THE SUPREME COURT

[Record No: 2019/18]

Clarke C.J.
O'Donnell J.
McKechnie J.
MacMenamin J.
Charleton J.
O'Malley J.
Irvine J.

Between/

G.D.

Plaintiff / Respondent

and

The Commissioner of An Garda Síochána, the Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General

Defendants / Appellants

Order for Reference by the Court of certain questions on the interpretation of European Union law to the Court of Justice of the European Union under Article 267 of the Treaty on the Functioning of the European Union dated

1. Introduction

1.1 This case relates to the regime established under the Communications (Retention of Data) Act 2011 ("the 2011 Act") which governs the retention of, and access to, telecommunications metadata by national authorities in Ireland and, in particular, by the Irish police force ("An Garda Síochána") in the course of the detection, investigation and prosecution of serious crime.

1.2 In March 2015, the plaintiff ("Mr. D.") was convicted by jury of the murder of Ms. O'H., for which he received a life sentence. He has at all times denied guilt. This conviction is the subject of an appeal by Mr. D., which is pending before the Irish Court of Appeal. In the course of the trial, Mr. D. unsuccessfully contested the admissibility of certain prosecution evidence based on retained telephony data. Mr. D. initiated these parallel civil proceedings, in the course of which this request for a preliminary ruling has arisen, which seek to challenge certain provisions of the 2011 Act under which such telephony metadata was retained and accessed. The objective of these proceedings is to seek a declaration of invalidity of the relevant legislative provision, with a view to contending at the appeal against Mr. D.'s conviction that the evidence of the telephony data ought not to have been admitted at his trial, thus rendering his conviction unsafe. The defendants ("the State") seek that the validity of the legislation is upheld.

1.3 This request for a preliminary ruling is made in the context of an appeal to the Supreme Court brought by the State as against the decision of the High Court. In the decision of the High Court (O'Connor J.) of 6 December 2018 (*Dwyer v. Commissioner of An Garda Síochána & ors* [2018] IEHC 685), Mr. D. was granted a declaration that s. 6(1)(a) of the 2011 Act was inconsistent with Article 15(1) of Directive 2002/58/EC ("the 2002

Directive"), read in light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union ("the Charter").

1.4 This request for a preliminary ruling seeks clarification regarding the requirements of Union law in relation to the retention of data for the purposes of combating serious crime, and the necessary safeguards which must regulate the access of such data, in view of the competence of a Member State in relation to matters of crime. The Court also seeks clarification on the scope and temporal effects of the declaratory relief, if any, which could be granted in the circumstances of this case.

2. European Legislation

2.1 Underpinning this reference are the provisions of the Treaty on European Union, in particular that of Article 5(4), regarding the principle of proportionality, and Article 6(1), recognising the rights and freedoms set out in the Charter. This Court also considers that the provisions of Protocol (No 21) to the Treaty, on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, may bear some relevance to these proceedings.

2.2 The Union directives which have been adopted in respect of the processing of personal data which are relevant for the purposes of this reference are Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the 1995 Directive"), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("the 2002 Directive") and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly

available electronic communication services or of public communications networks and amending Directive 2002/58/EC ("the 2006 Directive"), the latter subsequently being declared invalid by the CJEU in 2014, as detailed below.

2.3 Also central to this matter are the rights and freedoms recognised by the Charter, and in particular Articles 7, 8 and 52(1) thereof.

3. Irish Legislative Scheme

3.1 The 2011 Act was enacted with the express purpose of giving effect to the 2006 Directive, and its provisions are detailed in Appendix I to this reference. Insofar as is relevant to this case, s. 3 of the Act requires all service providers to retain the "fixed network telephony and mobile telephony data" for a period of two years. This is data which identifies the source, the destination, and the date and time of the start and end of a communication, the type of communication involved, and the type of and the geographic location of the communications equipment used. The content of communications does not fall within this type of data.

3.2 This data may be accessed and disclosed as a result of a disclosure request. Section 6 of the 2011 Act provides for the conditions under which a disclosure request may be made, and subs. (1) provides that a member of An Garda Síochána not below the rank of chief superintendent may make a disclosure request where that member is satisfied that the data are required for, *inter alia*, the prevention, detection, investigation or prosecution of a serious offence. A "serious offence" is defined as one which is punishable by imprisonment for a term of 5 years or more and also those other offences listed in Schedule 1 to the Act.

