Affaire C-140/20

Demande de décision préjudicielle

Date de dépôt :

25 mars 2020

Juridiction de renvoi :

Supreme Court (Irlande)

Date de la décision de renvoi :

25 mars 2020

Partie requérante :

G.D.

Parties défenderesses :

The Commissioner of the Garda Síochána

Minister for Communications, Energy and Natural Resources

Attorney General

SUPREME COURT

[omissis]

G.D.

Partie requérante/intimée

contre

Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Ireland and Attorney General (le commissaire d'An Garda Síochána, le ministre des Communications, de l'Énergie et des Ressources naturelles et l'Irlande, représentée par l'Attorney General)

Parties défenderesses/appelantes

Décision de renvoi par laquelle la Supreme Court (Cour suprême, Irlande) saisit la Cour de justice de l'Union européenne, conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne, de certaines questions relatives à l'interprétation du droit de l'Union

[Or. 2]

1. Introduction

1.1 La présente affaire concerne le régime mis en place par le Communications (Retention of Data) Act 2011 [loi de 2011 sur les communications (conservation des données)] (ci-après la « loi de 2011 ») qui régit la conservation et l'accès aux métadonnées des télécommunications par les autorités nationales en Irlande et, en particulier, par la police irlandaise [An Garda Síochána] dans le cadre de la détection et de la poursuite d'infractions graves ainsi que des enquêtes en la matière.

1.2. En mars 2015, le requérant (ci-après « M. D. ») a été déclaré coupable, par un jury, du meurtre de M^me^ O'H., pour lequel il a été condamné à la réclusion à perpétuité. Il a toujours nié sa culpabilité. Cette condamnation fait l'objet d'un appel de M. D., qui est pendant devant la Court of Appeal (Cour d'appel, Irlande). Au cours du procès, M. D. a contesté, sans succès, l'admissibilité de certains éléments de preuve à charge reposant sur des données de téléphonie conservées. M. D. a engagé la procédure civile parallèle dont nous sommes saisis, qui a donné lieu à la présente demande de décision préjudicielle, afin de contester certaines dispositions de la loi de 2011 en vertu desquelles de telles métadonnées de téléphonie avaient été conservées et consultées. Cette procédure a pour objectif de faire constater l'invalidité de la disposition législative pertinente, afin qu'il puisse être soutenu, lors de l'appel dirigé contre la condamnation de M. D., que les éléments de preuve constitués par les données de téléphonie n'auraient pas dû être admis dans le cadre de son procès, ce qui remettrait en cause les fondements de sa condamnation. Les défendeurs (ci-après l'« État ») concluent à ce que la validité des dispositions législatives soit confirmée.

1.3. La présente demande de décision préjudicielle s'inscrit dans le cadre d'un appel interjeté par l'État devant la Supreme Court (Cour suprême) contre la décision de la High Court (Haute Cour, Irlande). Par décision du 6 décembre 2018 (Dwyer v. Commissioner of An Garda Síochána & Others [2018] IEHC 685), la High Court (Haute Cour, composée du juge O'Connor) avait constaté, conformément aux conclusions de M. D., que l'article 6, paragraphe 1, sous a), de la loi de 2011 était incompatible avec l'article 15, paragraphe 1, de la directive 2002/58/CE, **[Or. 3]** [omissis] lu à la lumière des articles 7, 8 et 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

1.4. Par la présente demande de décision préjudicielle, la Supreme Court (Cour suprême) souhaite être éclairée sur les exigences du droit de l'Union en ce qui

concerne la conservation des données à des fins de lutte contre la criminalité grave ainsi que sur les garanties nécessaires qui doivent encadrer l'accès à ces données, compte tenu de la compétence des États membres en matière pénale. La juridiction de céans souhaite également être éclairée sur la portée et les effets dans le temps de la décision déclaratoire qui pourrait, le cas échéant, être rendue dans les circonstances de l'espèce.

2. Le droit de l'Union

2.1 Les dispositions qui sous-tendent le présent renvoi sont celles du traité sur l'Union européenne et, en particulier, l'article 5, paragraphe 4, relatif au principe de proportionnalité, et l'article 6, paragraphe 1, reconnaissant les droits et libertés énoncés dans la Charte. En outre, la juridiction de céans considère que les dispositions du protocole (nº 21) sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité, peuvent présenter une certaine pertinence dans le cadre de la présente procédure.

2.2 Les directives de l'Union, adoptées en ce qui concerne le traitement des données à caractère personnel, qui sont pertinentes aux fins du présent renvoi sont la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après la « directive de 1995 »), 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 (ci-après la « directive de 2002 ») et 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 **[Or. 4]** de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (ci-après la « directive de 2006 »), cette dernière ayant ensuite été déclarée invalide par la Cour en 2014, comme nous le verrons ci-dessous.

2.3 Sont également au cœur de la présente affaire les droits et libertés reconnus par la Charte, et notamment les articles 7, 8 et 52, paragraphe 1, de celle-ci.

