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/

GRAHAM DWYER

PLAINTIFF / RESPONDENT

AND

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

DEFENDANTS / APPELLANTS

Judgment of Mr. Justice Clarke, Chief Justice, delivered the 24th of February, 2020.

1. Introduction

1.1 The extent to which it is permissible for public authorities both to require private telephony service providers to retain certain data about communications and, potentially, to disclose that information to investigating and prosecuting authorities, has been a significant issue within the European Union for a number of years. In particular, a directive dealing with such matters, 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"), was found by the Court of Justice of the European Union ("CJEU") to be in breach of rights guaranteed by the Charter of Fundamental Rights of the European Union ("the Charter") and thus deemed invalid (see, *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*")).

1.2 Prior to the judgment in *Digital Rights*, Ireland had enacted the Communications (Retention of Data) Act 2011 ("the 2011 Act") which was intended to transpose the obligations of Member States under the 2006 Directive into Irish law. The 2011 Act governs the retention of metadata by service providers and access to such data by national authorities in Ireland including, in particular, by An Garda Síochána.

1.3 Indeed, it is worth noting that Ireland was brought to the CJEU by the European Commission arising out of its failure to transpose the 2006 Directive (see, *Commission v. Ireland* (Case C-202/09) [2009] E.C.R. I-203, ECLI:EU:C:2009:736) and was held by the Court to have failed to have fulfilled its obligations thereunder. The CJEU also subsequently rejected Ireland's challenge to the legal basis on which the 2006 Directive was enacted, which challenge was maintained on the grounds that the European Union

did not enjoy competence in the area of criminal investigation and prosecution (see, *Ireland v. Parliament & Council* (Case C-301/06) ECLI:EU:C:2009:68).

1.4 Subsequent to the annulment of the 2006 Directive in *Digital Rights*, questions emerged as to whether the 2011 Act was compatible with EU law. For the reasons set out in his judgment in these proceedings (*Dwyer v. Commissioner of An Garda Síochána & ors* [2018] IEHC 685), O'Connor J. granted a declaration that s. 6(1)(a) of the 2011 Act was inconsistent with Article 15(1) of an earlier EU 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"). The 2002 Directive had been purportedly amended by the 2006 Directive but, on the annulment of the 2006 Directive, the 2002 Directive reverted to its original form as a matter of course.

1.5 The factual circumstances giving rise to these proceedings concerned the trial of the plaintiff/respondent ("Mr. Dwyer") in respect of the murder of a Ms. O'Hara. In the course of that trial, reliance was placed by the prosecution on evidence which was said to link Mr. Dwyer to certain phones, to link him to telephony data which was said to identify the location at which those phones were on certain relevant occasions and, in respect of certain phones which were physically put in evidence, to link him to the content of certain communications which were found on those phones. As there is an appeal pending by Mr. Dwyer against his conviction, it is important to exercise considerable restraint in commenting on the facts of the case, save to the extent absolutely necessary to explain the specific issues which arise on this appeal. However, it is clear that the reason why Mr. Dwyer has maintained these proceedings is that it is intended that they will, if successful, form part of a contention at his criminal appeal that the relevant telephony data should not have been admitted in evidence and thus raise a question over the safety of his conviction.

1.6 As I understand it, no issue was raised at the criminal trial as to the manner in which the relevant telephony data was accessed by the investigating and prosecuting authorities, save to the extent that it is said that the entire legal basis on which that access was granted is invalid as a matter of European Union law. It follows that the argument which suggests that the relevant telephony data should not have been admitted in evidence and that his conviction is therefore unsafe first requires the establishment of that unlawfulness.

1.7 The defendants/appellants ("the State") have appealed to this Court against the finding of the High Court. The net issue for this Court is, therefore, confined to the question of the validity or otherwise of the 2011 Act, having regard to the 2002 Directive properly interpreted in the light of the Charter.

2. The Grant of Leave

2.1 The State obtained leave to appeal as a result of a determination of this Court (*Dwyer v. The Commissioner of An Garda Síochána & ors* [2019] IESCDET 108). The reasons for the grant of leave by this Court can be found in that determination.

2.2 In its application for leave, which was not opposed by Mr. Dwyer, the State suggested that the proceedings raised complex and novel questions of constitutional and EU law and would have significant implications for many others who are not parties to the case. The Court accepted that the question of the consistency of the provisions of the 2011 Act with EU law met the constitutional criteria for leave to appeal and leave was granted on the grounds set out in the notice of appeal appended to the State's application for leave.

2.3 On that basis, it is appropriate to turn in more detail to the issues which arise on this appeal.

3. The Issues

3.1 As indicated earlier, the sole ultimate issue which this Court has to determine concerns the validity of s. 6(1)(a) of the 2011 Act. That section provides as follows:-

> *"6.— (1) 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"*

3.2 However, certain other provisions of the 2011 Act are also relevant to this appeal. Section 6(1)(a) refers to "a serious offence", which is defined in s. 1 of the Act as one which is punishable by imprisonment for a term of 5 years or more and also as those other offences listed in Schedule 1 to the Act. Section 6(1)(a) also refers to "retained data". As the obligation on service providers to retain data also gives rise to an important issue on this appeal, it is necessary to refer to the provisions of the 2011 Act in that regard. Section 3 sets out service providers' obligation to retain data, and subs. (1) thereof provides:-

> *"(1) A service provider shall retain data in the categories specified in Schedule 2, for a period of 2 years in respect of the data referred to in Part 1 of Schedule 2…"*

3.3 The data referred to in Part 1 of Schedule 2 required to be retained is that "fixed network telephony and mobile telephony data" which is at issue in these proceedings. 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 geographic location of the communications equipment used. Section 5 of the 2011 Act, regarding service providers' access to data, provides:-

> *"5.— A service provider shall not access data retained in accordance with section 3 except—*
>
> *(a) at the request and with the consent of a person to whom the data relate,*
>
> *(b) for the purpose of complying with a disclosure request,*
>
> *(c) in accordance with a court order, or*

(d) as may be authorised by the Data Protection Commissioner."