3.3 Oversight mechanisms prescribed by the 2011 Act include the complaints procedure set out at s. 10 thereof, and the duties of a "designated judge", as provided by s. 12, who is given the task of reviewing the operation of the provisions of the Act.

3.4 It is apparent from the evidence before the High Court in these civil proceedings that, as a matter of internal policy, the head of An Garda Síochána, the Garda Commissioner, determined that applications for the disclosure of telephony data made under the 2011 Act should be dealt with in a centralised manner, by a single chief superintendent. The detective chief superintendent given responsibility for data disclosure was the head of the security and intelligence section of An Garda Síochána, and it is he or she who ultimately decides whether to issue a request for disclosure to the communication service providers under the provisions of the 2011 Act. A small, independent unit known as the Telecommunications Liaison Unit ("the TLU") was established to support the functions of the detective chief superintendent and to act as the single point of contact with service providers.

3.5 At the times relevant to this investigation, all disclosure requests had to be approved in the first instance by a superintendent (or an inspector acting in that capacity) and were then sent to be processed by the TLU. Investigators were directed to include sufficient detail in the request to enable an informed decision to be made, and to bear in mind that the chief superintendent might have to justify the decision later in court or to the designated High Court judge. The TLU and the detective chief superintendent are required to verify the legality, proportionality and necessity of disclosure requests sought by members of An Garda Síochána. Applications deemed not to comply with the requirements of the law or of internal garda protocols were returned for clarification or additional information. Under a Memorandum of Understanding issued in May 2011, service providers would not process

requests for call related data that did not come through this process. The TLU is also subject to audit by the Data Protection Commissioner.

4. Relevant Factual Context

4.1 The retention of, and access to, telecommunications metadata is governed under Irish law by the 2011 Act which, as mentioned above, was introduced in order to give effect to the 2006 Directive. The 2011 Act was adopted following infringement proceedings taken by the European Commission (*Commission v. Ireland* (Case C-202/09) [2009] E.C.R. I-203, ECLI:EU:C:2009:736) in November 2009, as a result of which Ireland was held to have failed to fulfil its obligations under the 2006 Directive by failing to adopt the provisions necessary to comply therewith.

4.2 It is noteworthy that in February 2009, the CJEU, in *Ireland v. Parliament & Council* (Case C-301/06) ECLI:EU:C:2009:68, dismissed Ireland's challenge to the 2006 Directive, which was based on a claim that it was not adopted on an appropriate legal basis, given the predominant objective of the directive was, it was submitted, to facilitate the investigation, detection and prosecution of crime.

4.3 The CJEU held that, based on the findings made at paras. 66-74 of its judgment, the substantive content of the 2006 Directive was directed essentially at harmonising the activities of service providers in the relevant sector, and therefore related primarily to the functioning of the internal market. Thus, it was held that its introduction under Article 95 TEC (as it then was) was appropriate. At paras. 80-84 of the judgment, it was specified that the 2006 Directive regulates operations which are independent of matters relating to access to and use of data by competent national law enforcement authorities.

4.4 On 8 April 2014, the CJEU delivered judgment in *Digital Rights Ireland Limited v. Minister for Communications, Marine and Natural Resources & Ors and Kärntner Landesregierung and Others* (Joined Cases C-293/12 and C-594/12), ECLI:EU:C:2014:238 ("*Digital Rights*"), declaring the 2006 Directive invalid. Therein, the CJEU found at para. 24 that the main objective of the 2006 Directive was to harmonise Member States' provisions concerning data retention by service providers for the purpose of the prevention, investigation, detection and prosecution of serious crime. As is apparent from paras. 32-40 of the Court's judgment, while the 2006 Directive was considered to have caused a wide-ranging and serious interference with the rights enshrined in Articles 7 and 8 of the Charter, this interference was not such as to adversely affect the essence of those rights. However, the CJEU held that while the material objective of the directive, to contribute to the fight against serious crime, was an objective of general interest, the interference with Charter rights caused was disproportionate. As recorded in paras. 56-66, in light of the generalised scheme of data retention which was provided for and the absence of any substantive and procedural conditions delimiting the access of the national authorities to the data, the CJEU concluded that the 2006 Directive did not lay down provisions which ensured that its interference with the relevant Charter rights was limited to what is strictly necessary, and further, it did not provide for sufficient safeguards to effectively protect personal data.