3. Le régime législatif irlandais

3.1 La loi de 2011 a été adoptée dans le but déclaré de mettre en œuvre la directive de 2006 et ses dispositions sont exposées en détail à l'annexe I de la présente demande. Les dispositions pertinentes en l'espèce de l'article 3 de la loi imposent à tous les fournisseurs de services de conserver les « données relatives à la téléphonie fixe en réseau et à la téléphonie mobile » pendant deux ans. Il s'agit des données qui permettent d'identifier la source et la destination d'une communication, de déterminer la date et l'heure du début et de la fin d'une communication, de déterminer le type de communication concerné, ainsi que

d'identifier le type et la localisation géographique du matériel de communication utilisé. Le contenu des communications ne relève pas de ce type de données.

3.2 Ces données peuvent être consultées et divulguées sur présentation d'une demande de divulgation. L'article 6 de la loi de 2011 prévoit les conditions dans lesquelles une demande de divulgation peut être introduite et le paragraphe 1 de cet article dispose qu'un fonctionnaire de la police nationale dont le rang n'est pas inférieur à celui de « chief superintendent » (commissaire divisionnaire) peut introduire une demande de divulgation si ce fonctionnaire estime que les données en question sont nécessaires aux fins, notamment, de la prévention, de la détection, de la recherche ou de la poursuite d'une infraction grave. Une « infraction grave » est définie comme étant une infraction passible d'une peine d'emprisonnement d'une durée égale ou supérieure à 5 ans ou l'une des autres infractions énumérées à l'annexe 1 de la loi. **[Or. 5]**

3.3 Parmi les mécanismes de contrôle prévus par la loi de 2011 figurent la procédure de réclamation établie à l'article 10 et les fonctions du « designated judge » (juge désigné), au sens de l'article 12, qui est chargé d'analyser l'application des dispositions de la loi.

3.4 Il ressort des éléments produits devant la High Court (Haute Cour) dans la présente procédure civile que, à titre de mesure interne, le chef de la police nationale, le « Garda Commissioner », a décidé que les demandes de divulgation de données de téléphonie introduites en vertu de la loi de 2011 devaient faire l'objet d'un traitement centralisé, par un seul commissaire divisionnaire. En matière de divulgation des données, le commissaire divisionnaire responsable est le chef de la section de la sécurité et du renseignement d'An Garda Síochána et c'est lui qui décide, en dernier ressort, d'adresser ou non une demande de divulgation aux fournisseurs de services de communications conformément aux dispositions de la loi de 2011. Une petite unité indépendante appelée la « Telecommunications Liaison Unit » (unité de liaison en matière de télécommunications, ci-après la « TLU ») a été créée afin de fournir un appui au commissaire divisionnaire dans l'exercice de ses fonctions et de servir de point de contact unique avec les fournisseurs de services.

3.5 Pendant la période pertinente pour la présente enquête, toutes les demandes de divulgation devaient être approuvées en premier ressort par un « superintendent » (commmissaire) (ou un « inspector » faisant fonction) et étaient ensuite envoyées à la TLU en vue de leur traitement. Les enquêteurs étaient invités à assortir leurs demandes de détails suffisants pour qu'une décision éclairée puisse être prise et à garder à l'esprit que le commissaire divisionnaire pouvait devoir justifier ultérieurement cette décision en justice ou devant le juge désigné de la High Court (Haute Cour). La TLU et le commissaire divisionnaire sont tenus de vérifier la légalité, la proportionnalité et la nécessité des demandes de divulgation émanant des fonctionnaires de la police nationale. Les demandes jugées non conformes aux exigences de la loi ou des procédures internes de la police étaient renvoyées afin que des éclaircissements ou des informations

complémentaires soient fournies. En vertu d'un protocole d'accord publié au mois de mai 2011, les fournisseurs de services s'engageaient à ne pas traiter **[Or. 6]** les demandes de données relatives à des appels qui ne leur étaient pas parvenues dans le cadre de ce processus. La TLU est également soumise au contrôle du Data Protection Commissioner (commissaire à la protection des données, Irlande).

4. Le contexte factuel pertinent

4.1 La conservation et l'accès aux métadonnées des télécommunications sont régis, en droit irlandais, par la loi de 2011 qui, ainsi que nous l'avons indiqué, a été introduite en vue de mettre en œuvre la directive de 2006. La loi de 2011 a été adoptée à la suite d'une procédure en manquement engagée par la Commission européenne (arrêt du 26 novembre 2009, Commission/Irlande, C-202/09, EU:C:2009:736) en novembre 2009, dans le cadre de laquelle il a été jugé que, en n'adoptant pas les dispositions nécessaires pour se conformer à la directive de 2006, l'Irlande avait manqué aux obligations qui lui incombent en vertu de cette directive.

4.2 Il convient de rappeler que, au mois de février 2009, la Cour avait, dans son arrêt du 10 février 2009, Irlande/Parlement et Conseil (C-301/06, EU:C:2009:68), rejeté le recours en annulation introduit par l'Irlande contre la directive de 2006 au motif que celle-ci n'avait pas été adoptée sur le fondement d'une base juridique appropriée, étant donné que, selon l'Irlande, l'objectif prédominant de ladite directive était de faciliter la recherche, la détection et la poursuite d'infractions pénales.

