Unapproved
No redaction required

AN CHÚIRT UACHTARACH

THE SUPREME COURT

S:AP:IE2022:000110

Neutral Citation: [2024] IESC 22

BETWEEN

THE PEOPLE (AT THE SUIT OF THE DIRECTOR OF PUBLIC PROSECUTIONS)

Prosecutor/Respondent

AND

CAOLAN SMYTH

Accused/Appellant

JUDGMENT of Mr Justice Maurice Collins delivered on 17 June 2024

PRELIMINARY

1. The admissibility of unlawfully obtained evidence has been the subject of animated judicial discussion over many decades, going back as far as the decision of this Court in *People (DPP) v O' Brien* [1965] IR 142 ("*O'Brien*"), encompassing this Court's decisions in *People (DPP) v Shaw* [1982] IR 1 and *People (DPP) v Kenny* [1990] 2 IR 110 ("*Kenny*") and culminating in the recent decisions of this Court in *People (DPP) v JC* [2015] IESC 31, [2017] 1 IR 417 ("*JC*"), *Criminal Assets Bureau v Murphy* [2018] IESC 12, [2018] 3 IR 640 ("*CAB v Murphy*") and *People (DPP) v Quirke* [2023] IESC 20, [2023] 1 ILRM 445 ("*Quirke (No 2)*").

2. Even so, this appeal and the related appeal in *People (DPP) v Gary McAreavey*, in which the Court also gives judgment today, present a novel issue never previously considered by this Court, namely the admissibility in a criminal prosecution in the State of evidence obtained in breach of *EU* law.

3. The issue may be shortly stated, though it has generated significant controversy between the parties and has led to the intervention before this Court of the Irish Human Rights and Equality Commission (IHREC). It is whether mobile telephony traffic and location data retained and accessed in accordance with the provisions of the Communications (Retention of Data) Act 2011 ("*the 2011 Act*"), is admissible in evidence in a criminal prosecution in circumstances where the relevant provisions of the 2011 Act were subsequently found to be incompatible with EU law.

4. That the evidence at issue here was unlawfully obtained is not now in dispute. That follows from this Court's Order of 13 July 2022 in *Dwyer v Commissioner of An Garda Síochána.* That Order affirmed a declaration previously made by the High Court (O' Connor J) to the effect that section 6(1)(a) of the 2011 Act, insofar as it related to telephony data retained "*on a general and indiscriminate basis*" pursuant to section 3 of the Act, was inconsistent with Article 15(1) of 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 ePrivacy Directive*"), read in light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union ("*the Charter*"). The Order of 13 July 2022 followed from the judgment of the CJEU in *Dwyer* (Case C-140/20 *GD v Commissioner of An Garda Síochána* EU:C:2022:258) ("*GD*") given on 5 April 2022 on foot of an Article 267 reference made by this Court in March 2020.

5. Equally, there is no dispute that the issue of its admissibility is essentially a matter of Irish law.[1] But there is sharp disagreement as to how the breach of EU law involved is properly to be characterised and, in particular, whether it involved a breach of the Charter (as Mr Smyth and Mr McAreavey, supported by IHREC, contend) or merely some lesser form of illegality (as the Director contends). Largely as a consequence of that dispute, there is also disagreement as to what is the appropriate test to be applied to the assessment of admissibility and in particular whether or not the test is that set out

[1] EU law is, of course, an integral and fundamental part of Irish law but for the purposes of analysis, it is nonetheless convenient to distinguish between the requirements of EU law and the requirements of national (Irish) law.

in *JC*. On the premise that *JC* is the test, there is further and sharp disagreement as to how the *JC* test is to be applied here and, in particular, whether this Court can and should proceed to apply the *JC* test itself (as the Director contends) or whether (as Mr Smyth and Mr McAreavey, supported by IHREC, contend) that is properly a matter for a retrial. Finally, the parties sharply disagree as to whether, on the application of the principles set out in *JC* ("*the JC test*") the disputed evidence ought to be admitted or excluded.

6. This judgment addresses Mr Smyth's appeal only. But its reasoning and conclusions apply equally to the identical admissibility issue presented in Mr McAreavey's appeal. A further and distinct issue is presented in that appeal, namely what are the constituent elements of the offence created by section 7(2) of the Criminal Law Act 1997 (as amended) ("*the 1997 Act*")[2] and, in particular, whether it is sufficient to ground a conviction for such an offence for the prosecution to prove that the accused assisted the principal offender knowing or believing that offender to be guilty of "*some other arrestable offence*", without having to plead or prove what that "*other arrestable offence*" was. That issue is addressed in the separate judgment that I give today in the McAreavey appeal.

[2] Section 7(2) provides that "[w]here a person has committed an arrestable offence, any other person who, knowing or believing him or her to be guilty of the offence or of some other arrestable offence, does without reasonable excuse any act, whether in or outside the State, with intent to impede his or her apprehension or prosecution shall be guilty of an offence."

7. For the reasons set out in this judgment, I conclude that the disputed traffic and location data was properly admitted in evidence here. I accept the argument of Mr Smyth (and of Mr McAreavey) that the evidence was obtained in breach of the Charter. I also accept that it follows from the principle of equivalence that the admissibility of that evidence falls to be determined by the application of the *JC* test. In my view, in the particular circumstances here, and having regard to the nature of the breach, that exercise can and should be undertaken by this Court and does not require a retrial. Applying *JC*, the evidence was properly admitted. It was not taken in deliberate or conscious violation of any Charter rights of Mr Smyth or Mr McAreavey and the breach of rights involved derived from subsequent legal developments, specifically the striking down of the relevant provisions of the 2011 Act as incompatible with EU law. Insofar as the decision in *JC* contemplates any broader assessment, such assessment weighs decisively in favour of admissibility here in my view.

8. I would therefore dismiss Mr Smyth's appeal and affirm his conviction for attempted murder.

PROSECUTION, TRIAL AND APPEAL

10. Mr Smyth was charged and convicted of the attempted murder of James Gately. A number of shots were fired at Mr Gately at a petrol station on the Clonshaugh Road, Dublin 17 in the early afternoon of 10 May 2017. The attack was captured on CCTV and was also witnessed by other customers. The CCTV footage showed a black Lexus vehicle bearing the registration 08 D 51984 pulling up next to Mr Gately's vehicle. The Lexus had a single occupant. Mr Gately was struck by shots discharged from the Lexus. Fortunately for him, he had the foresight to be wearing a bulletproof vest and, as a result, he survived the attack, though he received a serious head injury that required surgery.

11. Mr Smyth was subsequently charged with the attempted murder of Mr Gately, as well as with possession of a firearm with intent to endanger life contrary to section 15(2) of the Firearms Act 1925 (as amended). The prosecution's case was that he was the driver of the black Lexus and the person who shot Mr Gately.

12. The prosecution case against Mr Smyth had several strands. A number of Gardaí gave evidence that they recognised Mr Smyth as the person driving the black Lexus from CCTV footage from the petrol station. That evidence was accepted by the Special Criminal Court (SCC) (Judgment, pages 9-11). The prosecution also led evidence as to the movements of the vehicle on 9 May 2017 (the day prior to the shooting) and 10 May 2017 (the day of the shooting). CCTV footage was produced from various sources and locations, some of which were said to be linked to Mr Smyth. The prosecution also

relied on analysis of traffic and location data relating to mobile phone/SIM card number 085-8208691 ("*the 691 number*").[3] The prosecution sought to attribute the 691 number to Mr Smyth based on a number of linkages in respect of which it adduced evidence. These linkages are meticulously analysed in the Judgment of the Special Criminal Court (SCC) (at pages 13-22) and led the court to conclude that it had been proved beyond reasonable doubt that Mr Smyth was the person using the 691 number at the relevant time.

13. The evidence relied on by the prosecution to establish that the 691 number should be attributed to Mr Smyth (that he was the user of that number) included traffic data relating to that number indicating multiple contacts between the 691 number and phones/numbers registered to Mr Smyth's brother and father (including 18 contacts with his brother's phone in the period after the shooting). That evidence was analysed in detail by the SCC (SCC Judgment, pages 13-20). The court also placed reliance on the fact that the location data for the 691 number disclosed movements/locations consistent with the location of Mr Smyth as disclosed by the CCTV footage from 9 and 10 May 2017 (SCC Judgment, pages 20-21). It was also, in the SCC's view, consistent with the movement of the black Lexus over those two days, including the periods before and after the shooting on 10 May 2017 (SCC Judgment, pages 22-45).

14. Traffic data relating to the 691 number was also relied on by the prosecution to establish contact between Mr Smyth and Mr McAreavey. The prosecution sought to attribute

[3] A mobile phone number is associated with the SIM (Subscriber Identity Module) card rather than with the handset. A SIM card can be used in different handsets. It therefore appears to be more accurate to refer here to the "*691 number*" rather than to the "*691 phone*".

another mobile phone/SIM card, number 085-8308773 ("*the 773 number*") to Mr McAreavey. Again, the prosecution led evidence linking the 773 number to Mr McAreavey, including the fact that the relevant SIM card was seized during a search of his house. The SCC was in no doubt that the 773 number should be attributed to Mr McAreavey. Traffic data disclosed a voice call between the 691 and 773 numbers on 9 May 2017 (the day before the shooting) and one text and five voice calls on the following day (though none after 14:28 when the vehicles had come together near Castlebellingham, Co Louth, close to the location where the burnt-out black Lexus was subsequently found). Location data associated with those calls was consistent with the two vehicles (the black Lexus being driven by Mr Smyth and the van being driven by Mr McAreavey) heading towards that location (SCC Judgment, 56-59).

15. The admissibility of the evidence of the traffic and location data relating to the 691 and 773 numbers was strenuously contested by Mr Smyth and Mr McAreavey. That data had been retained by the relevant mobile phone operators pursuant to section 3 of the 2011 Act and was accessed by the Gardaí on foot of requests made pursuant to section 6 of the Act in June and November 2017. Mr Smyth and Mr McAreavey argued that these provisions of the 2011 Act were incompatible with EU law, citing in support a number of significant decisions of the CJEU, including Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* EU:C:2014:238 ("*Digital Rights Ireland*") and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB* & *Watson* EU:C:2016:970 ("*Tele2*"). The effect of these decisions, so it was said, was to render unlawful the "*general and indiscriminate*" retention of traffic and location data and to require a system of prior review/authorisation before any such data could lawfully be accessed.