4.5 In its judgment of 21 December 2016 in *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* (Joined Cases C-203/15 and C-698/15), ECLI:EU:C:2016:970 ("*Tele2 Sverige*"), the Court considered questions referred by two Member States arising from the *Digital Rights* judgment. In those cases, it was held that legislative measures governing data retention fall within the scope of the 2002 Directive, in light of Article 15(1) thereof. The CJEU then turned to consider the

compatibility of Swedish legislation which was originally intended to transpose the requirements of the 2006 Directive with Article 15(1) of the 2002 Directive.

4.6 The CJEU held, in light of the observations made in respect of the national legislation at paras. 97-99, that the "general and indiscriminate retention" which was provided for in Swedish legislation was a "very far-reaching" interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter (at para. 100). While it was held, at paras. 102 and 103, that only the objective of fighting serious crime is capable of justifying such retention measures, the Court stated that that objective of general interest "however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight". In light of the comprehensive and unrestricted nature of the retention prescribed by Swedish legislation, as set out at paras. 104-106, the CJEU held that such national legislation exceeded the limits of what is strictly necessary and could not be considered to be justified within a democratic society, as required by Article 15(1) of the 2002 Directive, as interpreted in light of the Charter. The Court concluded more generally, at para. 112, that Article 15(1) must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all data of all subscribers and users.

4.7 The CJEU also specified that Article 15(1) does not prevent a Member State from adopting legislation permitting the "targeted retention" of such data for the purpose of fighting serious crime, provided the retention is limited to what is strictly necessary. At paras. 109-111, a number of guidelines appear to have been set out by the Court, outlining the circumstances in which such targeted retention measures could be considered to satisfy the

requirements of Union law, as regards the rules which are to govern the scope and application of data retention measures.

4.8 In response to a further question, the Court set out, at paras. 115-125 of its judgment, a number of requirements arising from Article 15(1) of the 2002 Directive in relation to the access of competent national authorities to retained data. In particular, it was specified that in the area of criminal offences, only the objective of fighting serious crime can justify access to retained data. Further, in order to satisfy the requirements of the principle of proportionality, access to retained data must be limited to what is strictly necessary and should, as a general rule, be subject to a prior review by a court or an independent administrative body.

5. The Criminal Proceedings

5.1 In order to provide appropriate background information as to the relevance of the telephony data to the criminal trial in which Mr. D. was accused of the murder of Ms. O'H., the Court has set out, in Appendix II, a brief synopsis of the role which that evidence played in the investigation and trial. It should, however, be emphasised that the issue of the admissibility of that evidence against Mr. D. does not arise in the proceedings currently before the Supreme Court.

6. Positions of the Parties

6.1 There was a significant measure of agreement between the parties. It was, of course, accepted that the 2006 Directive is no longer law and that the amendments which it brought about to the 2002 Directive have been annulled. The central issues between the parties concerned the extent to which Irish law, principally in the form of the 2011 Act, can be said to remain valid having regard to the 2002 Directive, as interpreted in the light of the Charter. In particular, the parties differed as to the extent to which it may be said that the position

adopted by the CJEU in *Tele2 Sverige* altered or expanded on the position previously adopted in *Digital Rights*. It was accepted that the detection and prosecution of serious crime represents an object in respect of which proportionate measures, potentially interfering with privacy rights, can be adopted.

6.2 However, relying on certain passages from the judgment in *Tele2 Sverige*, it is argued on behalf of Mr. D. that "universal" retention of metadata is impermissible irrespective of the safeguards which may be in place concerning access to such data. The State opposed this interpretation and argued that a consideration of the case law of the CJEU as a whole suggested that an overall approach had to be taken to the regime to determine whether it protected privacy rights in a proportionate manner.

