénale ne revêtant pas de caractère grave.

91. En conséquence, je recommande à la Cour de *répondre à la question préjudicielle, telle que reformulée,* que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'une mesure permettant aux autorités nationales compétentes d'avoir accès, à des fins de lutte contre des infractions pénales, aux données d'identification des utilisateurs de numéros de téléphone activés depuis un téléphone mobile spécifique et durant une période limitée, en des circonstances telles que celles en cause au principal, entraîne une ingérence, dans les droits fondamentaux garantis par ladite directive et par la Charte, qui n'atteint pas un niveau de gravité suffisant pour qu'il faille réserver un tel accès aux cas dans lesquels l'infraction concernée revêt un caractère grave.

92. Eu égard à la réponse ainsi proposée, l'ensemble des observations qui suivent seront présentées seulement à titre *subsidiaire,* dans le but d'être complet.

105 Souligné par mes soins.

2. Sur la détermination éventuelle des critères pertinents pour caractériser la gravité suffisante d'une infraction

93. Au cas où la Cour jugerait, contrairement à ce que je préconise, qu'il y a lieu, nonobstant les circonstances bien particulières du présent litige au principal, de déterminer, dans la présente affaire, ce qu'il faut entendre par une « infraction grave » au sens de la jurisprudence issue des arrêts Digital Rights et Tele2 [106], il conviendrait encore de s'interroger, *en premier lieu*, sur le point de savoir si cette qualification constitue bien une *notion autonome* du droit de l'Union, qu'il appartiendrait donc à la Cour de définir. Or, à l'instar de la réponse proposée à titre principal par le gouvernement français, telle n'est pas ma conviction, pour les motifs qui suivent.

94. Tout d'abord, j'observe que la directive 2006/24, d'où l'usage de la notion d'« infraction grave » provient [107], ne contenait pas de définition de celle-ci, mais renvoyait à ce sujet aux ordres juridiques des États membres [108]. J'ajoute que les considérations pertinentes qui figurent dans les arrêts Digital Rights et Tele2 ne doivent pas être comprises, selon moi, comme tendant à harmoniser les règles de droit en vigueur dans les États membres qui concernent la teneur de cette notion.

95. À cet égard, je rappelle que la législation pénale et les règles de la procédure pénale relèvent de la compétence des États membres, même si l'ordre juridique de ces derniers peut néanmoins être affecté par les dispositions du droit de l'Union adoptées en ce domaine [109]. Aux termes de l'article 83, paragraphe 2, TFUE, c'est seulement dans les cas où l'harmonisation du droit pénal des États membres s'avère indispensable pour la mise en œuvre efficace d'une politique de l'Union, dans un domaine ayant fait l'objet de mesures d'harmonisation, que l'Union peut adopter des directives visant à établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine concerné. Or, en l'état actuel du droit de l'Union, il n'existe pas de disposition à portée générale qui donnerait une définition harmonisée de la notion d'« infraction grave » [110].

106 À savoir dans l'hypothèse où la Cour considérerait soit que l'ingérence en cause au principal est suffisamment grave pour qu'il soit répondu à la première question telle que posée par la juridiction de renvoi, soit qu'il est indifférent à cet égard que ladite ingérence ne soit pas grave.

107 Voir point 71 des présentes conclusions.

108 L'article 1er, paragraphe 1, de la directive 2006/24 énonçait que celle-ci avait « pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques [...], en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite *d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* » (souligné par mes soins). Voir aussi considérant 21 de cette directive.

109 Voir, notamment, arrêts du 15 septembre 2011, Dickinger et Ömer (C-347/09, EU:C:2011:582, point 31), ainsi que du 6 décembre 2011, Achughbabian (C-329/11, EU:C:2011:807, point 33).

110 À ce sujet, voir aussi point 112 des présentes conclusions.

96. Il m'apparaît que le pouvoir de déterminer ce qui constitue une « infraction pénale grave » appartient, en principe, aux autorités compétentes des États membres. Néanmoins, grâce aux renvois préjudiciels dont les juridictions des États membres peuvent la saisir, la Cour est chargée de veiller au respect de toutes les exigences résultant du droit de l'Union, et notamment d'assurer une application cohérente de la protection offerte par les dispositions de la Charte.