3.4 As also noted earlier, the effect of the annulment of the 2006 Directive was to provide that the 2002 Directive should continue in force in its unamended form. In relevant part, its provisions are set out as follows. Article 1 of the 2002 Directive, headed "Scope and aim", provides:-

"1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

3.5 Article 3(1) provides that the 2002 Directive "shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". Article 4 sets out service providers' obligations in respect of safeguarding the security of their services. Article 5, headed "Confidentiality of the communications", provides:-

"1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

…

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with

Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."

3.6 Article 6(1) of the 2002 Directive, in relation to traffic data, states:-

"Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1)."

3.7 Article 9(1) of the Directive, which article was headed 'Location data other than traffic data', provides:-

"Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. …"

3.8 Finally, Article 15(1) of the 2002 Directive, which is particularly relevant for the purposes of these proceedings, provides:-

"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

3.9 The CJEU, as already noted, determined in *Digital Rights* that the 2006 Directive was inconsistent with EU law and, in particular, the Charter. The key passages from the judgment of the CJEU in *Digital Rights* are as follows:-

> *"24. It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.*
>
> *…*
>
> *37. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."*

3.10 Turning to assess the justification of this interference, the Court considered that such an interference did not adversely affect the essence of those rights guaranteed by Articles 7 and 8 of the Charter. It continued:-

> *"41. As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.*
>
> *…*
>
> *44. It must… be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest."*

3.11 The CJEU then considered the proportionality of the interference with these rights, ultimately concluding that by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter. Its reasoning in this regard is set out at paras. 51-66, which requires to be set out in full:-

> *51. As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.*
>
> *52. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).*
>
> *53. In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.*
>
> *54. Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).*
>
> *55. The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, S. and Marper v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35).*
>
> *56. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all*

means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57. *In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.*

58. *Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.*

59. *Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.*

60. *Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.*

61. *Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each*

Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62. In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63. Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64. Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65. It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66. Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data…"

3.12 Obviously the validity or otherwise of various national measures which predated the decision of the CJEU in *Digital Rights* came into question thereafter. In the first major case on that topic, *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 CJEU approached the question of the validity of national measures governing data retention in the light of the 2002 Directive, interpreted in accordance with the terms of the Charter, in the following passages:-

"102. Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 60).

103. Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an 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 (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 51).

104. In that regard, it must be observed, first, that the effect of such [national legislation at issue in the underlying request for a preliminary ruling], in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.

105. Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 57 and 58).

106. Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 59).

107. National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 54 and the case-law cited).

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."

3.13 In response to a further question referred, the CJEU set out the correct approach to be taken by national courts in determining whether national legislation satisfies the requirements of Article 15(1) of the 2002 Directive, read in light of Articles 7, 8, 11 and 52(1) of the Charter, with respect to the access of the competent national authorities to retained data, at paras. 118-123:-

"118. In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 61).

119. Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015, Zakharov v. Russia, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.

120. In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).

121. Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, Rijkeboer, C 553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraph 95).

122. With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 66 to 68).

123. In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the Digital Rights judgment, paragraph 68, and the judgment of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraphs 41 and 58)."

3.14 At least some aspects of the legal framework which now exists for assessing whether national measures in this area comply with the law of the European Union are now clear. The retention of and access to data engages the rights of those whose data is retained and, in particular, accessed. Although it may not breach the essence of those rights so that such interference with rights can be justified, nevertheless any justification must be significant.

3.15 In particular, it would appear that the underlying justification for any relevant regime must be the fight against serious crime, which would appear to include, but not be limited to, organised crime and terrorism. Thus, retention and access schemes which are designed to assist in the detection and prosecution of minor crime will not be justified.

3.16 In addition, it would appear that the regime which requires service providers to retain data and which allows access to that data must be robust. In respect of the retention of data, there is a dispute between the parties as to whether, properly interpreted, the jurisprudence of the CJEU is such that retention can ever be permissible to allow a requirement of what I might describe as the "universal" retention of data. I will shortly return to what precisely I mean by that term. This question gives rise to the first issue which arose on this appeal. The scheme which is to be found in the 2011 Act is limited in two ways. First, the scheme only provides for the retention of so called telephony data and does not provide for the retention of the content of communications transmitted by means of fixed network or mobile telephony. In practical terms, this means that the data retained can demonstrate when a communication occurred, the source of the communication and to whom it was directed, the type of communication involved, the type of communications equipment used and ordinarily can, at least to some extent, identify the location where the relevant communications device was at the relevant time, by reference to masts used in the communication system. That data does, therefore, allow the identification of the location of a phone at many times and can also identify communications which were transmitted and received by that phone. However, to repeat, the data retention required under the 2011 Act specifically excludes, by virtue of s. 2 thereof, the retention of the communication itself (such as the content of a digital message). In practical terms, this means that it is possible, to some reasonably accurate extent, to trace the movements of a phone and the fact of communications made by and with that phone, but not to determine the content of any such communications.

3.17 There is also a temporal restriction on the retention requirements of the 2011 Act. Section 3(1) requires all service providers to retain the type of data, which is relevant for the purposes of this appeal, as described in Part 1 of Schedule 2 to the 2011 Act, for a period of two years.

3.18 However, subject to the limitations just referred to as to the type of data retained and the period for which it is retained, there are no other restrictions on the data required to be retained by reference to the targeting of specific locations or groups of persons or the like, which targeting is mentioned in the judgment of the CJEU in *Tele2 Sverige*. It is in that sense that I use the term "universal" retention of data. The retention is limited as to the type of data which is retained and is limited as to the time for which it can be retained, but the data retained is not limited or targeted by reference to persons, locations or the like.