4.3 La Cour a jugé que, sur la base des constatations opérées aux points 66 à 74 de son arrêt, le contenu matériel de la directive de 2006 visait pour l'essentiel à harmoniser les activités des fournisseurs de services dans le secteur concerné et, par conséquent, concernait de façon prépondérante le fonctionnement du marché intérieur. Son adoption en vertu de l'article 95 CE (tel qu'il se nommait à l'époque) a donc été jugée appropriée. Aux points 80 à 84 de l'arrêt, il a été précisé que la directive de 2006 réglementait des opérations qui étaient indépendantes de la question de l'accès aux données et de l'utilisation des données par les autorités nationales compétentes en matière répressive. **[Or. 7]**

4.4 Le 8 avril 2014, la Cour a rendu son arrêt dans les affaires jointes Digital Rights Ireland Limited/Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a. (C-293/12 et C-594/12, EU:C:2014:238, ci-après l'arrêt « Digital Rights »), par lequel elle a déclaré invalide la directive de 2006. La Cour y a constaté, au point 24, que la directive de 2006 avait pour objectif principal d'harmoniser les dispositions des États membres relatives à la conservation de données par les fournisseurs de services à des fins de prévention, de recherche, de détection et de poursuite des infractions graves. Ainsi qu'il ressort des points 32 à 40 de l'arrêt de la Cour, s'il a été considéré que la directive de 2006 avait entraîné une ingérence grave et d'une vaste ampleur dans

les droits consacrés aux articles 7 et 8 de la Charte, cette ingérence n'était pas de nature à porter atteinte au contenu essentiel de ces droits. Toutefois, la Cour a jugé que, si l'objectif matériel de la directive, consistant à contribuer à la lutte contre la criminalité grave, était un objectif d'intérêt général, l'ingérence dans les droits protégés par la Charte était disproportionnée. Comme cela est indiqué aux points 56 à 66, la Cour a conclu, eu égard au système généralisé de conservation des données qui avait été instauré et à l'absence de conditions matérielles et procédurales définissant l'accès des autorités nationales aux données, que la directive de 2006 ne prévoyait pas de dispositions garantissant que son ingérence dans les droits pertinents consacrés par la Charte était limitée au strict nécessaire et qu'elle ne prévoyait pas non plus de garanties suffisantes pour protéger efficacement les données à caractère personnel.

4.5 Dans son arrêt du 21 décembre 2016, Tele2 Sverige AB/Post- och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970, ci-après l'« arrêt Tele2 Sverige »), la Cour a examiné des questions, posées par deux États membres, qui résultaient de l'arrêt Digital Rights. Dans ces affaires, il a été jugé que des mesures législatives régissant la conservation des données relevaient du champ d'application de la directive de 2002, eu égard à l'article 15, paragraphe 1, de celle-ci. La Cour a ensuite examiné la **[Or. 8]** compatibilité, avec l'article 15, paragraphe 1, de la directive de 2002, de la législation suédoise qui visait initialement à transposer les exigences de la directive de 2006.

4.6 La Cour a jugé, à la lumière des observations formulées aux points 97 à 99 en ce qui concerne la législation nationale, que la « conservation généralisée et indifférenciée » prévue par la législation suédoise constituait une ingérence « d'une vaste ampleur » dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte (point 100). S'il a été jugé, aux points 102 et 103, que seule la lutte contre la criminalité grave était susceptible de justifier de telles mesures de conservation, la Cour a indiqué que cet objectif d'intérêt général « pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte ». Compte tenu du caractère global et non limité de la conservation prévue par la législation suédoise et relevé aux points 104 à 106, la Cour a considéré qu'une telle réglementation nationale excédait les limites du strict nécessaire et ne pouvait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive de 2002, interprété à la lumière de la Charte. La Cour a conclu de manière plus générale, au point 112, que l'article 15, paragraphe 1, doit être interprété en ce sens qu'il 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 de tous les abonnés et utilisateurs.

4.7 La Cour a également précisé que ledit article 15, paragraphe 1, ne s'opposait pas à ce qu'un État membre adopte une réglementation permettant la

« conservation ciblée » de telles données à des fins de lutte contre la criminalité grave, à condition que cette conservation soit limitée au strict nécessaire. Aux points 109 à 111, la Cour semble avoir établi des lignes directrices précisant les circonstances dans lesquelles de telles mesures de conservation ciblées pouvaient être considérées comme satisfaisant aux **[Or. 9]** exigences du droit de l'Union, en ce qui concerne les règles visant à régir la portée et l'application des mesures de conservation des données.

4.8 En réponse à une autre question, la Cour a énoncé, aux points 115 à 125 de son arrêt, une série d'exigences découlant de l'article 15, paragraphe 1, de la directive de 2002 en ce qui concerne l'accès des autorités nationales compétentes aux données conservées. En particulier, il a été précisé que, dans le domaine des infractions pénales, seule la lutte contre la criminalité grave pouvait justifier l'accès aux données conservées. En outre, pour satisfaire aux exigences du principe de proportionnalité, l'accès aux données conservées devait être limité au strict nécessaire et devait, en principe, être subordonné au contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

5. La procédure pénale

5.1 Afin de fournir des informations relatives au contexte qui soient utiles pour ce qui est de la pertinence des données de téléphonie pour le procès pénal dans le cadre duquel M. D. a été accusé du meurtre de M^me^ O'H., la juridiction de céans a établi, à l'annexe II, un résumé succinct du rôle que ces éléments de preuve ont joué dans le cadre de l'enquête et du procès. Il convient toutefois de souligner que la question de l'admissibilité de ces éléments de preuve défavorables à M. D. ne se pose pas dans le cadre de la procédure actuellement pendante devant la Supreme Court (Cour suprême).