97. Je relève que la qualification juridique en question est susceptible non seulement de varier d'un État membre à un autre, en fonction des traditions suivies et des priorités définies par chacun d'entre eux, mais également de fluctuer dans le temps, en fonction des orientations qui sont données à la politique pénale, vers plus ou bien moins de sévérité, pour tenir compte de l'évolution de la criminalité [111] ainsi que, plus généralement, des transformations de la société et des besoins existant, notamment en termes de répression pénale, au plan national.

98. En outre, je souligne que, sachant qu'il existe de grandes différences entre les barèmes de sanctions qui sont traditionnellement applicables dans les divers États membres [112], la gravité d'une infraction ne tient pas seulement à l'importance de la peine y afférente. Le point de savoir si une infraction revêt un caractère grave est très relatif, en ce sens qu'il dépend de l'échelle des sanctions qui sont en général appliquées dans l'État membre concerné. Ainsi, le fait qu'un État membre prévoie une peine d'emprisonnement peu élevée, voire une peine alternative à l'emprisonnement, ne préjuge pas pour autant de la gravité intrinsèque du type d'infraction concerné [113].

99. Il y a lieu, selon moi, de respecter les spécificités du système de droit pénal de chacun des États membres, pour autant que le droit de l'Union ne fixe pas des obligations liant ces derniers de façon stricte, par analogie avec ce que la Cour a jugé s'agissant de la sauvegarde de la sécurité publique [114], notion voisine à mes

111 Sur le caractère dynamique de la criminalité grave, voir, également, mes conclusions dans les affaires jointes Tele2 Sverige e.a. (C-203/15 et C-698/15, EU:C:2016:572, point 214).

112 À titre d'illustration, en matière de lutte contre la criminalité organisée, un rapport de la Commission daté du 7 juillet 2016 indique que les peines prévues par les États membres varient entre eux notablement (de trois mois à 17 ans d'emprisonnement) pour l'infraction grave que constitue la participation à une organisation criminelle [voir rapport au Parlement européen et au Conseil fondé sur l'article 10 de la décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée, COM(2016) 448 final, p. 7, point 2.1.4.1].

113 Comme le gouvernement danois l'a indiqué, des sanctions moins lourdes, par rapport à d'autres États membres, sont appliquées au Danemark, sans que cela signifie que l'infraction est considérée comme dénuée d'une particulière gravité. Par exemple, la sanction prévue pour possession de matériel pédopornographique est d'un an de prison, tandis qu'elle pourrait aller jusqu'à dix ans de prison, pour les mêmes faits, dans d'autres États membres, mais cela ne remet pas en cause le constat que cette infraction est particulièrement grave par nature.

114 Voir, notamment, l'arrêt du 22 mai 2012, I (C-348/09, EU:C:2012:300, points 21 à 23), aux termes duquel « le droit de l'Union n'impose pas aux États membres une échelle uniforme de valeurs en ce qui concerne l'appréciation des comportements pouvant être considérés comme contraires à la sécurité publique » et « les États membres restent libres de déterminer, conformément à leurs besoins nationaux pouvant varier d'un État membre à l'autre et d'une

yeux de la notion de lutte contre la criminalité grave, notamment eu égard au libellé de l'article 15, paragraphe 1, première phrase, de la directive 2002/58.

100. En conséquence, je suis d'avis, à titre subsidiaire, que la notion d'« infraction grave » au sens de la jurisprudence de la Cour issue des arrêts Digital Rights et Tele2 ne constitue pas une notion autonome du droit de l'Union dont la teneur devrait être définie par la Cour, même s'il n'en demeure pas moins que la dérogation prévue à l'article 15, paragraphe 1, de la directive 2002/58 doit être mise en œuvre par les États membres conformément aux obligations découlant du droit de l'Union, notamment des droits fondamentaux garantis par la Charte, et ce, sous le contrôle de la Cour.