6.3 It should be noted that the 2011 Act, as was, apparently, at the time required as a matter of European Union law, provided for the retention of all metadata subject to its terms. Thus if, as argued on behalf of Mr. D., "universal" retention is in itself impermissible, then the 2011 Act is inconsistent with European Union law.

6.4 On the other hand, if, as the State argues, a broader approach is appropriate, then it is necessary to consider the objects of the regime as a whole, the circumstances in which access is permissible, and to determine whether the 2011 Act is a proportionate interference with privacy rights guaranteed under European Union law and by the Charter. In particular, in that context, Mr. D. argues that the access regime provides insufficient independent protection against inappropriate access.

6.5 Mr. D. submits that safeguards provided for in the 2011 Act are minimal, and that the legislation does not lay down clear and precise rules indicating in what circumstances and under which conditions service providers must grant national authorities access to data, as required by the CJEU. In particular, the existing system of self-certification of requests for

disclosure of data which is carried out by An Garda Síochána is said not to satisfy the requirement that access requests be subject to a prior review carried out by either a court or an independent administrative body, as stipulated at para. 120 of *Tele2 Sverige*.

6.6 The State maintains that the 2011 Act established a detailed framework governing access to retained data. Further, the State argues that the TLU, enjoying functional independence from An Garda Síochána when carrying out its duties, satisfies the requirement of an "independent administrative body" which performs an *ex ante* review of access requests and that this system is reinforced by additional layers of judicial oversight provided through the designated judge, the prescribed complaints procedure and judicial review.

6.7 Finally, the State argues that, if the 2011 Act is ultimately considered to be inconsistent with Union law, the temporal effect of any declaration which this Court is to make as a result should be prospective only. This, it is submitted, is appropriate in the exceptional circumstances of this case, where at the time the relevant data was accessed in the main proceedings in late 2013, the State was required under Union law to give effect to the provisions of the 2006 Directive and to maintain a system of data retention of the kind prescribed in the 2011 Act. Further, the State argues that this is appropriate in circumstances where a declaration of inconsistency without any limitation on its effect would have significant consequences for the investigation and prosecution of serious crime in Ireland, in respect of those who have been tried and convicted, and in respect of ongoing investigations and prosecutions.

7. Evidence Tendered

7.1 The detective chief superintendent with responsibility for data disclosure who held the relevant office during the course of the investigation into the murder of Ms. O'H. gave evidence that, in addition to ensuring that the statutory criteria were met in respect of the

disclosure request, he also considered the principles of necessity, proportionality and relevance, and assessed the potential for collateral intrusion on the rights of other individuals.

7.2 The witness confirmed that, in his view, the requests for data in this case met these criteria. He also gave evidence of his own experience of the usefulness of telephony data in identifying or eliminating suspects in the investigation of a range of serious crimes, including murder. He believed that if access to telecommunications data was not available, the effectiveness of An Garda Síochána in combating terrorism and serious and organised crime would be significantly diminished. He was also aware of instances in which access to such data had played a crucial role in supporting investigations involving potential serious risk to life, such as kidnappings or the disappearance of vulnerable persons.

7.3 The other expert witnesses called on behalf of the State emphasised the importance of telephony and internet data in the prevention and investigation of serious crime, noting, *inter alia*, that in the United Kingdom such data is used as often by the defence as by the prosecution because of its potential for supporting or disproving theories as to a person's presence in a particular location.

7.4 The appropriateness of the term "surveillance" in the context of data retention was disputed by the witnesses, with the view being taken that this word denotes an active monitoring or tracking system, as opposed to the storage of "inert" data that might never be examined during the period for which it is kept. Meaningful surveillance, it was suggested, occurs when the data is sifted to the point that inferences about the individuals engaged in communication can be drawn.

7.5 The experts favoured a broad approach to data retention while accepting the need for strict control of, and safeguards and accountability for, access to that data. They doubted the practicality of targeting groups or geographical areas for data retention, citing the possibility

that such targeting could well be seen as unlawfully discriminatory while also being ineffective, given the agility of modern terrorist and criminal organisations. The "quick freeze" approach was seen as useful only in situations where there is an identifiable suspect at a very early stage of the investigation.