6. Les positions des parties

6.1 Il y avait une large convergence de vues entre les parties. Elles ont, bien entendu, admis que la directive de 2006 ne relevait plus du droit applicable et que les modifications qu'elle a apportées à la directive de 2002 avaient été annulées. Les principales questions opposant les parties concernaient la mesure dans laquelle le droit irlandais, principalement sous la forme de la loi de 2011, pouvait être considéré comme demeurant valide eu égard à la directive de 2002, interprétée à la lumière de la Charte. En particulier, les parties différaient sur la mesure dans laquelle il pouvait être affirmé que la position **[Or. 10]** adoptée par la Cour dans l'arrêt Tele2 Sverige avait modifié ou complété celle précédemment adoptée dans l'arrêt Digital Rights. Les parties ont admis que la détection et la poursuite d'infractions graves constituent un objectif en lien avec lequel des mesures proportionnées, potentiellement attentatoires aux droits relatifs au respect de la vie privée, peuvent être adoptées.

6.2 Toutefois, il est soutenu au nom de M. D., sur le fondement de certains passages de l'arrêt Tele2 Sverige, que la conservation « universelle » des métadonnées est illicite indépendamment des garanties pouvant exister quant à l'accès à de telles données. L'État s'est opposé à cette interprétation et a fait valoir qu'il ressortait de l'examen de la jurisprudence de la Cour dans son ensemble qu'il convenait d'adopter une approche globale pour déterminer si le régime protégeait de manière proportionnée les droits au respect de la vie privée.

6.3 Il convient de relever que, comme cela était apparemment requis par le droit de l'Union à l'époque, la loi de 2011 prévoyait la conservation de l'ensemble des métadonnées aux conditions qu'elle énonçait. Par conséquent, si, comme cela a été soutenu au nom de M. D., la conservation « universelle » est en soi interdite, alors la loi de 2011 est contraire au droit de l'Union.

6.4 En revanche, si, comme le soutient l'État, une approche plus large s'imposait, il conviendrait d'examiner les objectifs du régime dans son ensemble, ainsi que les circonstances dans lesquelles l'accès est autorisé, et de déterminer si la loi de 2011 constitue une ingérence proportionnée dans les droits au respect de la vie privée qui sont garantis par le droit de l'Union et par la Charte. En particulier, M. D. fait valoir dans ce contexte que les règles en matière d'accès offrent une protection autonome insuffisante contre les accès inappropriés.

6.5 M. D. soutient que les garanties prévues par la loi de 2011 sont minimales et que cette législation ne prévoit pas de règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services doivent accorder aux autorités nationales l'accès aux données, comme l'exige la Cour. En particulier, le système d'auto-certification des demandes de **[Or. 11]** divulgation de données actuellement mis en œuvre par An Garda Síochána ne satisferait pas à l'exigence selon laquelle les demandes d'accès doivent être soumises à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, comme le prévoit le point 120 de l'arrêt Tele2 Sverige.

6.6 L'État affirme que la loi de 2011 a établi un cadre détaillé régissant l'accès aux données conservées. En outre, l'État fait valoir que la TLU, qui jouit d'une indépendance fonctionnelle par rapport à An Garda Síochána dans l'exercice de sa mission, satisfait à l'exigence de l'existence d'une « entité administrative indépendante » qui procède à un examen ex ante des demandes d'accès et que ce système est renforcé par les niveaux supplémentaires de contrôle judiciaire constitués par le juge désigné, la procédure de réclamation prévue et le contrôle juridictionnel.

6.7 Enfin, l'État fait valoir que, s'il est considéré, en définitive, que la loi de 2011 est contraire au droit de l'Union, toute constatation qui en sera déduite par la juridiction de céans devra uniquement valoir, du point de vue de ses effets dans le temps, pour l'avenir. Selon l'État, cette solution s'impose dans les circonstances exceptionnelles de la présente affaire, dans laquelle, à la date de l'accès aux

données pertinentes dans le litige au principal à la fin de l'année 2013, l'État était tenu, en vertu du droit de l'Union, de mettre en œuvre les dispositions de la directive de 2006 et d'appliquer un système de conservation des données du type de celui qui était prévu par la loi de 2011. En outre, l'État fait valoir que cette solution est appropriée dans des circonstances où une constatation de l'incompatibilité non assortie d'une limitation de ses effets aurait des conséquences non négligeables pour la recherche et la poursuite d'infractions graves en Irlande, à l'égard de ceux qui ont été jugés et condamnés, ainsi que pour les enquêtes et les poursuites en cours.

7. Les éléments de preuve avancés

7.1 Le commissaire divisionnaire responsable en matière de divulgation des données qui occupait ces fonctions au cours de l'enquête sur le meurtre de M^me^ O'H. a indiqué dans sa déposition que non seulement il s'assurait du respect des critères légaux par la **[Or. 12]** demande de divulgation, mais qu'il prenait également en considération les principes de nécessité, de proportionnalité et de pertinence et évaluait le potentiel d'atteinte collatérale aux droits d'autres personnes.