101. À ce dernier sujet, je relève qu'il ressort de la jurisprudence de la Cour, en particulier, que ledit article 15, paragraphe 1, en ce qu'il permet aux États membres de limiter la portée de certains droits et obligations prévus par cette directive, doit faire l'objet d'une interprétation stricte et ne saurait donc conduire à ce que la dérogation à ces droits et obligations de principe devienne la règle [115]. Partant, la portée de ladite notion d'« infraction grave » ne saurait être entendue de façon excessivement large par les États membres.

102. *En second lieu*, et à titre infiniment subsidiaire, *dans l'hypothèse où la Cour considérerait que ladite notion est autonome*, elle devrait alors répondre à la question telle que formulée par la juridiction de renvoi et, partant, se prononcer sur la détermination des critères permettant d'apprécier, au niveau du droit de l'Union, si une infraction pénale revêt un caractère de gravité suffisant pour justifier une atteinte aux droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

103. Plus précisément, la Cour devrait déterminer si, pour établir l'existence d'une « infraction grave » au sens de ladite jurisprudence, il est suffisant de se fonder sur la peine prévue pour l'infraction alléguée ou s'il faut, en outre, que le comportement délictueux ait été particulièrement préjudiciable pour les intérêts juridiques individuels ou collectifs en jeu. À cet égard, il conviendrait selon moi, de même que selon les gouvernements danois, espagnol, français, hongrois, autrichien, polonais et du Royaume-Uni, d'opter non pas pour la première branche de cette alternative, mais pour sa seconde branche en substance, en privilégiant une définition basée sur une *pluralité de critères d'appréciation* [116].

époque à l'autre, les exigences de l'ordre public et de la sécurité publique, notamment en tant que justification d'une dérogation au principe fondamental de la libre circulation des personnes », mais « ces exigences doivent, toutefois, être entendues strictement, de sorte que leur portée ne saurait être déterminée unilatéralement par chacun des États membres sans contrôle des institutions de l'Union européenne ».

115 Voir, en ce sens, points 89 et suiv. de l'arrêt Tele2, au sujet de l'obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes.

116 Je précise que les gouvernements tchèque et estonien proposent de répondre, en substance, qu'il est possible de déterminer la gravité suffisante des infractions, en tant que critère justifiant

104. S'agissant de la gravité de l'infraction susceptible de justifier l'accès aux données, il serait à mon avis, eu égard au principe de proportionnalité, impossible de déterminer la gravité des faits incriminés en prenant en compte seulement la peine susceptible d'être infligée. En effet, étant donné les différences notables qui existent encore entre les systèmes répressifs des États membres, j'estime que la sanction encourue ne saurait être considérée comme pouvant refléter à elle seule, que ce soit sous l'angle qualitatif du type de peine et/ou sous l'angle quantitatif du niveau de peine, la particulière gravité d'une infraction pénale.

105. Même si la peine revêt une importance considérable, d'autres facteurs objectifs doivent tout autant entrer en ligne de compte, au cas par cas, à ce titre. Il s'agit plus spécialement, d'une part, du contexte dans lequel s'inscrit l'infraction alléguée – en ce que le comportement délictueux revêt un caractère intentionnel, est entouré de circonstances aggravantes et/ou a été commis en état de récidive légale –, d'autre part, de l'importance des intérêts de la société ayant pu être méconnus par l'auteur de l'infraction ainsi que de la nature et/ou de l'ampleur des préjudices ayant pu être subis par la victime de cette dernière [117], et, enfin, de l'échelle des peines applicables en général dans l'État membre concerné [118]. C'est à partir de ce faisceau de critères d'appréciation, alternatifs et non exhaustifs, qu'il y aurait lieu, à mon avis, de qualifier éventuellement une infraction pénale de « grave » au sens de la jurisprudence de la Cour en question.