3.19 On that basis, there was a significant issue between the parties at the hearing before this Court as to whether such universal (untargeted) retention was ever permissible, notwithstanding that it is limited to telephony metadata only and is also temporally

limited, no matter how robustly the regime for access to such data might be safeguarded. Counsel for Mr. Dwyer argued that a proper interpretation of the jurisprudence of the CJEU leads to the conclusion that there can be no such universal retention requirement. Counsel for the State argued to the contrary. Clearly, if the argument put forward on behalf of Mr. Dwyer is correct, then the 2011 Act is inconsistent with EU law because it does require universal retention, in the sense in which I have used that term.

3.20 The second main area of dispute concerns the manner in which access is obtained. If, as the State argues, a broader approach to the retention regime has to be taken in order to determine whether it protected privacy rights in a proportionate manner, counsel for Mr. Dwyer submits that the access regime under the 2011 Act provides insufficient independent protection against inappropriate access. It was argued on behalf of Mr. Dwyer 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 Counsel for the State maintained that the 2011 Act established a detailed framework governing access to retained data.

3.21 It is clear from the judgment of the CJEU in *Tele2 Sverige* that assuming that a particular retention regime is permissible, then as a general rule, competent national authorities can only be granted access to the data thus retained subject to a prior review carried out either by a court or by an independent administrative body. The access regime which applies under the 2011 Act does not involve any application to a court but rather an internal application to a separate unit within the Security and Intelligence section of An Garda Síochána, the Telecom Liaison Unit ("the TLU"). This unit processes the disclosure requests sought by members of An Garda Síochána and acts as the single point of contact for the administration of all requests for telecommunications data from An Garda Síochána to communications service providers. The TLU supports the functions of the Detective Chief Superintendent of the Security and Intelligence section, who is responsible for the determination of all internal applications for the disclosure of retained data and who ultimately decides whether to issue a request for disclosure to the communication service providers under the provisions of the 2011 Act. The TLU and the relevant Detective Chief Superintendent operate independently of the investigatory functions of An Garda Síochána.

3.22 At the times relevant to the investigation which is under consideration in Mr. Dwyer's case, all internal applications for disclosure 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. The TLU and the Detective Chief Superintendent are required to ensure that the application complies with the requirements of the 2011 Act and further to verify the legality, proportionality and necessity of the disclosure request sought. 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, it was determined that service providers would not process requests for call related data that did not come through this process. An issue,

therefore, arises as to whether that regime provides a sufficiently independent process prior to the disclosure of the relevant data, with Mr. Dwyer arguing that it fails to meet the standard identified in the jurisprudence of the CJEU.

3.23 In a similar context, the State draws attention to certain other provisions of the 2011 Act which are said to provide further assurance that the scheme will not be abused. 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").

3.24 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 ascertain whether An Garda Síochána is complying with its provisions. In carrying out these duties, the designated judge has the power to investigate any disclosure request made, and to access and inspect any relevant document or record relating thereto. The judge may report on any matters concerning the operation of the 2011 Act to the Taoiseach as they consider appropriate.

3.25 Further, under s. 4(2) of the 2011 Act, the Data Protection Commissioner is designated as the national supervisory authority for the purposes of the Act. 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 by members of An Garda Síochána 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).

3.26 On the basis of the State's argument, it is said to be appropriate to look at the scheme governing access as a whole and it is further argued that, not least having regard to the additional oversight referred to, the scheme in its totality provides sufficient independent assurance that access will not be abused.

3.27 The second issue which arises is, therefore, as to whether the Irish access regime is consistent with the jurisprudence of the CJEU deriving from *Tele2 Sverige*.

3.28 A third issue arises as to the potential temporal effect of a finding that aspects of the 2011 Act are inconsistent with EU law. That question centres on whether, as a matter of European Union law, it is permissible for a national court which finds that a measure of national law is inconsistent with EU law to determine that the effects of any such finding should not be retrospective and indeed might, in particular circumstances, only come into play at some defined point in time in the future. The question is as to whether such a course of action is open to this Court in the event of a finding of inconsistency with EU law being made, together, of course, with the question of whether it would be appropriate, in

the circumstances of this case, to reach a conclusion to defer the effect of such a determination in the event that this Court has, as a matter of European Union law, the power to make such a decision.

3.29 The issue comes into particular focus in the context of this case, where Ireland had been required by the CJEU itself in substance to enact the 2011 Act in order to transpose the 2006 Directive and had failed in its attempt to persuade the CJEU that no proper legal basis existed for the 2006 Directive. The case, under this heading, made on behalf of the State is to the effect that any determination should not be retrospective and might indeed be prospective from a date in the future, not least precisely because Ireland had been required by the CJEU itself to enact the 2011 Act.

3.30 At least some of the issues earlier identified are to an extent dependent on the facts. The key assessment of the validity of a measure which undoubtedly impacts on rights but which may be justified in the pursuit of legitimate objectives comes down to a question of proportionality. The jurisprudence of the CJEU in that regard can be found in, for example, *Schaible* (Case C-101/12) EU:C:2013:661, where the Court was asked to assess the validity of provisions of Council Regulation (EC) No 21/2004, which imposed certain obligations on the keepers of sheep and goats in respect of their identification and registration, in Union law, in light of the freedom to conduct a business guaranteed under Article 16 of the Charter. In *Schaible*, it was recalled that the principle of proportionality requires that measures adopted by European Union institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question. In addition, where there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued. The Court held that the aim of the measures, being to prevent the spread of infectious diseases, constituted a legitimate objective in the public interest. Having considered the alternative means of identification proposed by the applicant in the main proceedings, the CJEU concluded that the measures implemented under Regulation No 21/2004 were appropriate for attaining that objective, that the contested obligations were necessary to achieve that aim and that the disadvantages resulting from those obligations were not disproportionate to that objective pursued by the Regulation.