7.2 Le témoin a confirmé que, selon lui, les demandes de données présentées en l'espèce satisfaisaient à ces critères. Il a également fait état de sa propre expérience quant à l'utilité des données de téléphonie pour identifier ou éliminer des suspects dans le cadre des enquêtes portant sur un certain nombre d'infractions graves, et notamment le meurtre. Il a estimé que, si l'accès aux données relatives aux télécommunications n'était pas ouvert, l'efficacité d'An Garda Síochána dans la lutte contre le terrorisme et la criminalité grave et organisée serait considérablement réduite. Il avait également connaissance de cas dans lesquels l'accès à de telles données avait joué un rôle crucial à l'appui d'enquêtes impliquant un risque potentiel grave pour la vie, tels les enlèvements ou la disparition de personnes vulnérables.

7.3 Les autres experts cités au nom de l'État ont souligné l'importance des données de téléphonie et des données Internet dans la prévention et la recherche d'infractions graves, en relevant notamment que, au Royaume-Uni, ces données sont utilisées aussi souvent par la défense que par le ministère public, étant donné qu'elles sont susceptibles d'étayer ou d'infirmer des théories quant à la présence d'une personne en un lieu donné.

7.4 Le caractère approprié du terme « surveillance » dans le contexte de la conservation des données a été contesté par les témoins, au motif que ce terme désigne un système de suivi actif ou de localisation, par opposition au stockage de données « inertes » qui ne seront peut-être jamais examinées au cours de la période pendant laquelle elles sont conservées. Selon eux, une véritable surveillance s'exerce lorsque les données sont passées au crible, de sorte que des

conclusions puissent en être tirées en ce qui concerne les personnes qui étaient parties aux communications.

7.5 Les experts privilégiaient une approche large de la conservation des données tout en reconnaissant la nécessité d'un contrôle strict de l'accès à ces données, ainsi que la nécessité de garanties et d'une responsabilité en la matière. Ils doutaient du fait qu'il soit possible, en pratique, de cibler des groupes ou des zones géographiques en vue de la conservation des données, en invoquant l'éventualité **[Or. 13]** qu'un tel ciblage pourrait fort bien être considéré comme discriminatoire et donc illicite tout en étant inefficace, compte tenu de la mobilité des organisations terroristes et criminelles modernes. L'approche du « gel rapide » n'a été jugée utile que dans les situations où il existe un suspect identifiable à un stade très précoce de l'enquête.

7.6 L'utilité pratique des données de téléphonie conservées a été soulignée par le commissionnaire divisionnaire de la « Special Detective Unit ». Cette unité est la section antiterroriste d'An Garda Síochána, qui a pour fonction de lutter contre les menaces que font peser sur la sûreté de l'État des organisations illégales telles que l'Irish Republican Army ou des services de renseignement étrangers hostiles. Ce témoin a décrit un certain nombre d'affaires qui n'auraient pas pu être résolues sans l'utilisation des données conservées aux fins de prouver un contact entre suspects, de retracer l'itinéraire suivi par un suspect, de s'assurer que les images de vidéosurveillance soient préservées, de remettre en cause les déclarations d'un suspect ou d'identifier une personne non encore connue des services de la police nationale.

7.7 M. D. n'a cité aucun expert et n'a pas contesté la plupart des fondements factuels des éléments de preuve apportés par l'État. Il a, en revanche, tenté d'établir que le régime irlandais de conservation des données était « généralisé et indifférencié », pour reprendre les termes de la Cour dans l'arrêt Tele2 Sverige, et que le système en matière d'accès ne comportait pas de contrôle préalable par une juridiction ou une entité administrative indépendante. Les témoins tendaient à partager ce point de vue dans une certaine mesure et ils ont également admis que les modalités de contrôle en vigueur en Irlande semblaient moins rigoureuses qu'au Royaume-Uni.

8. Les constatations de fait

8.1 La Supreme Court (Cour suprême) relève que la jurisprudence de la Cour mentionne de manière répétée l'objectif de la lutte contre la criminalité grave. S'il est fréquemment fait référence, plus spécifiquement, à la criminalité organisée et au terrorisme, la Supreme Court (Cour suprême) considère que la notion de **[Or. 14]** criminalité grave ne se limite pas à ces catégories, mais englobe également des crimes tels que le meurtre qui fait l'objet de la procédure pénale à l'origine de la présente affaire.

8.2 La Supreme Court (Cour suprême) est consciente du fait que la détection, en particulier, de certaines catégories d'infractions graves et la poursuite de celles-ci sont de plus en plus influencées par des éléments de preuve tels que ceux qui ont été avancés dans la procédure pénale engagée contre M. D.

8.3 Si la criminalité organisée et le terrorisme peuvent effectivement, dans certains cas, faire naître des soupçons préalables à la commission d'une infraction spécifique particulière, le type d'infraction grave sur lequel porte la présente procédure implique rarement des circonstances qui pouvaient raisonnablement être connues des autorités chargées de l'enquête et qui pouvaient donner lieu à des soupçons préalables. L'expérience a montré à la Supreme Court (Cour suprême) que certaines de ces affaires n'ont été résolues qu'en raison de la disponibilité du type de données visées dans la présente procédure.