106. J'ajoute que l'interprétation ainsi proposée est conforme à l'approche qui m'apparaît avoir été adoptée par la Cour EDH dans sa jurisprudence relative à la « prévention des infractions pénales », en tant qu'objectif qui permet de justifier une ingérence dans le droit à la vie privée consacré à l'article 8 de la CEDH sous réserve que d'autres conditions soient aussi remplies [119]. Il ressort, à mes yeux, de cette jurisprudence que la lutte contre certaines catégories d'infractions peut

l'atteinte aux droits fondamentaux reconnus aux articles 7 et 8 de la Charte, en se fondant uniquement sur la peine encourue, mais que ces gouvernements estiment, toutefois, que chaque État membre devrait être libre de retenir aussi d'autres critères objectifs reflétant la spécificité de son ordre juridique, s'il l'estime nécessaire.

117 Je partage le point de vue du gouvernement français selon lequel il va de soi que les atteintes portées aux intérêts fondamentaux de la nation, aux institutions ou à l'intégrité du territoire national relèvent, par nature, du domaine de la « criminalité grave », mais que d'autres types d'infractions devraient aussi en relever, telles que les atteintes portées à la vie, à l'intégrité physique ou psychique et à la dignité des personnes, de même que les atteintes aux biens entraînant un préjudice patrimonial important pour la victime, ou encore celles s'inscrivant dans un phénomène sériel qui portent une atteinte répétée à l'ordre public. Sur ce dernier point, le gouvernement hongrois évoque aussi la possibilité de prendre en compte une multiplication exceptionnelle de certaines infractions dans la criminalité au niveau national.

118 À ce dernier égard, voir aussi point 98 des présentes conclusions.

119 Conformément au paragraphe 2 de l'article 8 de la CEDH, une telle ingérence ne peut être justifiée que si elle est prévue par loi, vise un ou plusieurs des buts légitimes énumérés à ce paragraphe et est nécessaire, dans une société démocratique, pour atteindre ce ou ces but(s).

valablement être invoquée dans ce cadre, par les États parties à la CEDH [120], au regard non pas tant seulement de la peine encourue, mais plutôt de divers facteurs d'évaluation, parmi lesquels figurent, en bonne place, la nature des infractions en cause ainsi que les intérêts publics et privés mis en présence par celles-ci [121].

107. Par conséquent, je suis d'avis que si la notion d'« infraction grave » au sens de la jurisprudence issue des arrêts Digital Rights et Tele2 était considérée par la Cour comme constituant une notion autonome du droit de l'Union, elle devrait être interprétée en ce sens que le caractère grave d'une infraction, susceptible de justifier l'accès des autorités nationales compétentes à des données personnelles en vertu de l'article 15, paragraphe 1, de la directive 2002/58, doit être mesuré non pas en tenant compte uniquement de la peine susceptible d'être infligée, mais en tenant compte au surplus d'un ensemble d'autres critères objectifs d'appréciation, tels que ceux ci-dessus mentionnés.

D. Sur la définition subsidiaire du niveau minimal de peine requis pour caractériser la gravité suffisante d'une infraction justifiant une ingérence dans les droits fondamentaux visés (seconde question)

108. Par sa seconde question, la juridiction de renvoi, en substance, invite la Cour, d'une part, à identifier le niveau minimal que la peine encourue devrait atteindre pour qu'une infraction pénale puisse être qualifiée de « grave », au sens de la jurisprudence issue des arrêts Digital Rights et Tele2, ainsi que, d'autre part, à dire si un seuil de trois ans d'emprisonnement, tel que prévu dans le code de procédure pénale espagnol depuis la réforme intervenue en 2015 [122], est conforme aux exigences du droit de l'Union.

109. Ces interrogations sont soumises seulement à titre subsidiaire, dans l'hypothèse où la Cour jugerait, en réponse à la première question préjudicielle, que le caractère grave d'une infraction pénale, facteur pouvant justifier une ingérence dans des droits fondamentaux en vertu de ladite jurisprudence, doit être déterminé en tenant compte uniquement du quantum de la peine privative de liberté qui est susceptible d'être infligée.