16. The objection to the evidence was directed particularly to the issue of access and it was advanced on the basis that Irish law – and in particular this Court's decision in *JC* – mandated its exclusion. No challenge was made to the *bona fides* of the individual Garda Superintendents and Chief Superintendents involved (though some inaccuracy in the available records was the subject of criticism), nor was it put to any of them that knew or ought to have known that the 2011 Act was contrary to EU law at the relevant time.[4] Rather than looking at individual members of An Garda Síochána, Counsel submitted that the focus should be on those who formulated policy – effectively the legislature – for failing to respond to EU law developments.[5] Counsel submitted that what was involved was something more than a mere illegality, involving a breach of the right of privacy protected by both the Charter and the Constitution.

17. At the time of the hearing before the SCC, the High Court (O' Connor J) had given judgment in *Dwyer* [2018] IEHC 685, [2019] 1 ILRM 461; [2019] IEHC 48, [2019] 1 ILRM 523. *Dwyer* involved a direct challenge to the 2011 Act on the grounds that it was incompatible with the ePrivacy Directive and/or the Charter. For the reasons set out in the judgments given by it, the High Court granted a declaration in the following terms:

[4] Transcript of 20 October 2020 (evidence of retired Chief Superintendent Maguire; statement of Superintendent Russell); transcript of 21 October 2020 (evidence of Det Chief Superintendent Richardson). All of these witnesses gave positive evidence that they believed the 2011 Act to be valid and of continuing effect.

[5] Transcript of 21 October 2020. The submissions of Mr Fitzgerald SC (counsel for Mr Smyth) on the admissibility issue were adopted by Mr Hartnett SC (counsel for Mr McAreavey).

"S.6(1)(a) of the Communications Retention of Data Act 2011, ("the Act"), insofar as it relates to telephony data, as defined in Part 1 of Schedule 2 of the Act, and which is retained on a general and indiscriminate basis as provided for in s.3 of the Act, is inconsistent with art.15(1) of 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, read in light of arts 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union."

18. The High Court placed a stay on that declaration pending appeal, this Court gave leave for a direct appeal to it and after hearing the parties, the Court (Charleton J dissenting) decided to make a reference to the CJEU pursuant to Article 267 TFEU: *Dwyer v Commissioner of An Garda Síochána* [2020] IESC 4, [2020] 1 ILRM 389. The questions referred are considered in more detail later but, in broad terms, they related to the effect of the ePrivacy Directive, interpreted in light of the Charter and the consequences that would follow if a national court was obliged to declare a national measure inconsistent with Article 15 of that Directive. That reference was pending at the time of the trial before the SCC (the timeline is rather confusing and for that reason a detailed chronology is appended to this judgment).

19. The SCC held that the traffic and location data was admissible, for the reasons set out in the ruling given by it (per the Presiding member, Hunt J) on 22 October 2020. At the start of that ruling, Hunt J noted that it was difficult to see how any privacy rights of Mr Smyth could be engaged in circumstances where he did not assert ownership of any

of the relevant phone numbers, SIM cards or handsets and where, if a link between him and those items was established by the prosecution, any privacy rights would not in any event extend to participation in criminal activity. He noted the development of the CJEU jurisprudence, including the annulment of Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications and amending Directive 2002/58/EC ("*the Data Retention Directive*") by the CJEU in in *Digital Rights Ireland*. He attached importance to the fact the crimes at issue had been committed less than 6 months after the CJEU's decision in *Tele2* which was the first time that the CJEU had addressed the question of the effect of the Charter and the decision in *Digital Rights Ireland* on national implementing measures. He noted that the State remained under an obligation to implement the ePrivacy Directive. Accordingly, the 2011 Act, pursuant to which the Gardaí had operated and which was presumed constitutional, retained a significant purpose.

20. Hunt J went on to refer to certain observations of Charleton J in his dissenting judgment in *Dwyer* and indicated some scepticism at any suggestion that the mere "*inert*" retention of data could be regarded as or equated to a system of mass surveillance. Any interference with the privacy rights of the accused was, in the SCC's view, very limited, as it involved access to targeted and limited categories of data which disclosed little if anything about the private lives of the accused. As against that, there was a very strong public interest in the investigation of the crimes here, which were serious crimes by any standard. That interest far outweighed any possible breach of a privacy right arising

from any failure to obtain advance judicial or other independent assent to obtaining access to the data here. To exclude the evidence would, in the opinion of the court, be entirely disproportionate. The court considered it useful to ask whether it was likely that, if there had been a requirement for prior judicial/independent authorisation, the outcome would have been different. The court did not think so – in the circumstances of this case it could not envisage any reasonable possibility of access being denied. Furthermore, the trial itself provided a full independent and effective safeguard against any potential abuse of privacy or data protection rights.

21. In the course of its ruling, the SCC noted that the admission of evidence obtained in breach of EU privacy rights remained a matter for national law, subject to respecting the principles of equivalence, effectiveness and adversarial opportunity. In the court's view, no breach of those principles had been alleged. The domestic privacy right relied on was not absolute or unqualified and, in the circumstances, had to yield to the interests of the State in investigating and prosecuting serious crime. The ruling makes no reference to *JC*.

22. The trial then proceeded, the disputed evidence was led by the prosecution and was clearly considered by the SCC to be probative and reliable and, as is evident from the SCC's judgment, it relied on that evidence in convicting Mr Smyth.

23. Mr McAreavey was charged with the offence of assisting an offender contrary to section 7(2) and 7(4) of the 1997 Act.[6] The prosecution's case against him was that, shortly after the shooting of Mr Gately, Mr McAreavey had driven in convoy with the black Lexus to a remote location near Newrath, Co Louth where the Lexus was burned out for the purpose of destroying evidence, using petrol that Mr McAreavey had bought earlier that day (which was also recorded on CCTV). This was reflected in the particulars of the offence set out in the indictment, which alleged that Mr McAreavey "*knowing or believing another person to have been guilty of an offence of attempted murder or of some other arrestable offence, did without reasonable excuse an act, with intent to impede his apprehension or prosecution, namely purchased petrol and assisted in the burning out of a vehicle used in the attempted murder."*[7] Mr McAreavey was tried on that charge alongside Mr Smyth.

24. For the reasons explained in the SCC's judgment, it was not satisfied that the evidence established beyond reasonable doubt that Mr McAreavey knew or believed that Mr Smyth was guilty of the offence of attempted murder. However, the court considered that the evidence established beyond any doubt that Mr McAreavey knew or believed that Mr Smyth had committed an arrestable offence of some description when he helped Mr Smyth to destroy the vehicle used in the shooting of Mr Gately. In the court's view, that was sufficient to ground a conviction under section 7(2) of the 1997 Act.

[6] Section 7(2) of the 1997 Act has already been set out above. Section 7(4) provides for the penalty that may be imposed on conviction.

[7] The form of indictment provided to the Court omits the words "*or of some other arrestable offence*". However, an amended indictment appears to have been served at the commencement of the trial and it is clear from the transcript that the indictment before the SCC included those words.

Appeal to the Court of Appeal

25. Mr Smyth and Mr McAreavey both appealed to the Court of Appeal and their appeals were heard together (the panel comprising the President and Edwards and Kennedy JJ) and addressed in a single judgment of the Court, delivered by the President on 28 July 2022 ([2022] IECA 182).

26. The judgment of the CJEU in *Dwyer* (*GD v Commissioner of An Garda Síochána*) was handed down after the hearing of the appeals but before the Court of Appeal gave its judgment.

Admissibility of the Mobile Phone Data

27. The Court of Appeal noted the "*central significance of the telephone evidence to the trial*". It was in that context that it addressed the arguments as to the admissibility of that evidence (para 12). It considered that the starting point for any discussion of this issue was the Data Retention Directive, which had been transposed into Irish law by the 2011 Act. It noted that in *Digital Rights Ireland* the CJEU had declared that Directive inconsistent with EU law as it failed to conform with the protection of privacy in Article 7 of the Charter. It noted that the breach of EU law arose on two grounds, the first being the blanket retention of data for a period of up to two years and the second being that access to data was not conditional upon prior authorisation by a court or independent

administrative body. The court noted that the real focus of attention had been on the access issue (para 17).

28. The court noted that the judgment of the CJEU in *Dwyer* was to the effect that the Irish regime did not comply with EU law, the focus being on the provision for blanket retention of data for a prolonged period and the fact that access to such data was not dependent on an application for an order to a court or independent tribunal (para 16).

29. The President summarised the arguments of the parties and cited extensively from the SCC's ruling on admissibility, stating that the court agreed with its approach and conclusions. The starting point for consideration of the issue was that it is for national courts to ascertain whether national measures breached EU law and to determine the consequences of that breach and, in particular, it was for the national courts to determine questions of the admissibility of evidence (para 25, citing paras 127 and 128 of the CJEU judgment in *Dwyer*).

30. The President noted that the crimes in issue here were committed less than six months after the CJEU judgment in *Tele2*. While in an "*ideal world*" there might have been a legislative response within that timeframe, any expectation to that effect would be "*unrealistic given the complexity of the issues at stake*". The actual request for data was both time-limited and focused. In terms of the timeline, it was also of significance that the shooting took place 18 months prior to the decision of the High Court in *Dwyer*. At the time of the investigation, the 2011 Act "*represented the statute law of the State and, accordingly, enjoyed a presumption of constitutionality*" (para 26). The court agreed with the finding of the SCC that any interference with privacy rights was "*limited in the*

extreme" and with its assessment that, in considering the extent of that interference, the fact that ownership of the phones had not been asserted was a relevant consideration (para 27).

31. Finally, as regards the absence of a requirement for prior authorisation from a judicial or independent administrative authority, the court found persuasive the point made by the SCC to the effect that, had such an authority been in existence and an application for access been made to it, it was inconceivable that access would have been refused. The court also agreed with the SCC that the public interest in the investigation of crime – part of which involved the rights of victims – comprehensively outweighed any limited privacy rights attached to the data that had been accessed. (para 28). Insofar as questions of admissibility of evidence were matters for the national court, the court was *"firmly of the view that the trial court did not fall into error in admitting the telephone evidence"* (*ibid*).