3.31 That exercise clearly involves at least some factual questions concerning the extent to which a legitimate objective can be achieved by particular means and, in the context of a proportionality test, assessing the contribution which the measure concerned might make towards achieving that objective and the degree of interference with protected rights. It follows that it is necessary to say something about the evidence in this case which was directed towards those questions.

4. The Evidence

4.1 While the trial judge did not make many specific findings of fact in that regard, it was accepted by counsel at the oral hearing that, save in a number of minor respects which do not appear to me to be particularly relevant of this appeal, the evidence of the factual situation on the ground, so far as telephony metadata evidence being deployed in criminal

investigation and prosecution is concerned, was uncontroverted. In those circumstances, it seems to me that this Court is entitled to rely on that evidence for findings of fact.

4.2 The expert witnesses called on behalf of the State before the High Court emphasised the importance of telephony and internet data in the prevention, investigation and prosecution of serious crime. In the evidence of Mr. Anderson QC, former UK Independent Reviewer of Terrorism Legislation, examples were provided of the utility of retained data in the context of criminal investigations which have taken place in the United Kingdom, noting its capacity to assist in the identification of suspects and of premises of interest, in the tracing the movements of a suspect and in the indication of associations between individuals or groups of individuals. This historical data was acknowledged by the experts as being of particular significance in the investigation of terrorism, organised crime, and serious sexual offences, as well as playing an important role in the identification of the relevant elements of certain offences, such as premeditation or conspiracy. Further, it was stated that historical location data can be used to locate vulnerable individuals or those in emergency situations, or to support the alibi of an innocent person in an exculpatory fashion.

4.3 To illustrate the significance of this data, Mr. Anderson gave evidence that the investigation and prosecution of crime was significantly impeded following the annulment of legislation requiring mandatory data retention by the German Constitutional Court in 2010. Statistics provided by the German federal and state police forces to the European Commission in 2013 were to the effect that in 44.5% of the cases involving requests for retained traffic data, there were no other means of conducting the investigation.

4.4 The expert witnesses also gave evidence that they considered that there were no equally effective alternatives to a universal regime of data retention. The “quick-freeze” system, under which preservation orders relating to particular individuals can be served on service providers after those individuals came under suspicion, would have limited efficacy in the context of the investigation of crime, as the majority of data regarding the suspect’s conduct prior to their identification would be unavailable. The evidence of Mr. O’Callaghan, an expert radio engineer, was to the effect that the “look-back period” in which investigating authorities could obtain the historical data of a suspect under the quick-freeze system would extend at most to a week prior to the issuing of a preservation order. Further, this system would be of no utility in identifying persons who are unknown to law enforcement authorities at the time of the offence.

4.5 Further, the targeted retention of data was also said by experts to be of limited efficacy in circumstances where the identity and location of a target are not always known at the point when such data is generated. Such targeting would suffer from a lack of accuracy, as was detailed in the evidence of Mr. Anderson, as the retained data would be of no utility if a suspect is operating outside the targeted geographical area, for example, thus depriving national authorities of important strategic options in investigating serious crimes. The experts further doubted the operational feasibility 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.

4.6 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 combatting threats to state security from unlawful organisations such as the Irish Republican Army or hostile foreign intelligence agencies. This witness confirmed that access to fixed network data and mobile telephony data by members of An Garda Síochána has been and continues to be critical in the identification of suspects as well as the elimination of persons of interest. He further described a number of cases that could not have been resolved without the use of retained data. In such cases, data was accessed for the purposes of proving contact between suspects, tracking a route taken by a suspect, ensuring that CCTV footage was preserved, challenging an account given by a suspect or identifying a person not previously known to An Garda Síochána.

4.7 In the light of that evidence, I would propose that this Court make the following observations and findings of fact.

5. Observations on and Findings of Fact

5.1 I do note 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, I do 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.

5.2 I am satisfied that the evidence established 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. Dwyer.

5.3 While organised crime and terrorism may 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 are concerned rarely involves any circumstances which could reasonably be known to investigating authorities in advance and which could lead to prior suspicion. It is, in my view, the experience of the members of the Irish courts dealing with criminal matters that some such cases have only been solved because of the availability of the type of data involved in these proceedings.

5.4 It seems to me 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. In addition to the charge of murder of a vulnerable person, which is the subject of the underlying criminal proceedings involving Mr. Dwyer, cases involving the grooming of children can often require similar methods for investigation and prosecution. As already noted, in a significant number of such cases, it would not be possible to detect, let alone adequately prosecute, the perpetrator without access to

telephony data of the type with which this case is concerned. In other cases, the ability to mount a successful prosecution would be severely impaired.

5.5 It seems particularly important 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. Dwyer, it is not permissible to have "universal" retention of data, 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, I would suggest that the Court make the following findings of fact:-

(i) Alternative forms of data retention, by means of geographical targeting or otherwise, would be ineffective in achieving the objective of the prevention, investigation, detection and prosecution of at least certain type 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 objective 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. 4.2-4.6.

5.6 Against that legal and factual background, it is necessary to discuss the proper course of action for this Court to adopt.

6. Discussion

6.1 While it is clear from *Tele2 Sverige* that it is for national courts to assess whether national measures breach European Union law and, if so finding, to determine such measures invalid, it is also necessary to consider whether there are questions of European Union law which remain unclear but which require to be clarified in order that an answer can be given to the validity issue with which this Court is concerned. In that context, it is necessary to consider the interaction of privacy rights with the need to tackle serious crime.

6.2 It is, of course, the case that the Irish Constitution, in common with the European Convention on Human Rights ("the Convention") and the Charter, recognises significant privacy rights encompassing a right of privacy in relation to personal data. It has not been suggested to date (and, in my view, could not be suggested) that the separate identification of a right to protection of personal data in Article 8 of the Charter should lead to any divergent analysis of the issues involved when it is sought to challenge the introduction of evidence obtained under a statutory regime permitting retention of data generated by fixed and mobile telephony networks and internet usage.