110. Eu égard à la réponse que je propose d'apporter à la première question préjudicielle, il n'y aura selon moi pas lieu pour la Cour de statuer sur la seconde

120 La Cour EDH a jugé que les infractions pertinentes doivent pouvoir être identifiées facilement par les citoyens, sans que cette exigence de prévisibilité requière que les États énumèrent de manière exhaustive celles qui peuvent déboucher sur une telle mesure (voir, notamment, Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, § 244).

121 Voir, notamment, Cour EDH, 26 juin 2006, Weber et Saravia c. Allemagne (CE:ECHR:2006:0629DEC005493400, §§ 106 et 115) ; Cour EDH, 4 décembre 2008, Marper c. Royaume-Uni (CE:ECHR:2008:1204JUD003056204, §§ 104 et 119), ainsi que Cour EDH, 30 mai 2017, Trabajo Rueda c. Espagne (CE:ECHR:2017:0530JUD003260012, §§ 39 et 40).

122 Voir points 15 et suiv. des présentes conclusions.

question. Néanmoins, j'entends présenter des observations à ce sujet, par souci d'exhaustivité.

111. S'agissant de la *première partie de la seconde question*, j'estime, à l'instar notamment des gouvernements tchèque et estonien, que le *niveau de peine encourue* qui permettrait à lui seul de qualifier une infraction de « grave » ne saurait être déterminé de façon uniforme pour l'ensemble du territoire de l'Union, eu égard aux considérations ci-dessus indiquées en réponse à la première question posée par la juridiction de renvoi [123].

112. D'ailleurs, cette variation dans la définition de ce qu'il faut entendre par une « infraction grave », et plus particulièrement quant au seuil de la peine à partir duquel cette qualification serait acquise, est également présente dans les actes du droit de l'Union. En effet, il peut être constaté que des actes de l'Union adoptés sur le fondement de l'article 83, paragraphe 1, TFUE prévoient des peines d'emprisonnement établies à des niveaux différents pour des infractions pourtant toutes considérées comme relevant d'une « criminalité particulièrement grave » [124], comme cela ressort, à titre d'illustration, de l'article 3 de la directive 2011/92/UE [125] et de l'article 15 de la directive (UE) 2017/541 [126], instruments relatifs, respectivement, à la lutte contre les abus sexuels commis sur des enfants et à la lutte contre le terrorisme. Ainsi, le législateur de l'Union lui-même n'a pas opté pour une définition uniforme de la notion d'« infraction grave » au regard d'un quantum déterminé de peine encourue.

113. Je rappelle que la liberté laissée aux États membres de décider du niveau minimal de peine requis pour que des infractions pénales soient dites « graves » est encadrée par les normes figurant dans les dispositions du droit de l'Union en la matière, mais aussi par le principe en vertu duquel une exception ne peut se voir conférer une ampleur si vaste qu'elle deviendrait de fait la règle générale [127].

123 Voir points 93 et suiv. des présentes conclusions.

124 Étant rappelé que l'article 83, paragraphe 1, TFUE permet l'adoption de « règles minimales relatives à la définition des infractions pénales et des sanctions dans des domaines de criminalité particulièrement grave revêtant une dimension transfrontière », énumérés à cette disposition.

125 Directive du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO 2011, L 335, p. 1), dont l'article 3 prévoit des peines s'échelonnant d'au moins un an jusqu'à au moins dix ans d'emprisonnement pour les divers types d'« infractions liées aux abus sexuels » visés à cet article.

126 Directive du Parlement européen et du Conseil, du 15 mars 2017, relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO 2017, L 88, p. 6), dont l'article 15, paragraphe 3, prévoit des peines privatives de liberté ne pouvant être inférieures à huit ou à quinze ans selon les divers types d'« infractions liées à un groupe terroriste » visés à l'article 4 de cette même directive.

127 Voir aussi point 101 des présentes conclusions.

114. En l'occurrence, même si chaque État membre a la faculté d'apprécier quel est le seuil de peine adéquat pour caractériser une infraction grave, il a cependant le devoir de ne pas fixer celui-ci à un échelon tellement bas, au regard du niveau habituel des peines applicables dans cet État [128], que les exceptions à l'interdiction de stocker et d'exploiter les données à caractère personnel qui sont prévues à cet article 15, paragraphe 1, seraient muées en principes, ainsi que le gouvernement irlandais l'a noté à juste titre.