32. The Court of Appeal's substantive analysis of the admissibility issue makes no reference to *JC.*

The Section 7(2) Offence

33. The Court of Appeal effectively upheld the approach taken by the SCC as to the essential ingredients of the section 7(2) offence.

34. In the result, both appeals were dismissed.

APPLICATIONS FOR LEAVE AND DETERMINATION

35. Mr Smyth and Mr McAreavey then applied for leave to appeal to this Court. Both identified issues arising in relation to the admissibility of the mobile phone evidence said to be matters of general public importance. In addition, Mr McAreavey contended that an issue of general public importance arose in relation to the interpretation and effect of section 7(2) of the 1997 Act. The Director opposed leave in each case. However, by two Determinations dated 16 December 2022 ([2022] IESCDET 137 & 138), the Court granted leave. As regards Mr Smyth, the Court considered that the admissibility of the mobile phone evidence gave rise to issues of general public importance requiring consideration of the effect of, and the interaction between, the relevant provisions of the Constitution, the Charter, the ePrivacy Directive, the Data Retention Directive and the 2011 Act, as well as certain key judgments of the CJEU and this Court's decision in *JC*. As regards Mr McAreavey, leave was granted in relation to those issues and also in relation to the issue of the proper construction of section 7(2).

36. Subsequent to the grant of leave, IHREC applied for and was given leave to intervene as *amicus curiae* in relation to the admissibility issues.

THE ISSUES IN THE APPEAL

37. In the course of the case-management of the appeals, the parties agreed a statement of issues as follows:

"1. Noting that it is common case that the provisions of the Communications (Retention of Data) Act 2011 relating to

a. *General and indiscriminate retention of phone location and call data, such as that at issue in this case, for the purpose of the investigation of crime, and*

b. *access to such retained data for the purpose of the investigation of crime on the authorisation of a member of An Garda Síochána*

are, for the reasons stated in the judgment of the Court of Justice of the European Union of the 5th April 2022 in Case C-140/20 GD v Commissioner of An Garda Síochána ECLI:EU:C:2022:258 in breach of EU law, in what circumstances is such data admissible in evidence against an accused?

a) *Is the test for admissibility that set out in People (DPP) v JC [2015] IESC 31, [2017] 1 IR 417 or is some other test applicable?*

b) *In considering the admissibility of the phone location and call data here, what is the significance (if any) of the fact that neither appellant asserted or accepted ownership of the 691 phone or the 773 phone?*

c) *Did the Special Criminal Court err in admitting the phone location and call data in evidence in the circumstances here?*

2. Where in a prosecution under section 7(2) of the Criminal Law Act 1997 the prosecution fails to prove that the accused knew or believed that the principal offender was guilty of the arrestable offence proven to have been committed by that offender, does the reference to "some other arrestable offence" in that subsection require the prosecution to identify some specific "other arrestable offence" and to prove that the accused knew or believed that the principal offender was guilty of that specific offence in order to ground a conviction or is it sufficient for the prosecution to prove that the accused knew or believed that that person was guilty of an unspecified offence of sufficient gravity as to constitute an "arrestable offence"?"

38. The first set of issues is common to both appeals whereas the second issue arises only in the appeal of Mr McAreavey. This judgment deals with the admissibility issues. The section 7(2) issue is addressed in my separate judgment given today in Mr McAreavey's appeal.

THE PATH TO *DWYER*

39. Before engaging further with these issues, however, something more must be said about the legal developments leading to this Court's Order of 13 July 2022 in *Dwyer* affirming the High Court's declaration that the retention and access provisions of the 2011 Act were incompatible with EU law. That exercise is particularly relevant given the Appellants' contention that, long before the CJEU's decision in *Dwyer* (*GD*) and this Court's Order of 13 July 2022, it was or ought to been obvious to the State and to the Oireachtas that the 2011 Act regime was in breach of EU law.

The ePrivacy Directive

40. The ePrivacy Directive was adopted in July 2002. Its provisions require Member States to ensure the confidentiality of electronic communications and related traffic and location data and to prevent any interception, surveillance or storage of such communications or data without the consent of users (Article 5) and require the erasure or anonymisation of such data when it is no longer required for the transmission of a communication (Article 6(1)) though that is subject to several exceptions in the remainder of Article 6 relating to the service provider's requirements to retain the data for billing purposes, for marketing purposes or for the provision of value added services. Articles 5 and 6 are expressly subject to Article 15(1), which is set out below. Article 9 of the Directive deals with "*location data other than traffic data*". The inclusion of a special provision dealing with location data is explained in recital (35). Location data

that is processed to enable the transmission of communications is "*traffic data*" within the meaning of the Directive and therefore within the scope of Article 6. However, digital mobile networks may have the capacity to process location data which are more precise than is required for transmission purposes and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. Article 9 restricts the processing of such data, requiring either that it be anonymised or, with the consent of the user/subscriber, processed to the extent and duration necessary for the provision of the service.[8]

41. Article 15(1) of the ePrivacy Directive provides as follows:

> "*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*

[8] It follows that the data at issue in this appeal probably all comes within the definition of "*traffic data*."

of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

The Data Retention Directive

42. The Data Retention Directive was adopted in March 2006. Article 1(1) of the Directive expressed its essential purpose:

> *"This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order 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."* (my emphasis).

43. To that end, the Directive *obliged* Member States to adopt measures to ensure that specified data would be retained (Article 3) for not less than six months and not more than two years from the date of the relevant communication (Article 6). The data to be retained was specified in Article 5 of the Directive and included mobile phone traffic and location data. Such data was to be retained and stored securely (Article 7) and "*provided only to the competent national authorities in specific cases and in accordance with national law*" (Article 4).

44. Ireland unsuccessfully sought the annulment of the Directive following its adoption, on the ground that it had not been adopted on an appropriate legal basis: C-301/06 *Ireland v European Parliament and the Council of the European Union* EU:C:2009:68. Ironically – given subsequent developments - the State was itself successfully sued by the European Commission for failing to transpose the Directive into national law: Case C-202/09, *Commission v Ireland* EU:C:2009:736.

The 2011 Act

45. The Oireachtas then enacted the 2011 Act, the long title to which recited that its purpose was to give effect to the Data Retention Directive. Section 2 of the Act made explicit what was implicit in the Directive, namely that it had no application to the *content* of electronic communications. Section 3 of the Act imposed an obligation on service providers to retain the categories of data specified in Schedule 2. Mobile phone traffic and location data fell within Schedule 2, Part 1 and was thus subject to retention for two years. Section 5 of the Act prohibited the service provider from accessing such data other than in certain specified circumstances, including for the purpose of complying with a "*disclosure request*". Section 6(1) then provided that a member of An Garda Siochána not below the rank of chief superintendent could request a service provider to disclose retained data where that member was satisfied that the data was required for:

> *"(a) the prevention, detection, investigation or prosecution of a serious offence,*
>
> *(b) the safeguarding of the security of the State,*

(c) the saving of human life"

"*Serious offence*" was defined in section 1(1) of the 2011 Act as an offence punishable by imprisonment for a term of 5 years or more, though a number of identified offences which did not satisfy that criterion were also deemed to constitute such an offence. Section 6(4) stipulated that such a request for disclosure should be made in writing save in cases of exceptional urgency where the request might be made orally, in which case section 6(5) required the oral request to be confirmed in writing subsequently. Apart from the requirement that requests for disclosure should be made or confirmed in writing, the 2011 Act did not prescribe any procedural requirements in relation to such requests.

46. Prior to the enactment of the 2011 Act, provision had been made for the retention of communications data, and access to such data for the purposes of the prevention, detection, investigation or prosecution of crime (including but not limited to terrorism) or the safeguarding of the security of the State by Part 7 of the Criminal Justice (Terrorist Offences) Act 2005. The 2011 Act repealed Part 7.

Digital Rights Ireland

47. The decision of the CJEU (Grand Chamber) in *Digital Rights Ireland* in April 2014 invalidated the Data Retention Directive. That decision was given on foot of two Article 267 references, one from McKechnie J in the High Court and the other from the Austrian Constitutional Court. The CJEU was critical of both the retention and access

regimes mandated by the Directive. As regards *retention*, the court considered that the retention of the broad range of data provided for by the Directive constituted a particularly serious interference with the rights protected by Articles 7 and 8 of the Charter,[9] though it was not such as to adversely affect the essence of those rights (Judgment, paras 38 - 40). The court accepted that the fight against terrorism and serious crime was an objective of general interest (para 42) and that the data required to be retained was a "*valuable tool for criminal investigations*" and thus the retention of such data could therefore be considered to be appropriate for attaining that objective (para 49). Even so, however fundamental that objective was, the breadth of the retention regime went beyond what was necessary, entailing an interference with "*the fundamental rights of practically the entire European population*" without requiring any relationship between the data to be retained and a threat to public security (paras 56-59). As regards *access*, the CJEU considered that the Directive did not contain substantive and procedural conditions restricting access and "*[a]bove 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 …*" (paras 60-62).

[9] Article 7 provides that "*Everyone has the right to respect for his or her private and family life, home and communications.*" Save for the substitution of "*communications*" for "*correspondence*", Article 7 reflects Article 8(1) ECHR. Article 8 of the Charter – which has no equivalent in the ECHR – provides in para (1) that "*Everyone has the right to the protection of personal data concerning him or her*". The CJEU also relied on Article 52(1) of the Charter which provides that "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*"

48. Having regard to the foregoing, the court held that, by adopting the Directive, the EU legislature had exceeded "*the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter*" (para 69). It was not necessary to examine the validity of the Directive in light of Article 11 of the Charter (para 70).

49. In the aftermath of the *Digital Rights Ireland* judgment, national data retention regimes were subjected to challenge in many Member States, resulting in a significant number of further Article 267 references to the CJEU.

Tele2

50. In November 2015, the Court of Appeal of England and Wales made a reference which was one of the two references addressed in *Tele2* (the other being a reference from the Administrative Court of Appeal in Stockholm). Although the Court of Appeal doubted that the CJEU in *Digital Rights Ireland* had intended to lay down mandatory requirements for national legislation, it nonetheless considered it appropriate to refer a number of questions arising from a challenge to the (UK) Data Retention and Investigatory Powers Act 2014 (DRIPA): [2017] 1 All ER 62.