6.3 The Charter itself recognises the possibility of processing of such data on a legitimate basis laid down by law. The analysis, whether under the Charter, the Convention or the Constitution, of any measure provided for by law permitting retention and access to such data is essentially similar. First, it is necessary to consider whether the measure affects a protected right. If so, it is necessary to determine whether any such interference pursues a legitimate objective. Next, and again if so, it must be determined whether the interference is no greater than is necessary to achieve the lawful object and is proportionate in so doing.

6.4 It is also the case that the Irish courts have very considerable experience, within the national legal order, of balancing important privacy rights with the requirement for the investigation and, if appropriate, prosecution of criminal offences. In so doing, the courts have subjected measures which might interfere with privacy rights to rigorous scrutiny. In that context, Irish courts dealing with criminal matters have also recognised that the rights of victims of crime form an important part of any overall assessment. In so doing, the Irish courts have drawn on Irish constitutional jurisprudence but also have had significant regard to the jurisprudence of the European Court of Human Rights ("the ECtHR").

6.5 However, the issue on this appeal concerns only the question of the validity of an Irish statute, the 2011 Act, having regard to Union law. The obligation of sincere cooperation between national courts and the CJEU, the differences of function and capacity in relation to obtaining evidence and making findings of fact, the allocation of competences and the principle of subsidiarity, all suggest that this Court should first consider whether the issues arising can be determined without the requirement to clarify any questions of Union law by means of a reference under Article 267 of the TEEU. In addition, even if persuaded that such a reference is required, this Court may take the course suggested by the CJEU, by setting out the reasons why it was considered necessary to make such a reference and also giving its own views on the issues to be considered in any reference. It is on that basis that I propose to consider the issues of Union law arising.

6.6 The analysis of the data protection regime implemented in Ireland under the provisions of the 2006 Directive has tended to treat the questions of retention and access as separate issues. It may be open to some doubt as to whether this is necessarily helpful or indeed truly possible. It is clear that the objective of retention is to permit access. It has no function otherwise. On the evidence adduced in this case, it is clear that the data retained in bulk is not itself related to any individual person holding rights under the Constitution, the Charter or the Convention. It is only when access is sought and obtained that it is possible to connect an individual to any specific retained data.

6.7 If it were possible to conceive of a situation in which it was simply impossible to ever access the data, then the argument that there would nevertheless be a serious breach of the individual's rights would be necessarily attenuated. It has been suggested that the fact of retention of universal data may give rise to vague feelings on the part of the individual that they are subject to surveillance even though individual surveillance would

not be possible without access to the data. In addition, any individual concerned must necessarily be aware of the fact both that data is generated and may be retained by operators for their own commercial purposes and may be available for lawful access during such period. If, however, that normal retention by service providers was the only interference with the right of protection of personal data then it would appear that any such intrusion would be capable of justification in the interests of investigation of serious crime. Such investigation, however, can only occur if access to the data is allowed. It is apparent, therefore, that a significant part of the proper concern with the retention of bulk undifferentiated data is the possibility of access (and identification), whether permitted (and if so, the terms of such permitted access) or unauthorised (and if so, the likelihood of such access and the range and extent of data to which access might be obtained). For these reasons, it may indeed be preferable to view retention and access together.

6.8 The consideration of these issues has, however, to date proceeded on a separate consideration of the question of universal retention as an interference with the right of data privacy followed by an analysis of the access regime. I, therefore, propose to adopt that course of action. It is clear that the retention of such data, even without the possibility of access or where any such access is on extremely restrictive terms, is an interference with a right to privacy in personal data. It is also clear that the objective of such retention is the investigation of serious crime. Such an objective is a lawful and permissible objective of considerable weight in any society governed by the rule of law.

6.9 In those circumstances, I will turn first to the position in Irish constitutional law. The State's obligation to vindicate, in the case of injustice done, the "life, person and good name" of a victim as a result of Article 40.3.2° of the Constitution was referred to by Hardiman J. in *A v. Governor of Arbour Hill Prison* [2006] IESC 45, [2006] 4 I.R. 88 at paras. 256 and 257, in the context of an application for relief under Article 40.4.2° of the Constitution, where the applicant had been convicted on a plea of guilty to a charge of a serious sexual offence against a minor under a legislative provision which had subsequently been declared unconstitutional. This obligation to vindicate victims' rights, Hardiman J. held, was a matter of high public policy which may be considered as a factor in favour of permitting "force and effect" to be given to orders made under a void statute.

6.10 In *The People (Director of Public Prosecutions) v. J.C.* [2015] IESC 31, [2017] 1 I.R. 417, this Court held that the determination of the admissibility of unconstitutionally obtained evidence was an exercise which required the balancing of the rights of the accused and the public interest in the lawful operation of our policing authorities against society's entitlement to secure the proper and legitimate conviction of those guilty of crime and the rights of victims to ensure that those who commit crimes against them are brought to justice where there is sufficient probative evidence to establish the guilt of the person concerned to the criminal standard (see, further, my judgment in that case at paras. 824-841). Similarly, in *Nash v. The Director of Public Prosecutions* [2015] IESC 32, this Court held that, in the assessment of prohibition of trial applications, the rights of the accused to a fair trial must be considered alongside the right of a victim of crime to have the

wrong done to them appropriately scrutinised in the context of a criminal trial. This balancing process was acknowledged in my judgment in those proceedings at para. 2.3, and by Charleton J. at para. 14 of his judgment, in which the entitlement of victims to "a fair investigation of the wrong done to them" was recognised.