8.4 Il semble à la Supreme Court (Cour suprême) que des affaires du type de celles qui ont été décrites, dont la présente affaire constitue un exemple particulier, concernent fréquemment de graves délits à l'encontre de femmes, d'enfants et d'autres personnes vulnérables. Ainsi qu'il a déjà été relevé, il ne serait pas possible, dans un nombre important de cas de ce type, de découvrir l'auteur des faits et, a fortiori, de le poursuivre de manière adéquate. Dans d'autres cas, la possibilité de monter un dossier d'accusation solide serait fortement compromise. En effet, il convient également de relever que, comme en l'espèce, la téléphonie elle-même est souvent utilisée dans de tels cas à des fins de pédopiégeage ou d'exploitation, d'une autre manière, de personnes vulnérables.

8.5 Il semble à la Supreme Court (Cour suprême) qu'il est particulièrement important de souligner, dès lors, qu'il n'est pas possible d'avoir accès à ce qui n'a pas été conservé. Si, sur la base de l'argument avancé au nom de M. D., il n'est pas permis de procéder à une conservation « universelle » des métadonnées, en dépit du caractère rigoureux des règles en matière d'accès, il s'ensuit que beaucoup de ces infractions graves visant des femmes, des enfants et d'autres personnes vulnérables ne pourront pas être **[Or. 15]** mises au jour ou faire l'objet de poursuites couronnées de succès. Dans ce contexte, la Supreme Court (Cour suprême) a constaté les faits suivants :

i) d'autres formes de conservation des données, au moyen d'un ciblage géographique ou autre, ne permettraient pas d'atteindre les objectifs de prévention, de recherche, de détection et de poursuite de certains types au moins d'infractions graves et, de plus, pourraient entraîner une violation potentielle d'autres droits de la personne ;

ii) l'objectif de la conservation des données par un moyen moins lourd que le régime général de la conservation des données, assorti des garanties nécessaires, est irréalisable ; et

iii) les objectifs de prévention, de recherche, de détection et de poursuite des infractions graves seraient fortement compromis en l'absence d'un régime

général de conservation de données. La juridiction de céans admet les éléments de preuve décrits aux points 7.2 à 7.6 ci-dessus et y souscrit.

8.6 La Supreme Court (Cour suprême) reconnaît que la question de l'admissibilité des preuves dans le cadre d'un procès pénal relève du droit national. Néanmoins, la question de la validité de certaines parties de la loi de 2011 est une question qui peut être soulevée dans le cadre d'une procédure civile. En outre, la question de la recevabilité des preuves devrait elle-même être abordée à la lumière d'un (éventuel) constat d'invalidité et de la nature précise, de l'étendue, de la justification, de la portée et des effets dans le temps d'un tel constat. Par conséquent, la juridiction de céans estime nécessaire de poser à la Cour les questions qui suivent.

9. Les questions préjudicielles

9.1 Un régime général/universel de conservation des données – même assorti de restrictions strictes en matière de conservation et d'accès – est-il, en soi, contraire aux dispositions de l'article 15 de la directive 2002/58/CE, interprétées à la lumière de la Charte ? **[Or. 16]**

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

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

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

9.5 Si une juridiction nationale est tenue de conclure qu'une mesure nationale est contraire aux dispositions de l'article 15 de la directive 2002/58/CE, interprétées à la lumière de la Charte, est-elle fondée à limiter les effets dans le temps d'une telle constatation si elle estime que ne pas limiter ses effets entraînerait « le chaos et un préjudice grave pour l'intérêt général » [conformément à l'approche adoptée, par exemple, dans le jugement R (National Council for Civil Liberties) v Secretary of **[Or. 17]** State for Home Department and Secretary of State for Foreign Affairs [2018] EWHC 975, point 46] ?

9.6 Une juridiction nationale invitée à constater l'incompatibilité de la législation nationale avec l'article 15 de la directive 2002/58/CE ou à écarter l'application de cette législation ou bien à déclarer que l'application d'une telle législation a violé les droits d'une personne physique, que ce soit dans le cadre d'une procédure engagée afin de faciliter la présentation d'un argument relatif à l'admissibilité des preuves dans une procédure pénale ou dans un autre cadre, peut-elle être autorisée à refuser de faire droit à cette demande en ce qui concerne les données conservées en application de la disposition nationale adoptée en vertu de l'obligation, prévue à l'article 288 TFUE, de transposer fidèlement en droit national les dispositions d'une directive ou à limiter une telle constatation à la période postérieure à la déclaration de l'invalidité de la directive 2006/24/CE par la Cour le 8 avril 2014 ?

Annexe I : Le régime législatif irlandais

1. Le Communications (Retention of Data) Act 2011 [loi de 2011 sur les communications (conservation des données)] a été adopté dans le but déclaré de mettre en œuvre la directive de 2006. Cette loi a été modifiée postérieurement aux faits essentiels qui ont eu lieu dans l'affaire au principal (à savoir la conservation et la consultation des données téléphoniques de M. D.). Toutefois, les dispositions de la loi qui sont pertinentes pour la présente procédure sont exposées ci-après.