115. De surcroît, il est constant que les ingérences dans les droits garantis par les articles 7 et 8 de la Charte, qui pourraient être autorisées par les États membres en vertu de l'article 15, paragraphe 1, de la directive 2002/58, restent, de surcroît, toujours subordonnées au respect des exigences générales découlant du principe de proportionnalité, tel qu'énoncé à l'article 52, paragraphe 1, de la Charte [129].

116. S'agissant de la *dernière partie de la seconde question*, le gouvernement estonien et la Commission indiquent, d'une part, qu'un seuil fondé exclusivement sur une peine d'au moins *trois ans d'emprisonnement* apparaît, dans l'absolu, être suffisant pour qualifier une infraction de « grave », au sens de la jurisprudence de la Cour relative à l'accès aux données personnelles issue de l'arrêt Digital Rights, et, d'autre part, qu'un tel seuil n'est pas manifestement incompatible avec le droit de l'Union en général [130], et plus particulièrement avec l'article 15, paragraphe 1, de la directive 2002/58.

117. Cependant, il serait, à mon avis, souhaitable que la Cour s'abstienne de prendre position en faveur d'un quantum précis de peine encourue, car ce qui est adapté pour certains États membres ne le sera pas forcément pour d'autres et ce qui vaut à ce jour pour un type d'infractions ne vaudra pas nécessairement de façon irrévocable à l'avenir, ainsi que l'ai déjà mentionné [131]. Dès lors qu'une détermination du seuil en question requiert une évaluation complexe et potentiellement évolutive, il convient selon moi de rester prudent à ce sujet et de réserver cette opération à l'appréciation du législateur de l'Union, dans la sphère des compétences conférées à celle-ci, ou à l'appréciation du législateur de chaque État membre, dans les limites des exigences résultant du droit de l'Union.

128 À ce sujet, voir point 98 des présentes conclusions.

129 Voir, notamment, considérant 11 et article 15, paragraphe 1, de la directive 2002/58, ainsi que points 94 à 96 et 116 de l'arrêt Tele2.

130 Voir, notamment, outre les dispositions visées aux notes en bas de page 125 et 126 des présentes conclusions, la directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JO 2016, L 119, p. 132), dont l'article 3, point 9, définit les « formes graves de criminalité » comme renvoyant aux « infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre ».

131 Voir point 97 des présentes conclusions.

118. À ce dernier égard, je relève que, en l'espèce, la juridiction de renvoi fait état d'un risque d'inversion entre la règle générale et les dérogations prévues par la directive 2002/58, risque évoqué ci-dessus [132], lorsqu'elle indique que « le seuil de trois ans de prison [introduit en 2015 par le législateur espagnol [133]] concerne une grande majorité des qualifications pénales ». Autrement dit, d'après cette juridiction, la liste actuelle des infractions susceptibles de justifier, en Espagne, des restrictions aux droits protégés en vertu des articles 7 et 8 de la Charte, qui a été instaurée par la réforme du code de procédure pénale, conduirait, en pratique, à ce que la majeure partie des infractions prévues au code pénal soient incluses dans ladite liste.

119. Or, à supposer que l'ingérence en cause au principal soit considérée comme grave par la Cour et à supposer que le résultat ainsi évoqué par la juridiction de renvoi soit avéré, ce dernier serait à mes yeux non conforme à l'obligation de proportionnalité à laquelle de telles restrictions sont soumises [134]. Il en va ainsi, selon moi, nonobstant l'existence d'un contrôle juridictionnel, invoquée par le gouvernement espagnol, puisque l'exercice de ce contrôle permet seulement d'empêcher la mise en œuvre de mesures jugées, au cas par cas, arbitraires ou trop intrusives, et non de freiner, d'une façon généralisée, le recours à des mesures de ce type et leur développement.