51. In July 2016, Advocate General Saugsmandsgaard Øe gave his Opinion in *Tele2*. He considered that general data retention obligations were, in principle, consistent with the ePrivacy Directive and that Member States were entitled to impose such a general

retention obligation, subject to compliance with strict conditions flowing both from Article 15(1) of the Directive and from the Charter (Opinion, para 116). He accepted that such obligations contributed to the fight against serious crime in that they enabled law enforcement authorities to "*examine the past*" by consulting communications data relating to persons suspected of connection to serious crime from the period before that person was identified as a suspect (paras 178-181). Any substantial limitation of the scope of a general data retention obligation could considerably reduce the utility of such a regime, not least because "*it is difficult, not to say impossible, to determine in advance what data may be connected with a serious crime*" and any such limitation could therefore result in the exclusion from retention of data that might have proved relevant in the fight against serious crime (para 213). Ultimately, however, he was of the view that the strict necessity for such a general retention obligation, and in particular the issue of whether any narrower retention regime would be as effective, was a matter for assessment by national courts (para 215). The proportionality of a general retention regime within a democratic society was also a matter for assessment by the national courts involving as it did "*mass interference*" with the data rights of most if not all of the population and which the Advocate General characterised as "*the power to catalogue the private lives of individuals and to catalogue a population in its entirety*" (para 246 – 262). Any retention regime had, in his view, to be accompanied by the safeguards identified by the CJEU at paras 60-68 of *Digital Rights Ireland*.

52. The CJEU (Grand Chamber) gave its judgment in December 2016. It first addressed the issue of whether the national legislation the subject of the references fell within the scope of the ePrivacy Directive, concluding that it did (Judgment, para 81). It then

addressed the substance of the Directive, emphasising those provisions – Articles 5, 6 and 9 – that were directed to the protection of the confidentiality of communications. While Article 15(1) enabled Member States to restrict the scope of the confidentiality principle, it did not permit the exception to become the rule as to do so would render Article 5 "*meaningless*" (para 89). Article 15(1) had to be interpreted in light of the fundamental rights guaranteed by the Charter and data retention regimes such as those at issue in the main proceedings raised questions relating to compatibility not only with Articles 7 and 8 of the Charter but also with Article 11.[10] Those rights had therefore to be taken into account in interpreting Article 15(1) of the Directive.

53. According to the court, general data retention provided a means of establishing a profile of the individual concerned, information that was no less sensitive, in terms of privacy, than the actual content of the communications (para 99) and the interference was "*very far-reaching*" and had to be considered to be "*particularly serious*" (para 100). That being so, only the objective of fighting serious crime was capable of justifying such a measure but such an objective, however fundamental, could not in itself justify the conclusion that general retention was necessary for the purpose of that fight (para 103). In explaining that finding, the CJEU observed that the effect of national legislation such as was at issue in the proceedings was to make retention the rule, where the system put in place by the Directive required retention to be the exception (para 104). Secondly, such legislation affected all persons using electronic communications services, including persons for whom there was no evidence capable of suggesting that their

[10] Articles 7 and 8 have been set out earlier, as has Article 52(1). Article 11(1) provides for freedom of expression and information in terms reflecting Article 10(1) ECHR.

conduct might have a link, however indirect or remote, with serious offences and also included persons whose communications were subject to obligations of professional secrecy (para 105). Furthermore, such legislation did not require there to be any relationship between the data to be retained and a threat to national security and, in particular, did not restrict retention to a particular time period, geographic area and/or a group of persons likely to be involved, in one way or another, in a serious crime or to persons who could, for other reasons, contribute to fighting crime through their data being retained (para 106). Accordingly, national legislation such as that at issue exceeded the limits of what was strictly necessary and could not be considered to be justified, within a democratic society, "*as required by Article 15(1) … read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter*" (para 107).

54. However, the court continued, Article 15(1) as so construed, did not prevent Member States from adopting legislation permitting "*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*" (para 108). In order to satisfy those requirements, national legislation must lay down clear and precise rules, requiring a connection between the data to be retained and the objective pursued and be based on objective criteria "*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*", including by the use of a "*geographical criterion*" where in one or more geographical areas there was a "*high risk of preparation for or commission of such offences*" (paras 109-111).

55. Finally, the Court turned to the issue of access. As regards the prevention, investigation, detection and prosecution of crime, only the objective of fighting serious crime was capable of justifying access to retained data. Clear, precise and binding rules governing access had to be laid down in national law and it was essential that access should, except in cases of urgency, be subject to prior review either by a court or an independent administrative body, made on the basis of a reasoned request by the competent national authority. Persons whose data was accessed had the right to be notified of such access as soon as such notification was no longer liable to jeopardise the relevant investigation.

56. In the operative part of its judgment (the *dispositif*) the CJEU ruled that Article 15(1) of the ePrivacy Directive "*read in the light of Articles 7, 8 and 11 and Article 52(1) of [the Charter]*" precluded national legislation "*which for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*" The same provisions precluded national legislation providing for access to the retained data "*where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime [and] where access is not subject to prior review by a court or an independent administrative authority.*"

57. The CJEU's judgment in *Tele2* does not engage in any real way with the observation made by the Advocate General in his Opinion that the general data retention regime provided an ability to "*examine the past*" that contributed to the fight against serious crime and that any substantial limitation of the retention regime could considerably

reduce its utility given that "*it is difficult, not to say impossible, to determine in advance what data may be connected with a serious crime.*" Furthermore, while the court stated that a "*targeted retention*" regime might, in principle, be compatible with Article 15(1), its judgment offered little by way of explanation of how, in practice, such a regime might operate usefully or effectively.

58. It is of some note that, when the matter went back to the Court of Appeal of England and Wales, the court declined to grant a declaration that the retention provisions of DRIPA were inconsistent with EU law. The court noted that that point had not been argued by the claimants, whose position had been that a general retention regime was permissible provided that it was accompanied by appropriate safeguards for access. In fact the claimants had expressly accepted that *Digital Rights* did not mean that only the data of suspects could be retained as such a restriction would be "*wholly impracticable*": [2018] QB 912, para 26(1).

59. In any event, it is evident that *Tele2* was not regarded as the last word on the compatibility of Member States' data retention and access regimes with the ePrivacy Directive or the Charter and was not understood as resolving for once and for all the lawfulness of general retention in all circumstances.

60. Thus:

- In **April 2016** (3 months after the decision in *Tele2*) the Provincial Court in Tarragona made a reference seeking the guidance of the CJEU as to the criteria

for assessing whether an offence was a "*serious offence*" for the purpose of assessing the justification of interference with the rights recognised by Articles 7 and 8 of the Charter (Case C-2017/16 *Ministerio Fiscal* EU:C:2018:788).

- In **October 2017**, the (UK) Investigatory Powers Tribunal made a reference concerning the lawfulness of the acquisition and use by the security services of traffic and location data (Case C-623/17 *Privacy International* EU:C:2020:790)

- In **July 2018**, the French Conseil d'État made two separate Article 267 references (Cases C-511/18 and C-512/18, *La Quadrature du Net* EU:C:2020:791). These raised a question as to whether general retention could be justified by reference to the right to security guaranteed by Article 6 of the Charter and the requirements of national security. The referring court rejected challenges to the French legislation based on Article 8 ECHR. Explaining its decision to make a reference in Case C-512/18, it stated that the "*usefulness of such a retention practice is therefore unparalleled with a view to investigating, establishing and prosecuting criminal offences*" (para 9).

- In **August 2018**, the Belgian Constitutional Court made a reference which also raised a question directed to the lawfulness of general retention for the purposes of criminal investigation, with specific reference to sexual offences against minors. (Case C-520/18, *Ordre des barreaux francophones et germanophone*). The questions referred invoked the "*positive obligations*" on States under *inter*

alia, Article 4 of the Charter (prohibition on torture and inhuman or degrading treatment).

- In **November 2018**, the Estonian Supreme Court made a reference relating to access (Case C-746/18 *Prokuratuur* EU:C:2021:152).

- In **October 2019**, the German Federal Administrative Court made two separate references raising a series of questions directed to the lawfulness of the German retention regime (Cases C-793/19 and C-794/19, *Spacenet* EU:C:2022:702).

61. This pattern of references was not random. In his Opinion in Cases C-511/18 and C-512/18, *La Quadrature du Net* EU:C:2020:6,[11] Advocate General Sánchez-Bordona acknowledged that the CJEU's case-law, and in particular its decision in *Tele2,* were a "*cause for concern for the authorities of some Member States because, in the view of those authorities, they have the effect of depriving them of an instrument they regards as necessary for the purposes of safeguarding national security and combatting [sic] crime and terrorism*". For that reason, he noted, some Member States were calling for that case-law to be "*repealed or refined*" (para 2). Such concerns, he noted, were pointed up in four references in the court which was delivering Opinions that day (15 January 2020), namely Case C-623/17 *Privacy International* EU:C:2020:790, *La*

[11] Which related only to the two French references as the Belgian reference was the subject of a separate Opinion, though the three references were subsequently joined for the purposes of judgment,

Quadrature du Net EU:C:2020:791 itself and Case 520/18, *Ordre des barreaux francophones et germanophone.*

Dwyer v Commissioner of An Garda Síochána – Supreme Court

62. In proceedings issued in January 2015, Graham Dwyer, who was being prosecuted for murder, issued proceedings seeking declarations (*inter alia*) to the effect that the provisions of the 2011 Act providing for the retention of, and access to, traffic and location data were inconsistent with the ePrivacy Directive read in light of Articles 7, 8, 11 and 52(1) of the Charter. In December 2018, the High Court (O' Connor J) held that sections 3 and 6(1)(a) of the 2011 Act were incompatible with the Charter ([2018] IEHC 685, [2019] 1 ILRM 461) but stayed a declaration to that effect pending appeal ([2019] IEHC 48. [2019] 1 ILRM 523). This Court gave leave for a direct appeal.

63. Having heard the parties, the Court (Charleton J dissenting) decided that it was necessary to refer a number of questions to the CJEU pursuant to Article 267 TFEU ([2020] IESC 4, [2020] 1 ILRM 389). The Court's reasons were set out in the judgment of Clarke CJ (O' Donnell, McKechnie, MacMenamin, O' Malley and Irvine JJ agreeing) given on 24 February 2020. The decision to make a reference, and the basis for it, are of crucial importance to the resolution of these appeals (so far as the admissibility issues are concerned) and the judgment of the former Chief Justice therefore requires detailed consideration.