2. L'article 1er de la loi de 2011 définit le terme « données » comme visant « les données relatives au trafic ou les données de localisation et les données connexes nécessaires pour identifier l'abonné ou l'utilisateur ». L'article 3, paragraphe 1, impose à tous les fournisseurs de services de conserver, notamment, les données décrites à l'annexe 2, partie 1, de la loi de 2011, pendant deux ans. Il s'agit des « données relatives à la téléphonie fixe en réseau et à la téléphonie mobile » qui sont décrites comme étant les données permettant d'identifier la source et la destination d'une communication, de déterminer la date et l'heure du début et de la fin d'une communication, de déterminer le type de communication concerné, ainsi que d'identifier le type **[Or. 18]** et la localisation géographique du matériel de communication utilisé. Le contenu des communications ne relève pas de ce type de données.

3. En vertu des articles 4 et 5 de la loi, les fournisseurs de services doivent prendre certaines mesures pour veiller à ce que les données soient protégées contre les accès non autorisés. En vertu de l'article 4, paragraphe 2, de la loi de

2011, le commissaire à la protection des données est désigné comme autorité de surveillance aux fins de cette loi.

4. L'article 6 prévoit les conditions dans lesquelles une demande de divulgation peut être introduite. Le paragraphe 1 de cet article dispose :

> « Un fonctionnaire de la police nationale dont le rang n'est pas inférieur à celui de "chief superintendent" peut demander à un fournisseur de services de lui communiquer les données conservées par ce fournisseur de services conformément à l'article 3 si ce fonctionnaire estime que les données en question sont nécessaires à des fins :
>
> (a) de prévention, de détection, de recherche ou de poursuite d'une infraction grave,
>
> (b) de sauvegarde de la sûreté de l'État,
>
> (c) de préservation de la vie humaine. »

5. C'est l'article 6, paragraphe 1, sous a), qui est pertinent aux fins de la procédure engagée par M. D. dans le cadre du litige de droit national. L'« infraction grave » est définie à l'article 1er de la loi de 2011 comme étant une infraction passible d'une peine d'emprisonnement d'une durée égale ou supérieure à 5 ans ou l'une des autres infractions énumérées à l'annexe 1 de la loi. L'article 6, qui n'est pas directement pertinent aux fins de la présente procédure, confère un droit d'accès similaire aux officiers supérieurs de l'armée lorsque les données sont nécessaires pour sauvegarder la sûreté de **[Or. 19]** l'État, ainsi qu'aux agents des Revenue Commissioners (administration fiscale) en ce qui concerne les infractions fiscales graves. L'article 7 de la loi impose aux fournisseurs de services de faire droit à de telles demandes.

6. En vertu de l'article 9, paragraphe 1, de la loi de 2011, le commissaire d'An Garda Síochána doit établir et transmettre au Minister for Justice and Equality (ministre de la Justice et de l'Égalité, Irlande) un rapport annuel portant sur les données visées à l'annexe 2 qui ont fait l'objet de toutes les demandes de divulgation introduites en vertu de l'article 6, paragraphe 1, au cours de la période pertinente. Ce rapport est destiné à constituer l'un des éléments servant de base au rapport adressé par l'État à la Commission européenne en application de l'article 9, paragraphe 8.

7. L'article 10 de la loi de 2011 définit la procédure de réclamation qui se rapporte à la divulgation de données. Les personnes qui estiment que leurs données ont été consultées en violation de l'article 6 de la loi peuvent solliciter l'ouverture d'une enquête à ce sujet. Cette enquête est effectuée par une personne exerçant la fonction de « Complaints Referee », actuellement un juge de la Circuit Court (tribunal itinérant, Irlande) en activité, qui est désignée en vertu d'une législation préexistante concernant l'interception des communications, l'Interception of Postal Packets and Telecommunications Messages (Regulation)

Act 1993 (loi de 1993 portant réglementation de l'interception des colis postaux et des messages transmis par télécommunication, ci-après la « loi de 1993 »).

8. Indépendamment de cette procédure, les articles 11 et 12 de la loi de 2011 confèrent à un juge désigné en vertu de l'article 8 de la loi de 1993 le pouvoir de contrôler l'application des dispositions de la loi de 2011 et de présenter un rapport sur son application au Taoiseach (Premier ministre). Le juge désigné a le pouvoir d'enquêter sur toute demande de divulgation introduite ainsi que de consulter et d'inspecter tout document ou enregistrement pertinent.

Annexe II : La procédure pénale

1. M^me^ O'H. a disparu de Dublin le 22 août 2012. Des SMS retrouvés sur son ordinateur portable ont fait naître de graves inquiétudes et il a été constaté qu'ils provenaient d'un téléphone qui avait été enregistré sous un faux nom (ci-après le « téléphone 474 »). La dépouille de M^me^ O'H. **[Or. 20]** n'a été découverte qu'en septembre 2013. Quelques jours plus tard, deux autres téléphones, abandonnés à un endroit distinct, ont été récupérés. Ces appareils ont été appelés, dans les éléments de preuve, les téléphones « maître » et « esclave » et l'examen des données conservées a fait apparaître qu'ils n'avaient été utilisés que dans le but de communiquer entre eux. Le contenu des SMS extraits de ces appareils mobiles (et non de données conservées) comportait certains détails personnels se rapportant manifestement à M^me^ O'H. et indiquait qu'elle entretenait une liaison avec l'utilisateur du téléphone « maître ». Les messages figurant dans ces téléphones et sur le téléphone 474 indiquaient également que l'homme avec qui elle avait cette liaison avait un penchant pour la violence au couteau contre les femmes, avait tué un mouton et avait coupé M^me^ O'H. avec un couteau à plusieurs reprises.