7.6 The practical utility of retained telephony data was emphasised by the detective chief superintendent of the Special Detective Unit. This unit is the counter-terrorism section of An Garda Síochána, with the function of combating threats to State security from unlawful organisations such as the Irish Republican Army or hostile foreign intelligence agencies. This witness described a number of cases that could not have been resolved without the use of retained data for the purpose of proving contact between suspects, or tracking a route taken by a suspect, or ensuring that CCTV footage was preserved, or challenging an account given by a suspect, or identifying a person not previously known to An Garda Síochána.

7.7 Mr. D. did not call any expert evidence and, for the most part, did not challenge any factual basis for the State's evidence. His concern was, rather, to seek to establish that the Irish data retention scheme was "general and indiscriminate", as termed by the CJEU in *Tele2 Sverige*, and that the access system did not include prior review by a court or an independent administrative body. The witnesses were inclined to accept these propositions to some extent, and they also accepted that the oversight arrangements in place in Ireland appeared less robust than in the United Kingdom.

8. Findings of Fact

8.1 The Supreme Court notes the repeated references in the jurisprudence of the CJEU to the object of combating serious crime. While specific reference is frequently made to organised crime and terrorism, the Supreme Court does not consider that the concept of

serious crime is confined to those categories, but also involves crimes such as the murder which is the subject of the criminal proceedings underlying this case.

8.2 The Supreme Court is aware that the detection of, in particular, certain categories of serious crime and the prosecution thereof is increasingly influenced by evidence such as that which was tendered in the criminal proceedings against Mr. D.

8.3 While organised crime and terrorism may well in some cases give rise to prior suspicion in advance of the commission of any particular specific crime, the type of serious crime with which these proceedings is concerned rarely involves any circumstances which could reasonably be known to investigating authorities and which could lead to prior suspicion. In the experience of the Supreme Court, some such cases have only been solved because of the availability of the type of data involved in these proceedings.

8.4 It seems to the Supreme Court that cases of the type described, of which this case is a particular example, frequently involve serious offences against women, children and other vulnerable persons. As already noted, in a significant number of such cases, it would not be possible to detect, let alone adequately prosecute, the perpetrator. In other cases, the ability to mount a successful prosecution would be severely impaired. Indeed, it should also be noted that, as in this case, telephony itself is often used in such cases for the purposes of grooming or otherwise exploiting vulnerable persons.

8.5 It seems particularly important to the Supreme Court to emphasise, therefore, that it is not possible to access that which has not been retained. If, on the basis of the argument put forward on behalf of Mr. D., it is not permissible to have "universal" retention of metadata, notwithstanding the robustness of any access regime, then it follows that many of these serious crimes against women, children and other vulnerable persons will not be capable of

detection or successful prosecution. Against that background, the Supreme Court has made the following findings of fact:-

(i) Alternative forms of data retention, by means of geographical targeting or otherwise, would be ineffective in achieving the objectives of the prevention, investigation, detection and prosecution of at least certain types of serious crime, and further, could give rise to the potential violation of other rights of the individual;

(ii) The objective of the retention of data by any lesser means than that of a general data retention regime, subject to the necessary safeguards, is unworkable; and

(iii) The objectives of the prevention, investigation, detection and prosecution of serious crime would be significantly compromised in the absence of a general data retention regime. The Court accepts and agrees with the evidence described in paras. 7.2-7.6 above.

8.6 The Supreme Court recognises that the question of admissibility of evidence in a criminal trial is a matter of national law. Nevertheless, the question of the validity of parts of the 2011 Act is a matter which can be raised in civil proceedings. Furthermore, the question of admissibility of evidence would itself have to be addressed in the light of a finding of invalidity (if any) and the precise nature, extent, rationale, scope and temporal effect thereof. Accordingly, the Court considers it is necessary to refer the following questions to the CJEU.

9. Questions referred

9.1 Is a general/universal data retention regime – even subject to stringent restrictions on retention and access – *per se* contrary to the provisions of Article 15 of Directive 2002/58/EC, as interpreted in light of the Charter?

9.2 In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive 2006/24/EC, and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive 2002/58/EC?