6.11 As mentioned, the Irish courts have also drawn on the jurisprudence of the ECtHR in this regard. That case law has recognised the need to provide significant protection to the rights of victims in the criminal process. It is well established that Member States are subject to certain positive obligations to secure for individuals the effective enjoyment of their Convention rights. Under the doctrine of positive obligations, the ECtHR has recognised that States owe certain procedural obligations to victims of crime who have suffered an infringement of their Convention rights. Under Article 8, which guarantees the right to respect for private and family life, it has been held that a State's criminal law provisions in respect of grave acts, such as rape and sexual abuse of children, where fundamental values and essential aspects of private life are at stake, must provide practical and effective protection of a victim's rights (see, *X and Y v. the Netherlands* (App. No. 8978/80) (1985) 8 E.H.R.R. 235, at paras. 23-24, 27 and 30).

6.12 In *K.U. v. Finlan*d (App. No. 2872/02) (2009) 48 E.H.R.R. 52, the ECtHR held there had been a violation of Article 8 in circumstances where the applicant, a minor, was the subject of an advertisement of a sexual nature on an internet dating site and where the identity of the person who had placed the advertisement could not, however, be obtained from the Internet service provider due to the legislation in place at the time. It was held that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator. In respect of a State's positive obligations under Article 8 in respect of victims of crime, and vulnerable victims in particular, the ECtHR said the following:-

> *"46. … [T]he Court notes that the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and to bring him to justice. Here, the Court notes that it has not excluded the possibility that the State's positive obligations under Article 8 to safeguard the individual's physical or moral integrity may extend to questions relating to the effectiveness of a criminal investigation even where the criminal liability of agents of the State is not at issue (see Osman v. the United Kingdom, 28 October 1998, § 128, Reports of Judgments and Decisions 1998-VIII). For the Court, States have a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal law provisions in practice through effective investigation and prosecution (see, mutatis mutandis, M.C. v. Bulgaria, cited above, § 153). Where the physical and moral welfare of a child is threatened, such injunction assumes even greater importance. The Court notes in this connection that sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of*

their private lives (see Stubbings and Others v. the United Kingdom, 22 October 1996, § 64, Reports 1996 IV).

47. … It is plain that both the public interest and the protection of the interests of victims of crimes committed against their physical or psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice… and the victim to obtain financial reparation from him."

6.13 The ECtHR has also held that States have an obligation to conduct an effective investigation into alleged wrongdoing committed against victims of crime who have suffered infringements under Article 2, which protects the right to life (*Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* (App. No. 47848/08) (Unreported, European Court of Human Rights, 17 July 2014) at para. 147); Article 3, which prohibits torture and inhuman and degrading treatment (C*.A.S. and C.S. v. Romania* (App. No. 26692/05) (Unreported, European Court of Human Rights, 20 March 2012) at paras. 69-70); and Article 4, which prohibits slavery and forced labour, (*S.M. v. Croatia* (App. No. 60561/14) (Unreported, European Court of Human Rights, 19 July 2018) at paras. 59-60); even if the wrongdoing concerned has been inflicted by private individuals. The ECtHR has held that the investigation must be effective in the sense that it should, in principle, be capable of leading the establishment of the facts of the case and to the identification and punishment of those responsible. It has been held that, while the result of the investigation is not compulsory, the means employed are (*Eremia v. The Republic of Moldova* (App. No. 3564/11) (Unreported, European Court of Human Rights, 28 May 2013) at para. 51).

6.14 The issue in this case therefore becomes one as to whether that permissible objective (or, indeed, on one view the mandated objective) may be achieved by measures less intrusive of the right of privacy than a regime of universal retention of bulk undifferentiated data, subject to the possibility of subsequent access. It is contended that the universal retention permitted by the 2011 Act fails such a test because it is possible to achieve the permitted objective by less intrusive means and in particular by targeted retention <u>in advance</u>, whether by reference to individuals, groups, or geographic areas

6.15 This contention is troubling from the perspective of Irish constitutional law and the analysis which an Irish court would apply under the Constitution, the Convention and the Charter. First, it appears to be based on a hypothesis which is not supported by any evidence and is indeed contradicted by such evidence as has been adduced in these proceedings. Second, it is apparent that any question of retention of data in advance by reference to geographical criteria would itself involve questions of profiling and differential treatment of individuals on the basis of location and/or their association with others. Assuming, however, that such a course of action would be permissible, it would in principle be something quite different to the regime established by the 2011 Act and would be more intrusive of the rights of the individuals concerned, who themselves may have no necessary connection to any suspected or anticipated crime. Such measures, described as targeted retention, would almost inevitably involve not merely <u>retention</u> but

also access to relevant data, identification of the individual and normally access to the content of the communication concerned.

6.16 Most significantly, it is apparent, both as a matter of logic and as established by the evidence in this case, that any such measure cannot achieve the objective of permitting the investigation of serious crimes such as the subject matter of these proceedings, where there is no reason to suspect a particular individual or group in advance. The conclusion therefore that a regime of universal data retention in bulk is *per se* impermissible, irrespective of the terms of such retention or the conditions of access, would appear not to be a conclusion that the legitimate and important objective of investigating serious crime could be achieved by methods less intrusive of the rights of individuals, but rather a conclusion that the objective of investigating serious crime cannot justify the universal retention of bulk communications data however regulated or controlled. This is a value judgment but one not apparent from the Charter nor, it would appear, one which would be made either under the Convention or the Irish Constitution. In circumstances where the Charter refers to and embodies the common constitutional traditions of the Member States, it is arguable that it should not be interpreted in such a way as to impose such a value judgment on Member States at odds with their constitutional traditions, particularly in circumstances where Article 15(1) of 2002 Directive is permissive and does not require Member States to adopt any system of retention. Thus, a Member State whose traditions would lean against any system of universal retention is free to adopt such a course of action.