64. Having discussed *Digital Rights Ireland* and *Tele2* and described the regime established by the 2011 Act, Clarke CJ addressed the evidence heard in the High Court. A number of witnesses had given evidence for the State as to the importance of telephony and internet data in the prevention, investigation and prosecution of serious crime. The witnesses included David Anderson QC (now KC), who had previously been the Independent Reviewer of Terrorism Legislation in the United Kingdom. The evidence – which was essentially undisputed – was that there were no equally effective alternatives to a universal regime of data retention. Both the "*quick freeze*" system (under which preservation orders relating to particular individuals could be served on service providers after those individuals came under suspicion) and the "*targeted retention of data*" were said to be of "*limited efficacy*". Evidence was also given that a number of cases could not have been resolved without the use of retained data (paras 4.2-4.6). On the basis of this evidence, the Chief Justice went on to make a series of very significant findings of fact: paras 5.1-5.5. These findings are substantially repeated in the Order for Reference to the CJEU and I shall set out them out in that context below.

65. Clarke CJ then referred to the fact that, in common with the ECHR and the Charter, the Irish Constitution recognised significant privacy rights, encompassing a right of privacy in relation to personal data. But such rights were not absolute. The effective investigation of serious crime was "*a lawful and permissible objective of considerable weight in any society governed by the rule of law*" (para 6.8). That was recognised in Irish constitutional law jurisprudence as well as the jurisprudence of the European Court of Human Rights (ECtHR). Indeed the ECtHR jurisprudence indicated that States have

an obligation to conduct an effective investigation into certain categories of crime (para 6.13, referring to Articles 2 – 4 ECHR). The issue therefore was whether that permissible/mandated objective could 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*" (para. 61.14). Clarke CJ was clearly unpersuaded by the contention that less intrusive means – such as "*targeted retention in advance*" – could achieve the permitted objective. In the first place, that contention appeared to rest on a hypothesis that was contradicted by the evidence. Secondly, targeted retention itself raised significant issues regarding profiling and differential treatment. Most significantly, both as a matter of logic and as established by the evidence, any targeted retention measure could not achieve the objective of permitting the effective investigation of serious crimes "*where there is no reason to suspect a particular individual or group in advance*" (para 6.16). Thus any conclusion that the regime of universal data retention was impermissible *per se*, regardless of the terms of retention or conditions of access, necessarily rested on a "*value judgment*" that "*the objective of investigating serious crime cannot justify the universal retention of bulk communications data however regulated and controlled*" (para 6.16). Such a value judgment was not one apparent from the Charter nor, it would appear, one which would be made under either the ECHR or the Constitution. Given that the Charter referred to and embodied the common constitutional traditions of the Member States, the Chief Justice thought it arguable that it should not be interpreted so as to impose such a value judgment on Member States at odds with their constitutional traditions, particularly as Article 15(1) of the ePrivacy Directive was merely permissive and did not require any Member State to adopt any system of retention (para 6.16).

66. While not discounting the observations of the CJEU to the effect that general data retention could generate a feeling of being subject to "*constant surveillance*", Clarke CJ suggested that the extent to which such matters might affect citizens may vary from Member State to Member State, not least because of their different historical experiences. It might be appropriate not to look to the States which attached the highest or lowest weight to such matters but instead to take a broad view, particularly when it was open to Member States to choose a higher standard of protection (and a correspondingly less effective regime of retention and access) (para 6.17).

67. While all due weight had to be given to the general interference with privacy which a system of general retention involved, significant regard had to be given 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*". Having referred to the weight to be given to the rights of the victims of serious crime, rights which would be "*impaired to a very significant degree*" should it prove impossible to detect or successfully prosecute the perpetrators of the crimes against them, Clarke CJ continued:

> "*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." (my emphasis).

68. As regards the issue of access, Clarke CJ stated:

"*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."

69. A further issue that arose related to the temporal effect of any finding of validity, Clarke CJ being inclined to the view that, in light of the jurisprudence of the CJEU, the Court

could determine that any finding of invalidity should not have retrospective effect and that, if such a jurisdiction existed, it would be appropriate to exercise it (paras 6.23-6.24).

70. None of those issues were, in the Chief Justice's view, *acte clair* (paras 6.26-6.29) and it followed that a reference to the CJEU was necessary (para 6.30).

71. In his judgment, Charleton J gave two concrete examples of high profile and very serious crimes which illustrated the utility of the general data retention regime in the investigation and prosecution of crime. A prior authorisation regime would not have solved those crimes: geographic targeting would have involved "*mere guesses*" (para 8). In his view, a reference to the CJEU was not required, for two distinct reasons. One related to the issue of EU competence in the area of criminal justice. The other was that, in his view, issues of the proportionality of a legislative measure infringing on rights should be resolved by national courts. In his view it could not be "*part of European law that collection of data in an inert way and subject to serious criminal sanction for breach of protections, as provided for in Irish law and practice, offends human rights under the Charter or legislation*" (para 11). In Charleton J's view, there was sufficient evidence before the court to allow it to apply the four-stage test established by *acquis communautaire*.[12] That was *a* "*national task*" (para 13-14). It is evident from the thrust

[12] Namely whether (i) the measure pursues a legitimate goal; (ii) it is suitable to achieve that goal; (iii) it is the least restrictive measure available in order to achieve the aim equally well as the measure chosen and (iv) the competing interests have been balanced correctly.

of his judgment that Charleton J was of the view that the impugned provisions of the 2011 Act satisfied the four-stage test and were therefore compatible with EU law.

72. The Order for Reference (perfected on 25 March 2020) set out the following under the heading "*Findings of Fact*":

> *" 8.1 The Supreme Court notes the repeated references in the jurisprudence of the CJEU to the object of combating serious crime. While specific reference is frequently made to organised crime and terrorism, the Supreme Court does not consider that the concept of serious crime is confined to those categories, but also involves crimes such as the murder which is the subject of the criminal proceedings underlying this case.*
>
> *8.2 The Supreme Court is aware that the detection of, in particular, certain categories of serious crime and the prosecution thereof is increasingly influenced by evidence such as that which was tendered in the criminal proceedings against Mr. [Dwyer].*
>
> *8.3 While organised crime and terrorism may well in some cases give rise to prior suspicion in advance of the commission of any particular specific crime, the type of serious crime with which these proceedings is concerned rarely involves any circumstances which could reasonably be known to investigating authorities and which could lead to prior suspicion. In the experience of the Supreme Court, some such cases have only been solved because of the availability of the type of data involved in these proceedings.*

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

8.5 It seems particularly important to the Supreme Court to emphasise, therefore, that it is not possible to access that which has not been retained. If, on the basis of the argument put forward on behalf of Mr. [Dwyer], it is not permissible to have "universal" retention of metadata, notwithstanding the robustness of any access regime, then it follows that many of these serious crimes against women, children and other vulnerable persons will not be capable of detection or successful prosecution. Against that background, the Supreme Court has made the following findings of fact:

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

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

(iii) The objectives of the prevention, investigation, detection and prosecution of serious crime would be significantly compromised in the absence of a general data retention regime.

The Court accepts and agrees with the evidence described in paras. 7.2-7.6 above."

The evidence described at paras 7.2 – 7.6 of the Order of Reference was the evidence led by the State in the High Court as to the significant value of the general data regime in the investigation and prosecution of serious crime, the adverse impact on the effectiveness of An Garda Síochána if that system of general data retention was no longer available and the limited utility of any alternative data retention regime. Reference was also made in those paragraphs to evidence as to the inappropriate use of the term "*surveillance*" to describe the storage of "*inert*" data.

73. The questions referred by this Court were as follows:

"'(1) Is a general/universal data retention regime – even subject to stringent restrictions on retention and access – per se contrary to the provisions of Article 15 of[the ePrivacy Directive], interpreted in the light of the Charter?

(2) In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to [the Data Retention Directive], and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have

regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of [the ePrivacy Directive]?

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

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

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

Home Department and Secretary of State for Foreign Affairs [2018] EWHC 975 [(Admin)], at paragraph 46)?

(6) May a national court invited to declare the inconsistency of national legislation with Article 15 of [the ePrivacy Directive], and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of [the Data Retention Directive] issued by the [judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238)]?'"

74. I attach particular importance to the clear statement in question (4) that the court had "*concluded, on all the evidence available, that [general data] retention is both essential and strictly necessary to the achievement of the objective of combating serious crime*". That aptly summarises the analysis and conclusions of Clarke CJ and the Court. In effect, this Court carried out the assessment identified by the Advocate General in *Tele2,* on the basis of the detailed evidence heard in the High Court, and concluded that any narrower retention regime would not be effective and that a general retention regime was necessary and proportionate.

75. So far from it being clear to this Court in *Dwyer* that the general retention regime provided for in the 2011 Act was incompatible with EU law, all seven members of the Court considered that such a regime, at least as it related to the investigation and prosecution of serious crime, was in principle permissible as a matter of EU law. Charleton J clearly considered that the issue was so clear as not to require the Court to make a reference to the CJEU. While the remainder of the Court took a different view on the issue of a reference, they were, nonetheless, of the view that a general retention regime was permissible in principle: para 6.19 of Clarke CJ's judgment. In arriving at that position, the Court had careful regard to the CJEU's decisions in *Digital Rights Ireland* and *Tele2*.

76. As to the issue of access, the majority of the Court leant to the view that the 2011 Act lacked adequate safeguards to satisfy the requirements of EU law. Even so, the Court did not regard the position as clear.

77. In his dissenting judgment in this case, Hogan J refers to this Court's decision in *Dwyer* but, in my respectful view, does not give it sufficient weight. The views expressed by the Court, particularly its view that a general retention regime was in principle permissible for the purpose of combatting serious crime, cannot properly be dismissed as mere "*judicial dicta*" that are not "*directly in point*." They were the considered views of the highest court in the State which were entitled to significant weight in the judicial dialogue to which Hogan J refers and which must also be given significant weight when assessing whether reliance on the 2011 Act in 2017 can objectively be characterised as "*reckless*" or "*grossly negligent*." If it had appeared to this Court that the retention

and/or access provisions of the 2011 Act were clearly incompatible with EU law, the Court would have been duty-bound under the EU Treaties to grant a declaration to that effect forthwith. But that is not how matters appeared to the Court.