9.3 In assessing, in the context of determining the compatibility with European Union law and in particular with Charter Rights of a national measure for access to retained data, what criteria should a national court apply in considering whether any such access regime provides the required independent prior scrutiny as determined by the Court of Justice in its case law? In that context can a national court, in making such an assessment, have any regard to the existence of ex post judicial or independent scrutiny?

9.4 In any event, is a national court obliged to declare the inconsistency of a national measure with the provisions of Article 15 of the Directive 2002/58/EC, if the national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime?

9.5 If a national court is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive 2002/58/EC, as interpreted in the light of the Charter, is it entitled to limit the temporal effect of any such declaration, if satisfied that a failure to do so would lead to "resultant chaos and damage to the public interest" (in line with the approach taken, for example, in *R (National Council for Civil Liberties) v Secretary of*

State for Home Department and Secretary of State for Foreign Affairs [2018] EWHC 975, at para. 46)?

9.6 May a national court invited to declare the inconsistency of national legislation with Article 15 of the Directive 2002/58/EC, and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of the Directive 2006/24/EC issued by the CJEU on the 8th day of April, 2014?

Appendix I: The Irish Legislative Scheme

1. The Communications (Retention of Data) Act 2011 was enacted with the express purpose of giving effect to the 2006 Directive. Subsequent to the key events which took place in the main proceedings (i.e. the retention and accessing of Mr. D.'s telephony data), the Act has been subject to amending legislation. Insofar as the Act relates to these proceedings, however, its relevant provisions are set out below.

2. Section 1 of the 2011 Act defines "data" as "traffic data or location data and the related data necessary to identify the subscriber or user". Section 3(1) requires all service providers to retain, *inter alia*, the data described in Part 1 of Schedule 2 to the 2011 Act, for a period of two years. This is referred to as "fixed network telephony and mobile telephony data", which is described as data to identify the source, the destination, and the date and time of the start and end of a communication, the type of communication involved, and the type of

and the geographic location of the communications equipment used. The content of communications does not fall within this type of data.

3. Under ss. 4 and 5 of the Act, service providers must take specified measures to ensure the data is protected against unauthorised access. Under s. 4(2) of the 2011 Act, the Data Protection Commissioner is designated as the supervisory authority for the purposes of the Act.

4. Section 6 provides for the conditions under which a disclosure request may be made. Section 6(1) states:-

> "A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for—
>
> (a) the prevention, detection, investigation or prosecution of a serious offence,
>
> (b) the safeguarding of the security of the State,
>
> (c) the saving of human life."

5. It is s. 6(1)(a) which is relevant for the purposes of the proceedings brought by Mr. D. in the dispute under national law. A "serious offence" is defined in s. 1 of the 2011 Act as being one which is punishable by imprisonment for a term of 5 years or more, and also as those other offences listed under Schedule 1 to the Act. Section 6, which is not directly relevant for the purposes of these proceedings, confers a similar right of access on senior officers of the Army where the data is required for the purpose of safeguarding the security of

the State, and on officers of the Revenue Commissioners in respect of serious revenue offences. Section 7 of the Act obliges service providers to comply with such requests.

6. Under s. 9(1) of the 2011 Act, the Garda Commissioner must prepare and submit an annual report to the Minister for Justice and Equality in respect of the data specified in Schedule 2 that were the subject of all disclosure requests made under s. 6(1) during the relevant period. This report is intended to form part of the basis for a State report to the European Commission, pursuant to s. 9(8).

7. Section 10 of the 2011 Act sets out the complaints procedure which relates to the disclosure of data. Persons who believe that their data has been accessed in contravention of s. 6 of the Act may apply for an investigation into the matter. This investigation is carried out by a person holding the office of Complaints Referee, currently a serving Circuit Court judge, nominated under pre-existing legislation concerned with the interception of communications, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 ("the 1993 Act").

8. Separately, pursuant to ss. 11 and 12 of the 2011 Act, a judge designated under s. 8 of the 1993 Act is conferred with the power to review the operation of the provisions of the 2011 Act and to report on its operation to the Taoiseach. The designated judge has the power to investigate any disclosure request made, and to access and inspect any relevant document or record.