6.17 I would make one further comment on the observations in the jurisprudence of the CJEU already referred to above, to the effect that the retention of data without the registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance, thus impacting on the rights of those citizens to privacy. I do not disagree with those observations or seek to discount them in any way. However, the precise extent to which such matters may have such an effect on citizens may well vary from Member State to Member State, not least because of the different experiences within Member States of pervasive scrutiny on the part of police authorities. The question, however, is as to the weight to be attached to such matters and, in particular, the extent to which retention alone can give rise to a significant interference with the right to privacy (no matter how robust an access regime may be). I appreciate that, subject to such discretion as European legislation may confer on Member States (and having regard to the principle of subsidiarity now expressly provided for in Article 5(3) of the Treaty on European Union), Union law cannot have a different meaning in different Member States. However, it is at least open to significant argument that, when attempting to assess the weight to be attached to particular factors where that weight is not expressly determined either in the treaties or in European legislation, it may not be appropriate to look to those States which attach the highest or, indeed, the lowest weight to such matters, but rather that it is appropriate to take a broad view of the potentially differing positions that may pertain across the Member States. This is particularly so when it remains open to member States to choose a higher

standard of protection of the privacy rights involved and a correspondingly less effective regime of retention and access.

6.18 In assessing the extent to which a system of universal retention may be compatible with Union law, I would, of course, afford all due weight to the general interference with privacy which is involved in such a system. I would fully accept that such a system could not be justified by reference to the pursuit of objects which fall short of the prevention, detection and prosecution of serious crime, as identified in the jurisprudence of the CJEU as constituting objectives of general interest. However, in the light of the evidence tendered in these proceedings and of the findings of fact which I propose that this Court should make, it seems to me that significant regard would have to be attributed to the fact that many serious crimes against vulnerable people are most unlikely, on the undisputed evidence, to be capable of successful prosecution in the absence of a system of universal retention. In that context, I would consider that considerable weight must be attached to the undoubted rights of the victims of such crime, which rights will be impaired to a very significant degree indeed if it should prove impossible to detect or successfully prosecute the perpetrators of crimes against them.

6.19 I would suggest that the rights of such persons need to be kept very much in mind in determining any appropriate balance. If, therefore, I were called on to resolve the issue of Union law concerning whether a universal system of retention is, at least at the level of principle, permissible, I would hold that it is. To consider otherwise is to say that the very significant rights of the victims of serious crime, including many vulnerable victims, have to be set at nought to protect a privacy right which does not extend, in itself, to the revelation of any information concerning any citizen but rather only the retention of some limited information so that it may possibly be disclosed if truly required. However, the first issue which needs to be addressed concerns whether, as Charleton J. proposes in his dissenting judgment, this issue can finally be determined by this Court without making a reference to the CJEU under Article 267 of the TFEU.

6.20 I consider the views of Charleton J. on the facts to attract particular weight in this area, in light both of his very considerable experience as a criminal lawyer at the Bar who was involved in many significant cases and also in light of his very broad experience as a senior judge in this area. I would not necessarily disagree with any of the factual observations in relation to criminal investigation and prosecution which are to be found in his judgment. However, the question for this Court, it seems to me, is as to whether this issue can be resolved without determining a potentially unclear issue of Union law.

6.21 So far as the second aspect of this case is concerned, being the question of the access regime to be found in the 2011 Act, I would, were I deciding this matter myself, be inclined to conclude that the Irish regime does not provide adequate safeguards to meet the requirements of Union law in the light of the jurisprudence of the CJEU. There may well be some merit in decisions concerning the appropriateness or otherwise of access to retained data being made by persons with real experience in criminal investigation and prosecution. There is also the point that, in the Irish context, any investigating senior

member of An Garda Síochána will know that questions about the admissibility of evidence very regularly feature as significant issues in trials on charges of serious criminality. Such matters are robustly analysed. Thus, any member of An Garda Síochána who has a quasi-independent role in permitting access to retained data will know that his/her actions may come under intense scrutiny in the context of a criminal trial. In addition, it is necessary to at least pay some regard to the features of *ex post facto* scrutiny, both judicial and otherwise, which is contained in the Irish legislative scheme and to which reference has already been made.

6.22 However, notwithstanding those factors, it does not seem to me that the access system which is to be found in the 2011 Act is sufficiently robust to meet the standards identified by the CJEU in its jurisprudence. But again, a question remains as to whether it would be appropriate to make such a final determination without referring questions to the CJEU in respect of the proper approach to the assessment of the access regime. Furthermore, in the particular context in which the issue arises here, it may in any event be important to know the precise basis of any invalidity and its extent.

6.23 Finally, there are those questions concerning the temporal effect of any finding of invalidity. I would be inclined to the view that, in the light of the jurisprudence of the CJEU, there may well be a jurisdiction for this Court to determine that any finding of invalidity should not apply to events which occurred prior to that finding being made.

6.24 I would also be of the view that, should such a jurisdiction exist, it would be appropriate to exercise it in favour of thus limiting the temporal effect of any declaration of invalidity in all the circumstances of this case. I would do so not least because of the fact that it had appeared that Ireland was required, as a matter of Union law as determined by the CJEU in *Commission v. Ireland*, to introduce measures along the lines of the 2011 Act and, in substance, had actually introduced that legislation as a result of the determination of the CJEU in those proceedings.

6.25 However, again, the first issue is as to whether it is possible to make such a finding without an Article 267 reference. It follows that, under each of the three headings which I have sought to analyse, an initial question arises as to whether it is open to this Court, at this stage, to make a final determination on those matters without a reference.