La Quadrature du Net, Privacy International and Prokuratuur

78. The CJEU gave judgment in *La Quadrature du Net* and *Privacy International* on the same day (6 October 2020) while judgment in *Prokuratuur* was given in March 2021.

79. In its judgment in *La Quadrature du Net*, the court (Grand Chamber) declared that the importance of the objective of safeguarding national security went beyond that of the other objectives referred to in Article 15(1), including the objectives of combatting crime in general, even serious crime, and of safeguarding public security and thus was, in principle, capable of justifying measures entailing more serious interferences with fundamental rights than might be justified by such objectives (para 136). Thus, according to the court, Article 15(1) did not, in principle, preclude a legislative measure permitting the retention of traffic and location data of "*all users of electronic communications services*" for a "*limited period of time*" provided that "*there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat .. to national security which is shown to be genuine and present or foreseeable.*" (para 136). Even a measure that was "*applied indiscriminately*" to all users of electronic communications services was, in principle, justifiable on grounds of national security (*ibid*), though any such measure would have to be limited and time and subject to various other safeguards.

80. As regards measures providing for the "*preventative retention*" of traffic and location data for the purposes of combating crime and safeguarding public security, the court took a very different view. Notwithstanding the importance to be attached to those objectives, they were not capable of justifying the "*general and indiscriminate retention*" of such data (para141-142). Even the positive obligations that might arise under Articles 3, 4 and 7 of the Charter, relating to the establishment of rules to facilitate effective action to combat criminal offences, could not have the effect of justifying interference as serious as that entailed by retention of traffic and location data of practically the entire population "*without their being a link, at least an indirect one, between the data of the persons concerned and the objective pursued*" (para 145). Those (lesser) objectives could, however, justify the "*targeted retention*" of traffic and location data. Persons identified as posing a threat to public or national security could be targeted (para 49) or data could be retained on the basis of a geographic criterion, targeting areas of high crime or places particularly vulnerable to the commission of serious crimes, such as airports, stations or tollbooth areas (para 150). The CJEU also endorsed "*expedited retention*" of data (the "*quick freeze*" procedure referred to by this Court in *Dwyer*) (para 160 and following).

81. Two other aspects of the Grand Chamber's judgment in *La Quadrature du Net* warrant notice. First, the court articulated a principle that access to traffic and location data retained in accordance with a measure taken under Article 15(1) of the ePrivacy Directive could be justified only by the particular public interest objective for which the service providers were directed to retain that data (para 166). It followed that data

lawfully retained on national security grounds was accessible only for national security purposes and could not be accessed for the purposes of combating crime, even serious crime (a restriction reiterated by the CJEU in *GD*).

82. Second, in Case C-520/18 the Conseil d'État had asked whether it could apply a provision of national law empowering it to limit the temporal effects of any declaration of illegality in respect of provisions of national law found to be incompatible with Article 15(1), read with the Charter. The Grand Chamber held that it could not, as to maintain the effect of national law in such circumstances, even temporarily, would undermine the primacy and uniform application of EU law (para 217-200). However, the court went on to address the issue which it perceived as underlying the question, namely whether EU law precluded the use, in criminal proceedings, of information and evidence obtained as a result of the general and indiscriminate retention of traffic and location data in breach of EU law. The Grand Chamber's answer to that question was repeated in *Prokuratuur* and is referred to further below.

83. *La Quadrature du Net*'s holding that general retention of traffic and location data may, in principle, be justified by reference to the objective of safeguarding national security was a significant development in the jurisprudence. There was no suggestion of any such qualification or exception in *Tele2*. Furthermore, in so holding, the Grand Chamber departed from the advice of the Advocate General.[13]

[13] Opinion of Advocate General Sánchez-Bordano. paras 119-123 & 155(1).

84. Even so, the CJEU's acceptance in *La Quadrature du Net* that national security is different did not save the legislative regime at issue in *Privacy International* which provided for the bulk transfer of traffic and location data from service providers to the security and intelligence services, which retained the data and had free access to it. That, the court concluded, exceeded what was permissible under Article 15(1), read in light of Article 4(2) TEU and Articles 7, 8, 11 and Article 52(1) of the Charter (para 81).

85. The questions referred in *Prokuratuur* related to access rather than retention. The CJEU (Grand Chamber) emphasised that access to traffic and location data could be justified only for the purposes of combatting *serious* crime or preventing *serious* threats to public security (para 35). An issue of admissibility of evidence also arose, which the CJEU addressed in the same terms as in *La Quadrature du Net*.

GD v Commissioner of An Garda Síochána – Opinion of the Advocate General

86. Advocate General Sánchez-Bordano gave his Opinion in *Dwyer (GD*) on 18 November 2021. Aspects of its language are surprising and it is evident that the Advocate General was impatient of the fact that (as he put it) this Court had "*insisted*" on maintaining its request for a preliminary ruling notwithstanding the judgments in *La Quadrature du Net*, *Privacy International* and *Prokuratuur* (Opinion, para 7). As the Opinion states, when asked whether it was continuing with its request for a ruling following the judgment in *La Quadrature du Net*, this Court had replied that the type of case

underlying the proceedings in *Dwyer* differed significantly from the type of situations which underlay the proceedings giving rise to that judgment. The Advocate General characterised that reply as "*particularly laconic*". However, the burden of the reply seems very clear to me - in sharp contrast to the references in *La Quadrature du Net* (and the earlier references in *Digital Rights Ireland* and *Tele2*), the proceedings in *Dwyer* arose from an actual criminal investigation and prosecution in respect of a very serious criminal offence. Furthermore – and critically – the reference was made on the basis of detailed factual findings which, it was reasonable to expect, would be central to the CJEU's consideration of the questions referred and in particular to the question of whether general retention was justified for the purpose of combatting serious crime. In the event, any such expectation was to be confounded.

87. In his analysis, the Advocate General accepted that the court's case-law had led to a "*more rigorous and stricter regime*" than that which followed from the case-law of the ECtHR in relation to Article 8 ECHR[14] but, he said, Article 52(3) of the Charter did not prevent EU law from providing more extensive protection even in respect of corresponding rights (para 38). In his view, it would be to misapply *La Quadrature du Net* to apply the statements made in that judgment about national security to offences, including serious offences, which do not threaten national security but rather public security and other interests protected by law. Measures addressing these different categories could not have the same scope or else that distinction between them would be rendered meaningless (para 43). Having referred to the measures that were

[14] The two regimes appear now to have converged: see the very recent decent of the ECtHR (First Section) in *Škoberne v Slovenia* (Application 19920/20).

permissible for the purposes of combatting serious crime (expedited and targeted retention), the Advocate General concluded his analysis by rejecting the suggestion made by the Commission (supported by "*many of the governments which entered an appearance*") that "*serious crime*" should be regarded as a *tertium genus* and treated (as regards the scope of permissible retention) in the same way as national security (paras 49-56).

88. A feature of the Advocate General's analysis of the retention issue is its lack of any real engagement with this Court's factual findings. These are accurately summarised (paras 17-18) but do not otherwise feature in the Opinion. Nowhere does the Advocate General confront the fact (as found by this Court) that traffic and location data is frequently decisive for the detection and prosecution of certain categories of serious offence, that the objective of the retention of data by any lesser means than that of a general data retention regime is unworkable and that the objectives of preventing, investigating, detecting and prosecuting serious crime would be "*significantly compromised*" in the absence of a general data retention regime. As already observed, all appear to be matters that are not simply relevant, but fundamental, to any assessment of whether a general retention regime is, in principle, justifiable for the purpose of combatting serious crime. That was certainly the view of this Court in *Dwyer*.

89. As regards access, the Advocate General noted that access was not subject to prior review by a court or independent authority but was instead at the discretion of a Garda officer of a certain rank. It was for the referring court to examine, in light of the decision

in *Prokuratuur*, whether such an officer had the status of an "*independent authority*" and the nature of a "*third party*".

90. As regards the possibility of limiting the effects of a declaration of incompatibility, the Advocate General referred to *La Quadrature du Net* and expressed the view that there were no reasons to delay the effects of the judgment which would follow from finding that the 2011 Act was inconsistent with EU law.

GD v Commissioner of An Garda Síochána – Grand Chamber

91. The judgment of the Grand Chamber follows closely its analysis in *La Quadrature de Net*, emphasising that the general retention of traffic and location data constituted a serious interference with the rights guaranteed by Article 7 and 11 of the Charter that was not limited or remedied by the fact that access to such data was regulated in a manner that fully respected the court's case-law (para 47). While those rights were not absolute, any interference with them had to be proportionate. As regards the objectives that might justify a measure taken under Article 15(1), there was a "*hierarchy among those objectives*", with the objective of safeguarding national security being of greater importance than the other objectives, including the objective of combatting crime, even serious crime and of safeguarding public security (para 57).

92. As for the European Commission's submission that "*particularly serious crime*" could be treated in the same way as a threat to national security, the court considered that "*criminal behaviour, even if of a particularly serious nature , cannot be treated in the*

same way as a threat to national security" (para 63). As the Advocate General had observed, that would involve the creation of an "*intermediate category*" between national security and public security (which, it seems, the court did not support). The court emphasised that its case-law did not preclude legislative measures that provided for targeted retention of traffic and location data, the general retention of IP addresses, the general retention of data relating to civil identity of users, as well as expedited retention (para 67). All of these measures are then addressed in some detail. As regards measures providing for targeted retention and expedited retention, the court thought that this Court's order for reference showed a "*narrower understanding of the scope of those measures*" than was indicated by the case-law. Targeted retention could be based on targeting persons suspected of being a threat to national or public security or of involvement in crime or and/or on the basis of using a geographic criterion. It was also "*possible*" that other objective criteria might be considered but it was for the Member States, not for the court, to identify those criteria (para 83) and, in any event, the fact that it might be difficult to provide "*a detailed definition of the circumstances and conditions under which targeted retention may be carried out*" was not a reason for Member States, by turning the exception into the rule, to provide for the general retention of traffic and location data (para 83). The judgment also discusses expedited retention at some length. These various measures could be combined. All, however, were subject to the requirement of proportionality (para 93) and in that context the court recalled that, while the fight against serious crime was indeed "*of the utmost importance*" and its effectiveness might depend to a great extent on the use of "*modern investigatory techniques*", that objective, however fundamental it might be, did not "*in itself*" justify a measure providing for the general and indiscriminate retention of all

traffic and location data (para 94). Even the positive obligations of Member States could not have the effect of justifying the serious interference with rights entailed by legislation providing for general retention of such data, relating to practically the entire population "*in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued*" (para 95). In fact, the objective of fighting serious crime does not even justify accessing traffic and location data retained for national security purposes (paras 96-100).