Appendix II: The Criminal Proceedings

1. Ms. O'H. disappeared from Dublin on 22 August 2012. Text messages which were backed up to her laptop gave rise to serious concern and were found to have originated from a phone which was registered in a false name ("the 474 phone"). The remains of Ms. O'H.

were not discovered until September 2013. Some days later, two further phones were recovered abandoned at a separate location. These were referred to in evidence as the "master" and "slave" phones, and examination of retained data made it clear that they had been used only for the purpose of communicating with each other. The content of text messages retrieved from these handsets (and not from any retained data) included certain personal details clearly relating to Ms. O'H. and indicated that she was in a relationship with the user of the "master" phone. The messages from these phones and the 474 phone also indicated that the relationship was with a man who had a taste for knife violence against women, who had killed a sheep and who had cut Ms. O'H. with a knife on a number of occasions.

2. Mr. D. was identified as a suspect in the investigation through the use of retained telephony data. The timing and geographical location of calls made by the "master" phone on one particular day in July 2012 led to the identification of Mr. D.'s car from motorway toll records. The locations of his home and place of work were consistent with the cell sites most frequently used by the "master" phone. The retained mobile telephony data generated by Mr. D.'s own phone (provided to him by his employer and referred to as "the 407 phone") was then accessed by investigating Gardaí, under the provisions of the 2011 Act. This data was examined with a view to establishing whether the movements of that phone correlated with the location data available in respect of the 474 phone and the "master" phone.

3. It should be noted that some other prosecution evidence, which was not the result of access to retained data, indicated a connection between the 407 phone and Ms. O'H., and also indicated a connection between Mr. D. and the 474 and "master" phones. However, the analysis of retained data relating to the 474 phone, the "master" and "slave" phones and the

407 phone, with the purpose of connecting them to Mr. D., was a significant feature of the case.

4. Mr. D. denies any connection with the 474 and the "master" and "slave" phones. Although he accepts that he can assert a privacy interest only in respect of his own phone, it is his case that all of the retained data was obtained in breach of EU law and he objects to the use of such data for the purpose of connecting him to the other phones. While he challenges the lawfulness of the 2011 Act as a matter of European Union law, there was no suggestion either at his criminal trial or in these proceedings that the specific manner in which the legislation was operated in the particular circumstances of this case was abusive or inappropriate. He does, however, make a challenge, in principle, to the adequacy of the safeguards relating to access.

5. These civil proceedings were commenced by Mr. D., in light of the judgment of the CJEU in *Digital Rights*, on the same day as the commencement of his criminal trial. In the course of that trial he challenged the admissibility of the telephony data by reference to both Irish constitutional law and Union law. The judge, following a hearing in the absence of the jury, ruled that the data was admissible. On 27 March 2015, Mr. D. was convicted by jury of the murder of Ms. O'H.

6. Mr. D. has appealed his conviction. In the grounds of appeal it is contended, *inter alia*, that the trial judge erred in admitting into evidence the telephony data in relation to his phone, and the other mobile phones attributed by the prosecution to him, on the basis that the statutory regime governing the retention of, and access to, such data was in breach of his rights under Union law. As mentioned, this appeal awaits to be heard by the Court of Appeal and will not progress further until this civil case is disposed of by the Supreme Court. As is clear from the above, Mr. D.'s interest in these plenary proceedings is that a finding in his

favour will enable him to argue in the criminal appeal that that his conviction cannot stand, because it was, in part, founded upon evidence that should have been excluded as having been unlawfully obtained. It will be open to him to argue that, following the ruling of the CJEU in *Digital Rights*, the investigators should not have been given access to the relevant data and that it was therefore inadmissible in evidence. However, the exclusion of evidence in a trial is a matter for the court of trial and the criminal appellate process. In the appeal currently before this Court, the only issue is whether the High Court was correct in determining that s. 6(1)(a) of the Communications (Retention of Data) Act 2011 is inconsistent with EU law.