2. M. D. a été identifié à titre de suspect dans le cadre de l'enquête grâce à l'utilisation de données de téléphonie conservées. L'horaire et la localisation géographique des appels passés à partir du téléphone « maître » au cours d'un jour précis du mois de juillet 2012 ont conduit à l'identification de la voiture de M. D. dans le registre des péages autoroutiers. La localisation de son domicile et de son lieu de travail correspondaient aux antennes relais les plus fréquemment utilisées par le téléphone « maître ». Les données de téléphonie mobile conservées qui avaient été générées par le téléphone de M. D. (lequel lui avait été fourni par son employeur et a été dénommé le « téléphone 407 ») ont ensuite été consultées par les enquêteurs de la police nationale, en vertu des dispositions de la loi de 2011. Ces données ont été examinées en vue de déterminer si les mouvements de ce téléphone étaient en corrélation avec les données de localisation disponibles qui étaient afférentes au téléphone 474 et au téléphone « maître ».

3. Il convient de relever que certains autres éléments de preuve à charge, qui ne résultaient pas de l'accès aux données conservées, indiquaient qu'il existait un lien entre le téléphone 407 et M^me^ O'H. et indiquaient également qu'il existait un lien entre M. D. et les téléphones 474 et « maître ». Toutefois, l'analyse des données conservées relatives au téléphone 474, aux téléphones « maître » et « esclave » et

au **[Or. 21]** téléphone 407, dans le but de les relier à M. D., était un aspect important de l'affaire.

4. M. D. nie tout lien avec le téléphone 474, ainsi qu'avec les téléphones « maître » et « esclave ». Bien qu'il admette qu'il ne peut faire valoir un intérêt au respect de sa vie privée que pour ce qui est de son propre téléphone, il soutient que toutes les données conservées ont été obtenues en violation du droit de l'Union et il s'oppose à l'utilisation de ces données aux fins de le relier aux autres téléphones. S'il conteste la licéité de la loi de 2011 au regard du droit de l'Union, il n'a pas allégué, que ce soit au cours de son procès pénal ou dans le cadre de la présente procédure, que la législation a été appliquée concrètement, dans les circonstances particulières de l'espèce, de manière abusive ou inappropriée. En revanche, il conteste, dans son principe, le caractère suffisant des garanties en matière d'accès.

5. La présente procédure civile a été engagée par M. D., à la lumière de l'arrêt Digital Rights de la Cour, le même jour que l'ouverture de son procès pénal. Dans le cadre de ce procès, il a contesté l'admissibilité des données de téléphonie au regard tant du droit constitutionnel irlandais que du droit de l'Union. Le juge, après une audience en l'absence du jury, a considéré que les données étaient recevables. Le 27 mars 2015, M. D. a été déclaré coupable, par un jury, du meurtre de M^{me} O'H.

6. M. D. a fait appel de sa condamnation. Dans le cadre des moyens d'appel, il a notamment reproché au juge de première instance d'avoir, à tort, admis en preuve les données de téléphonie relatives à son téléphone et aux autres téléphones portables qui lui ont été attribués par le ministère public, au motif que le régime légal régissant la conservation et l'accès à ces données violait les droits que lui confère le droit de l'Union. Comme nous l'avons indiqué, l'audience relative à cet appel devant la Court of Appeal (Cour d'appel) n'a pas encore eu lieu et la procédure restera suspendue jusqu'à ce que la Supreme Court (Cour suprême) ait statué sur la présente affaire civile. Ainsi qu'il ressort de ce qui précède, l'intérêt de M. D. dans la présente procédure devant l'assemblée plénière est qu'un constat en sa **[Or. 22]** faveur lui permette de soutenir, dans le cadre de l'appel pénal, que sa condamnation doit être infirmée, car elle était, en partie, fondée sur des éléments de preuve qui auraient dû être écartés au motif qu'ils avaient été obtenus illégalement. Il aura la possibilité de faire valoir que, à la suite de la décision rendue par la Cour dans l'affaire Digital Rights, l'accès aux données pertinentes n'aurait pas dû être accordé aux enquêteurs et que ces données étaient dès lors irrecevables à titre de preuve. Toutefois, l'exclusion des preuves du procès relève du juge du fond et de la procédure pénale en appel. Dans le cadre de l'appel actuellement pendant devant la juridiction de céans, la seule question qui se pose est celle de savoir si c'est à juste titre que la High Court (Haute Cour) a jugé que l'article 6, paragraphe 1, sous a), du Communications (Retention of Data) Act 2011 était contraire au droit de l'Union.

[omissis : la partie qui suit est l'ordonnance formelle renvoyant à la Cour les questions (déjà énoncées au point 9 ci-dessus) et suspendant la procédure dans l'attente de la décision de la Cour]