93. As regards access, the court's analysis relied extensively on its earlier decision in *Prokuratuur.*

94. As to the question of imposing temporal limits on any declaration of incompatibility, the court largely relied on its analysis in *La Quadrature du Net*. As regards the effect of such a declaration on the admissibility of evidence against GD in the criminal proceedings against him, the court referred to *HK v Prokuratuur* from which it followed that "*admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness*" (para 127).

95. The operative part of the judgment (the *dispositif*) is in the following terms:

> *"1. Article 15(1) of 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 (Directive on*

privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data. However, that Article 15(1), read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for

– *the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;*

– *the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;*

– *the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and*

– *recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the*

expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data, which have been retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.

3. EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of the Charter of Fundamental Rights. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of

procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

96. The judgment of the Grand Chamber did not engage with the findings of fact made by this Court in the order for reference or directly address this Court's conclusion, based on the evidence heard in the High Court, that general retention was "*both essential and strictly necessary*" to combat serious crime. However, it seems clear from the court's analysis and conclusions that, ultimately, it considered that the interests of Member States in combatting even the most serious crimes (and the interests of the victims of such crimes and their families in seeing such crimes effectively investigated and punished) must yield to the privacy interests of users of electronic communications services. If (as this Court found as a fact) the objectives of preventing, investigating, detecting and prosecuting serious crime would be "*significantly compromised*" by the absence of a general retention regime, and if perpetrators of serious crimes went unpunished as a result, that is, it appears, a price that must be paid by Member States and their citizens to vindicate those privacy interests. That was so, it appears, regardless of what safeguards might be put in place to maintain the security of the data retained and to regulate and restrict access to such data and even if those safeguards complied in every respect with the requirements identified by the CJEU in its caselaw. That is so, even though the categoric distinction drawn by the court between national security on the one hand and serious crime/public security on the other, and the implications of that distinction for the lawfulness of general data retention, is far from obvious from the language of Article 15(1) of the ePrivacy Directive or of the Charter and appears to be highly contestable as a matter of principle.

97. That was, it appears, the value-judgment ultimately made by the CJEU. If so, it is evident that it was and is a judgment that is not shared by many Member States, who are of course the actors with responsibility for, and actual experience of, criminal law enforcement. The Article 267 reference procedure constitutes an important "*judicial dialogue*" between the CJEU and the national courts but it is difficult to avoid the conclusion that the dialogue here has been rather one-sided.

98. Be that as it may, the judgment in *GD* of course binds this Court and must be fully respected and sincerely implemented. It was on the basis of that judgment that this Court dismissed the appeal from the decision of the High Court and affirmed the declaratory order made by O' Connor J. But the decision ultimately rendered by the CJEU does not deprive this Court's decision in *Dwyer* of all effect. The views expressed by this Court in the decision to make a reference are also entitled to respect and are not retrospectively nullified by the CJEU's judgment in *GD*.

Subsequent CJEU cases

99. Before leaving the CJEU jurisprudence, further reference should be made to Joined Cases C-793/19 & C-794/19 *Spacenet* EU:C:2022:702, in which, once again, both Advocate General and Grand Chamber struggled to explain how permissible targeted retention measures might actually be effective or useful in combatting serious crime. That is a significant deficiency, given the emphasis placed by the court in *GD*, and once again in *Spacenet*, on the availability of such measures as mitigating the negative effects

of the unavailability of general retention (in the face of the evidence-based findings of this Court in *Dwyer* that such measures were not in fact effective). The court has now effectively said that it is a matter for the Member States to identify permissible targeted measures and that, even if there is difficulty in doing so, that does not in any event justify the adoption of a general retention regime: paras 112 & 113.

100. Finally, there is the very recent and significant CJEU decision in Case C-470/21 *La Quadrature du Net* EU:C:2024:370. That was another reference from the Conseil d'État, directed to whether Article 15(1) of the ePrivacy Directive, read in the light of the relevant provisions of the Charter, precludes national legislation allowing an administrative authority with responsibility for protecting copyright and related rights against internet infringement, access to "*civil identity data*" corresponding to IP addresses, in order to identify infringers and take action against them, without that access being subject to prior review by a court or independent administrative body. Following the oral hearing before the Grand Chamber, the Grand Chamber requested that the case be referred to the Full Court. The Full Court re-opened the oral procedure and Advocate General Szpunar delivered a second Opinion in September 2023, expressing the view that EU law did not preclude such legislation. The Full Court recently gave its decision on the reference. That decision is complex and significant. For present purposes, perhaps its principal significance is that it further illustrates that the law in this area is still developing. It is also notable for the court's emphasis on the importance of effective criminal investigation and on the fact that, absent access to the data, there would be a "*real risk of systemic impunity*" not only for copyright infringement but for other offences committed online or "*facilitated by the specific*

characteristics of the internet": paras 116-119. The criminality at issue in *La Quadrature du Net* – infringement of copyright – was clearly of a much lesser order than the serious crime at issue in *Dwyer*. The data at issue was also less sensitive – though, as the court noted, in certain circumstances it could allow "*precise conclusions to be drawn about the private life of the IP address holders*" (paras 110-111). In the result, the court upheld the lawfulness of France's graduated response regime, subject to the safeguards identified in its judgment, including the need for review by a court or independent administrative body (which may be partially but not entirely automated) at the third and final stage of the graduated response procedure (paras 141-151).

THE ADMISSIBILITY ISSUES

The Law Governing the Issue of Admissibility

101. This issue is relatively straightforward. Admissibility is governed by Irish law, subject to the principles of equivalence and effectiveness. That was stated in express terms by the Grand Chamber in paragraph 127 of its judgment in *GD* and reiterated in the *dispositif*.

102. The judgment in *GD* refers back to *Prokuratuur* where the issue is addressed at somewhat greater length, as follows:

> "*41 Finally, given the fact that the referring court has before it a claim that the reports drawn up on the basis of the traffic and location data are inadmissible, on the ground that Paragraph 111 of the Law on electronic communications is contrary to Article 15(1) of Directive 2002/58 as regards both retention of and access to data, it should be noted that, as EU law currently stands, it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed criminal offences, of information and evidence obtained by general and indiscriminate retention of such data contrary to EU law (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18,*

C-512/18 and C-520/18, EU:C:2020:791, paragraph 222) or by access of the national authorities thereto contrary to EU law.

42 The Court has consistently held that, in the absence of EU rules on the matter, it is for the national legal order of each Member State, in accordance with the principle of procedural autonomy, to establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar situations subject to domestic law (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 223 and the case-law cited).

43 As regards the principle of effectiveness in particular, it should be noted that the objective of national rules on the admissibility and use of information and evidence is, in accordance with the choices made by national law, to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences. That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence (judgment of 6 October

2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 225).

44 In deciding whether to exclude information and evidence obtained in contravention of the requirements of EU law, regard must be had, in particular, to the risk of breach of the adversarial principle and, therefore, of the right to a fair trial entailed by the admissibility of such information and evidence. If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and that is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement. Therefore, the principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority thereto in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 226 and 227)." (again, my emphasis).

103. The reference to "*the risk of breach of the adversarial principle*" in para 44 of *Prokuratuur* refers back to the CJEU decision in Case C-276/01 *Steffensen* EU:C:2003:228 and, through it, to the decision of the ECtHR in *Mantovanelli v France* (1997) 24 EHRR 370. Neither *Mantovanelli* nor *Steffensen* was concerned with any issue of the admissibility of illegally obtained evidence and their relevance in this context is quite unclear.[15] *Mantovanelli* involved a claim of medical negligence arising from the death of the applicants' daughter following a series of surgeries and skin grafts on her hand, the applicants' case being that an excessive amount of a particular anaesthetic (halothane) had been administered to her. The applicants applied for the appointment of an expert but that application was refused. Subsequently, the court appointed an expert who interviewed five persons from the hospital, including the surgeon and anaesthetist. In breach of the applicable rules, the applicants were not given notice of those interviews and thus had no opportunity to cross-examine the personnel involved or examine files reviewed by the expert. The expert's report (which relied on the interviews and the files he had reviewed which had not been seen by the applicants) exonerated the hospital and the court dismissed the action. An appeal court dismissed the applicant's appeal on the basis that, although the report was produced in an irregular manner, the court below was not bound to order its removal from the case file or direct that a new report to be prepared. In any event – so the appeal court said – the applicants had had an opportunity to challenge the report but had raised no objections to its findings or assessment.

[15] See the discussion in Panzavolta et al, "Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union" (2022) 26 *International Journal of Evidence and Proof* 199-222 ("*Panzavolta*") at 204-205.

104. The ECtHR found a breach of Article 6(1) ECHR. The breach was not the admission of evidence obtained in breach of provisions of national law – the court reiterated that the ECHR does not lay down rules of evidence as such or exclude the admission of such evidence as a matter of principle. That was a matter for the national courts to assess.[16] Nonetheless, the court concluded that the proceedings were not fair as required by Article 6(1). The expert's report pertained to a technical field that was not within the judge's knowledge and was therefore likely to have a "*preponderant influence*" on the court's assessment but the applicants were not able to comment effectively on the report by reason of being excluded from the interviews and from examining documents: at para 36.

105. *Steffensen* was similarly concerned with an infringement of the adversarial principle in circumstances where the right of a food manufacturer to obtain a "*second opinion*" on the compliance of its foodstuffs with food standards had been denied. The CJEU (Third Chamber) cited *Mantovanelli* as authority for the principle that Article 6 ECHR does not lay down rules on evidence as such (para 75) and also for the principle that fairness requires that parties be given a real opportunity to comment effectively on evidence

[16] See to the same effect *Schenck v Switzerland* (1988) 13 EHRR 242, *Teixeira de Castro v Portugal* (1998) 28 EHRR 101 and *Khan v United Kingdom* (2000) 31 EHRR 1016. In a number of decisions involving electronic surveillance/phone tapping (*Bykov v Russia*, Application 4378/02, paras 88-91 (Grand Chamber) and *Dragojević v Croatia*, Application 68955/11, paras 127-130) and a very recent decision involving general retention of traffic and location data (*Škoberne v Slovenia*, Application 19920/20, para 146), the ECtHR has reiterated the principle that admissibility of evidence is a matter for national law, and that evidence obtained in breach of the ECHR – specifically Article 8 - is not *per se* inadmissible.

against them, particularly where the evidence was technical and likely to have a preponderant influence on the court's assessment (para 77).