6.26 However, in the context of that analysis, it seems to me to be impossible to say that Union law in certain relevant respects is clear. First, there is the debate between the parties as to whether the universal retention of metadata for a limited period of time is impermissible, irrespective of the robustness of any access regime. As noted earlier, if the arguments put forward on behalf of Mr. Dwyer in that regard are correct, then it follows that the regime set out in the 2011 Act must necessarily be found to be in breach of European Union law. On the other hand, if the arguments put forward on behalf of the State are correct, then wider considerations come into play. That question must be answered in order to make a final determination on the validity of the 2011 Act. It does not seem to me that the answer to that question is *acte clair*.

6.27 Second, there are issues concerning the nature of the Irish access regime. These questions include the extent to which it can be permissible for a separate body within a police force to provide the form of independent prior review which the CJEU has indicated is necessary for a valid access scheme. Second, there are questions as to the extent to which it is permissible, in the overall assessment, to have regard to the sort of measures of oversight on which the State places reliance. Assuming that the answer to the first question is such that this Court must then go on to consider the compatibility of the Irish access scheme with Union law, then those questions will have to be answered in order to reach a final determination on the validity of the 2011 Act. It again seems to me that the answers to those questions are not *acte clair*.

6.28 Third, there is the question, set out in some detail earlier in this judgment, as to whether this Court has the competence, in accordance with European Union law, to determine that the effects of any determination of invalidity of the 2011 Act should not be retrospective or might, indeed, only come into play at some defined stage in the future. Assuming that this Court comes to the conclusion that the 2011 Act is invalid by virtue of its inconsistency with European Union law, then it follows that this question too will have to be answered in order that a final decision be made as to the order which this Court should make. The answer to that question is not, in my view, *acte clair*.

6.29 It seems to me to follow from that analysis that each of those matters are questions of the law of the European Union which are not acte clair in the sense in which that term is used in the jurisprudence of the CJEU (see, *Srl CILFIT and Lanificio di Gavardo SpA v. Ministry of Health* (Case 283/81), [1982] E.C.R. 3415, ECLI:EU:C:1982:335). Each of those questions potentially arise in order that this Court can make a final decision on this appeal. I use the term "potentially" only in the limited sense that the second set of questions, concerning the nature of the Irish access regime, would solely arise in the event that the first question is answered in a manner which permits universal retention of data.

6.30 It follows that, in my view, these proceedings cannot be determined without a reference to the Court of Justice under Article 267 of the Treaty on the Functioning of the European Union. This Court is a court of final appeal and is obliged to make such a reference unless any relevant issues of European Union law which are necessary to the final determination of the appeal before it are *acte clair*. For the reasons set out in this judgment, I am not satisfied that the issues identified are *acte clair* and it seems to me to follow that a reference must be made.

6.31 The final question which arises concerns timing. At the oral hearing, counsel for the State mentioned that there were a number of Article 267 TFEU references currently before the Court of Justice in circumstances where additional clarity might be brought to some of the issues with which this Court is concerned. The cases are as follows: *Privacy International* (Case C-623/17) ECLI:EU:C:2020:5; *La Quadrature du Net and Others* and *French Data Network and Others* (Joined Cases C-511/18 and C-512/18) ECLI:EU:C:2020:6; *Ordre des barreaux francophones and germanophone and Others* (Case C-520/18)

ECLI:EU:C:2020:7; and *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* (Case C-746/18) ECLI:EU:C:2020:18.

6.32 However, while the opinion of the Advocate General has been delivered in each of those cases, the judgments of the Court are still awaited, and this Court further understands that there may be other references at an earlier stage of their progress through the procedures of the CJEU. On the other hand, this Court has to take into account the fact that Mr. Dwyer is currently in prison and that his appeal to the Court of Appeal against his conviction cannot properly be progressed until finality is brought to these issues. In those circumstances, it does not seem to me that it would be appropriate to wait until the CJEU has delivered judgment in the cases currently before it. It may be that greater clarity will be brought to some of the issues which this Court has to consider by the judgments which the CJEU will deliver in the cases referred to. It is even possible that clarity may be brought to all of the issues, such that the answers to the questions raised in the reference would no longer be required. However, there remains a significant possibility that at least some of the questions will nonetheless require to be answered in one form or another.

6.33 Having regard to the fact that Mr. Dwyer will remain in prison until his criminal appeal can progress, it seems to me to be appropriate to make a reference at this stage and to invite the CJEU to progress the reference through the expedited procedure, subject to a review being carried out after the CJEU has delivered judgment in those cases in respect of which the opinions of the Advocates General were delivered in January 2020, so as to ascertain whether all of the questions still require to be answered.

7. Conclusions

7.1 For the reasons set out in this judgment, I consider that there are three key areas of European Union law where the law is not *acte clair* but where clarification of that law is necessary to reach a proper decision on this appeal.

7.2 In simple terms, those areas are:-

(a) Whether a system of universal retention of certain types of metadata for a fixed period of time is never permissible irrespective of how robust any regime for allowing access to such data may be;

(b) The criteria whereby an assessment can be made as to whether any access regime to such data can be found to be sufficiently independent and robust; and

(c) Whether a national court, should it find that national data retention and access legislation is inconsistent with European Union law, can decide that the national law in question should not be regarded as having been invalid at all times but rather can determine invalidity to be prospective only.

7.3 In those circumstances, it seems to me that it is necessary that this Court refers questions to the CJEU under the provisions of Article 267 of the Treaty on the Functioning of the European Union. I propose that the Court should make such a reference in the terms set out in a separate document which I will circulate along with the delivery of this

judgment. I would propose that the parties be given a period of seven days to make observations on the text of that document. In that context, I would emphasise that the decision which I propose should be made by this Court today would definitively determine that there should be a reference and would also definitively determine the broad issues which require to be addressed in that reference. The observations which I propose that the parties should be permitted to make should, therefore, be confined to matters of detail or issues concerning the precise wording of the reference document. I would propose that the Court, having considered such observations as may be received within that timeframe, should then finalise the reference document and arrange for its transmission to the CJEU.