SUPREME COURT

Appeal No. 18 of 2019

IN THE MATTER OF ARTICLE 267 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION AND IN THE MATTER OF A REFERENCE TO THE COURT OF JUSTICE OF THE EUROPEAN UNION

THE CHIEF JUSTICE

MR JUSTICE O'DONNELL

MR JUSTICE McKECHNIE

MR JUSTICE MacMENAMIN

MR JUSTICE CHARLETON

MS JUSTICE O'MALLEY

MS JUSTICE IRVINE

2015 No. 351 P

BETWEEN

G. D.

PLAINTIFF

AND

THE COMMISSIONER OF AN GARDA SÍOCHÁNA THE MINISTER FOR COMMUNICATIONS ENERGY AND NATURAL RESOURCES IRELAND AND THE ATTORNEY GENERAL

DEFENDANTS

ORDER DATED THE 25th DAY OF MARCH 2020
FOR REFERENCE TO THE
COURT OF JUSTICE OF THE EUROPEAN UNION PURSUANT TO

ARTICLE 267 OF THE TREATY

The Motion on the part of the Defendants pursuant to Notice of Appeal dated the 8th day of February 2019 by way of application for leave to appeal from the Judgment of the High Court (Ms Justice O'Connor) given on the 6th day of December 2018 and the Order made on the 11th day of January 2019 declaring that section 6(1)(a) of the Communications (Retention of Data) Act 2011 - insofar as it relates to telephony data as defined in Part 1 of Schedule 2 of the Act and which is retained on a general and indiscriminate basis as provided for in Section 3 of the Act - is inconsistent with Article 15(1) of Directive 2002/58/EC read in light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union and for an Order setting aside the said Judgment and Order having come on for hearing before this Court on the 16th 17th and 18th days of December 2019

Whereupon and having read the Determination of this Court dated the 28th day of May 2019 granting leave to appeal herein the said Notice of Appeal the said Judgment and Order of the High Court the documents therein referred to and the written submissions filed on behalf of the respective parties and having heard Counsel for the Defendants and Counsel for the Plaintiff

And Counsel for the Plaintiff having intimated that an application will be made to the Court at the conclusion of the Appeal for a recommendation that the State pay the costs of the Plaintiff including Solicitor and two Senior and one Junior Counsel in accordance with the Legal Aid - Custody Issues Scheme

IT WAS ORDERED that the case should stand for judgment

And the same having been listed for judgment on the 24th day of February 2020 in Waterford and having been then called on accordingly in the presence of said respective Counsel

And judgment having been delivered and the parties having been given an opportunity to make observations on a draft Order of Reference

And It appearing that the facts and proceedings are as set forth and included in the Judgment and the Order of Reference annexed hereto

And it further appearing to this Court that the determination of the issues between the parties on this appeal raise questions concerning the correct interpretation of certain provisions of European Union Law namely the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks

THE COURT HAS DECIDED TO REFER to the Court of Justice of the European Union pursuant to Article 267 of the Treaty on the Functioning of the European Union as set out in the said Judgment and Order of Reference the questions:

1. Is a general/universal data retention regime – even subject to stringent restrictions on retention and access – *per se* contrary to the provisions of Article 15 of Directive 2002/58/EC, as interpreted in light of the Charter?

2 In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive 2006/24/EC, and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to

access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive 2002/58/EC?

3 In assessing, in the context of determining the compatibility with European Union law and in particular with Charter Rights of a national measure for access to retained data, what criteria should a national court apply in considering whether any such access regime provides the required independent prior scrutiny as determined by the Court of Justice in its case law? In that context can a national court, in making such an assessment, have any regard to the existence of ex post judicial or independent scrutiny?

4 In any event, is a national court obliged to declare the inconsistency of a national measure with the provisions of Article 15 of the Directive 2002/58/EC, if the national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime?

5 If a national court is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive 2002/58/EC, as interpreted in the light of the Charter, is it entitled to limit the temporal effect of any such declaration, if satisfied that a failure to do so would lead to "resultant chaos and damage to the public interest" (in line with the approach taken, for example, in *R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, at para. 46)?

6 May a national court invited to declare the inconsistency of national legislation with Article 15 of the Directive 2002/58/EC, and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of the Directive 2006/24/EC issued by the CJEU on the 8th day of April, 2014?

AND IT IS ORDERED that the further hearing of this Appeal do stand adjourned until after the said Court of Justice of the European Union shall have given its preliminary ruling on the said questions or until further Order in the meantime

JOHN MAHON

REGISTRAR

THE CHIEF JUSTICE

Perfected this 25th day of March 2020