120. Enfin, je souligne que l'approche proposée dans l'ensemble de la présente section concorde, à mon sens, avec celle retenue par la Cour EDH dans sa jurisprudence relative à la protection des données personnelles. Certes, comme l'évoquent le gouvernement irlandais et la Commission, cette juridiction a jugé suffisamment claires des législations nationales qui définissaient les infractions « graves », susceptibles de justifier une ingérence dans la vie privée, en se référant à une peine encourue égale ou supérieure à trois ans d'emprisonnement [135]. Néanmoins, je considère qu'elle n'a pas érigé ledit quantum de peine en critère absolu et figé aux fins de cette définition, sachant que sa jurisprudence m'apparaît centrée sur l'exigence d'une prévisibilité et d'une clarté suffisantes pour les citoyens au regard non pas tant de la peine encourue, mais plutôt de la nature des infractions permettant une telle ingérence [136]. Par ailleurs, si la Cour EDH reconnaît aux États une certaine latitude pour apprécier l'existence et l'étendue de la nécessité d'une telle ingérence, elle soumet toutefois cette marge d'appréciation

132 Voir point 101 des présentes conclusions.

133 Réforme mentionnée aux points 15 et suiv. des présentes conclusions.

134 Voir aussi point 115 des présentes conclusions.

135 Voir, en ce sens, Cour EDH, 18 mai 2010, Kennedy c. Royaume-Uni (CE:ECHR:2010:0518JUD002683905, §§ 34 et 159), ainsi que Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie (CE:ECHR:2015:1204JUD004714306, § 244).

136 Voir point 106 des présentes conclusions.

à un contrôle au niveau européen [137]. En particulier, elle veille à prévenir les risques d'abus induits par des législations renvoyant à un éventail d'infractions tellement large qu'elles aboutissent à ce que la plupart des infractions permettent de justifier des mesures intrusives [138].

121. En conclusion, j'estime que, dans l'hypothèse où la Cour jugerait – contrairement à ce que je préconise – qu'il y a lieu de tenir compte uniquement de la peine encourue pour qualifier une infraction pénale de « grave » au sens de sa jurisprudence issue de l'arrêt Digital Rights, il conviendrait alors de répondre à la seconde question préjudicielle que les États membres sont libres de fixer le niveau minimal de la peine pertinente à cette fin, pour autant qu'ils se conforment aux exigences résultant du droit de l'Union, et en particulier celles selon lesquelles les ingérences dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte doivent rester exceptionnelles et respecter le principe de proportionnalité.

V. Conclusion

122. Au vu des considérations qui précèdent, je propose à la Cour de répondre aux questions préjudicielles posées par l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone, Espagne) de la manière suivante :

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 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'une mesure permettant aux autorités nationales compétentes d'avoir accès, à des fins de lutte contre des infractions pénales, aux données d'identification des utilisateurs des numéros de téléphone activés depuis un téléphone mobile spécifique et durant une période limitée, dans des circonstances telles que celles en cause au principal, entraîne une ingérence, dans les droits fondamentaux garantis par ladite directive et par la Charte, qui n'atteint pas un niveau de gravité suffisant pour qu'il faille réserver un tel accès aux cas dans lesquels l'infraction concernée revêt un caractère grave.

137 Voir, notamment, Cour EDH, 6 septembre 1978, Klass et autres c. Allemagne (CE:ECHR:1978:0906JUD000502971, § 49), ainsi que Cour EDH, 18 mai 2010, Kennedy c. Royaume-Uni (CE:ECHR:2010:0518JUD002683905, §§ 153 et 154).

138 Voir Cour EDH, 10 février 2009, Iordachi et autres c. Moldova (CE:ECHR:2009:0210JUD002519802, § 44), où la législation moldave a été considérée comme manquant de clarté, notamment, au motif que plus de la moitié des infractions prévues par le code pénal entraient dans la catégorie des infractions susceptibles de donner lieu à une mesure d'interception des communications téléphoniques. Voir, également, Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie (CE:ECHR:2015:1204JUD004714306, § 248).