106. The issues addressed in *Mantovanelli* and *Steffensen* appear to me to be quite distinct from the issues that arise as regards the admissibility of unlawfully obtained evidence. The manner in which lawfully obtained evidence is deployed can give rise to a breach of the adversarial principle. Conversely, the deployment of unlawfully obtained evidence will not necessarily implicate the adversarial principle. There is no necessary or logical connection between the two. Moreover, as Clarke J observed in *JC*, the fact that evidence has been obtained as a result of an unauthorised search of a dwelling house does not affect its probative value: at para 825. In any event, it was not suggested here that there was any breach of the adversarial principle or that the admission of the phone data evidence rendered the trial unfair in any way analogous to *Mantovanelli* or *Steffensen.* The Appellants were given advance notice of the traffic and location data evidence that the Director intended to rely on at trial. They had an opportunity to object to the admission of that evidence (and did so, albeit without success). They also had an opportunity to challenge the reliability and probative value of that evidence, whether by way of cross-examination of the Director's witnesses and/or by calling their own experts. In fact, the evidence was not subject to any such challenge. None of this is controversial. Counsel for Mr Smyth (who dealt with the admissibility issues in oral argument on behalf of both his client and Mr McAreavey) made it clear that he was not contending that the particular ground for exclusion identified in paragraph 44 of *Prokuratuur* had any application here. Rather, his submission was that that specific

ground was no more than a particular illustration of the application of the broader principle of effectiveness.

107. The statement in paragraph 43 of the CJEU's judgment in *Prokuratuur* (echoing a statement to the same effect in *La Quadrature du Net*, at para 225) to the effect that the objective of national rules on admissibility is "*in accordance with the choices made by national law, to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences*" is also a rather curious one. That is, no doubt, one possible objective of rules on admissibility of unlawfully obtained evidence. However, as is evident from this Court's decisions in *JC*, *CAB v Murphy* and *Quirke (No 2)*, as well as the case-law, both domestic and international referred to in those decisions, there are many other potential rationales and other interests and values potentially involved in this area. The point is well-captured by O' Malley J (Clarke CJ, McKechnie, MacMenamin and Dunne JJ agreeing) in *CAB v Murphy:*

> *"[125] Having regard to the range of Irish authorities cited above, it seems clear that the exclusionary rule is not a free-standing rule that evolved or exists purely for the benefit of defendants in either criminal or civil proceedings. While it originated in the context of a criminal trial (The People (Attorney General) v. O'Brien[1965] I.R 142), its broader purpose is to protect important constitutional rights and values. It will have been seen that, at different times and dealing with different issues, individual judges have laid greater or lesser emphasis on particular aspects of those rights and values. However the common*

themes are the integrity of the administration of justice, the need to encourage agents of the State to comply with the law or deter them from breaking it, and the constitutional obligation to protect and vindicate the rights of individuals. These are all concepts of high constitutional importance. Each of them, or a combination thereof, has been seen as sufficient to ground a principle that is capable of denying to the State or its agents the benefit of a violation of rights carried out in the course of the exercise of a coercive legal power."

108. In addition, the potential exclusion of evidence potentially engages significant societal and community interests in the administration of justice, particularly (though, as is illustrated by *CAB v Murphy*, not exclusively) the administration of criminal justice. Exclusion of probative evidence exacts a price. That is a very important thread running through the analysis of the majority in *JC:* see eg per O' Donnell J at paras 452 & 456 and 488-489, Clarke J at paras 824-826 and MacMenamin J at paras 944 and 954.

109. Different jurisdictions – including the different Member States of the EU - may (and, as a matter of fact, do) adopt different exclusionary rules, that give more or less weight to the different policy rationales and to the different interests at stake.[17] Given that the rules governing admissibility/exclusion are a matter for national law, it follows that the choice of rationale(s) for any rule of exclusion is a matter for each Member State and not a matter of EU competence: Member States are not required to adopt uniform policies or uniform rules.

[17] See generally Giannoulopoulos, Improperly Obtained Evidence in Anglo-American and Continental Law (Oxford, 2019)

110. In any event, this aspect of the judgment in *Prokuratuur* did not really feature in the argument in these appeals. Perhaps of greater significance is that the remainder of paragraph 43 makes it clear that the principle of effectiveness does not require the *per se* exclusion of evidence gathered in breach of EU law. Any such rule of exclusion would, of course, be fundamentally inconsistent with the basic principle that admissibility is a matter for national law.

111. In fact, none of the parties argued for the application of any absolute exclusionary rule. IHREC did refer us to Case C-419/14 *WebMindLicences* EU:C:2015:832 which can be read as supporting an absolute rule of exclusion where evidence is obtained in breach of the Charter: paras 86 – 91. But the Charter was directly applicable in *WebMindLicences* (because the underlying proceedings related to VAT) and so the issue presenting here did not arise. IHREC relied on *WebMindLicences*, and other CJEU authority such as Case C-213/89 *Factortame* EU:C:1990:257, not as authority for an absolute exclusionary rule but in order to support its contention that the principle of effectiveness required the application of *JC* and that the evidence at issue ought to be excluded if found to have been gathered in conscious or reckless breach of EU law. Neither was it suggested that the ECHR jurisprudence supported the existence or application of any absolute exclusionary rule. That is clearly not the case. The overall fairness of the trial process is the touchstone of the ECHR jurisprudence.[18]

[18] See *Panzavolta*, at 203 as well as the ECtHR decisions cited in footnote 15 above.

112. Apart from the argument that, as a matter of *Irish* law, *Kenny* rather than *JC* continued to be the applicable test in the circumstances here – an argument which is, for reasons I shall explain, misconceived - the high-water mark of Mr Smyth's argument (which was, in this respect, effectively supported by IHREC) was that the principles of equivalence and effectiveness required the application of the *JC* test. According to both Mr Smyth (and Mr McAreavey) and IHREC application of the *JC* test was both *required* by the principles of equivalence and effectiveness and was, in principle, *sufficient* to satisfy those principles.

113. There is perhaps one further point that arises from the observations of the Grand Chamber in *Prokuratuur*. At paragraph 42, the court states that it has consistently held that it is a matter for Member States, in accordance with the principle of procedural autonomy, to "*establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law*" subject to the principles of effectiveness and equivalence. That is clearly so. But what is at issue here is not an action intended to safeguard rights derived from EU law, at least not directly. The issue here relates to the admissibility of evidence in criminal proceedings in circumstances where the evidence was obtained in breach of EU law. A court addressing that issue is not engaged in safeguarding EU law rights or providing a remedy for their breach: see the comments of O' Donnell J in *JC*, at para 488. Of course, the rights involved are an essential element in the court's assessment but there are other factors that are relevant in this context also.

Is the test for admissibility that set out in JC or is some other test applicable?

Mr Smyth's contention that Kenny remains the applicable test

114. It was said by Mr Fitzgerald SC (for Mr Smyth) that *JC* does not establish any "*universal test*" for all breaches of constitutional rights in this jurisdiction, reference being made in this context to the statement of O' Donnell J in *JC* that he was addressing only issues relating to search warrants and not questions of evidence consequent upon arrest or detention (para 396 of the report) and the statement of Clarke J (para 868 of the report) that he was addressing issues relating to evidence gathering on foot of a search warrant or other statutory authority and not issues concerning the lawfulness of detention, where questions could arise as to the probative value of the evidence (para 868 of the report). Arguably – so Mr Fitzgerald SC suggested - a question arose as to whether access to traffic and location data retained in breach of EU law fitted within the "*evidence gathering*" category of cases to which *JC* clearly applies or whether the rule in *Kenny* arguably continued to apply to such material.

115. Any such argument faces two insurmountable difficulties. Firstly, this is clearly a case about *evidence gathering*, not a case about *statements/admissions* made while in custody. The reason for that distinction in *JC* is that the circumstances affecting the lawfulness of evidence gathered while in custody - such as an incriminating statement made by an accused – *may* affect the probative value of the evidence, such as where the statement was made as a result of oppressive questioning. In contrast, the unlawful nature of a search does not affect the reliability or probative value of real evidence

obtained as a result of it. While *JC* can be read as leaving open the question of whether some different rule ought to apply to that category of evidence, no such issue arises here. This case concerns the gathering of real evidence and, even if it is not strictly a search warrant case, the issues presented are very closely analogous to the issues in *JC*: evidence was gathered (retained and then accessed) ostensibly pursuant to lawful authority (here the provisions of the 2011 Act; in *JC* a search warrant issued pursuant to section 29 of the Offences Against the State Act 1939) that was subsequently declared invalid. The circumstances giving rise to the unlawfulness do not impact on the probative value or reliability of the evidence here, any more than was the case in *JC*.

116. Secondly, *JC* clearly overruled *Kenny*. Nothing said in the judgments of the majority in *JC* suggests that *Kenny* was left with any residual existence or application. That position was confirmed by this Court in *Quirke (No 2)*, which also explained that the principles in *JC* are of general application and are not in fact confined to search warrant cases: per Charleton J (for a unanimous 7 member court), at paras 32 – 34. Accordingly, the suggestion that *Kenny* continued to enjoy some form of juridical half-life in the aftermath of *JC* must be rejected.

The Director's argument that JC does not apply where the breach is of an unenumerated constitutional right

117. The Director too relied on an argument that *JC* did not enshrine a universal test of admissibility applicable to constitutional breaches, though to the opposite effect. *JC*, it

was said, involved an unconstitutional search of the dwelling house and the majority of the court in *JC* made it clear that it was reserving the question of whether the *JC* test applied in other areas. According to the Director, the constitutional protection for the dwelling (which Article 40.5 of the Constitution declares to be "*inviolable*") differs from the standard of protection applicable to unenumerated personal rights, such as privacy, under Article 40.3.1, which rights were liable to restriction and qualification. On that basis, the Director invited the Court to apply some less exacting admissibility test than that set out in *JC* (presumably some version of the test for unlawfully obtained evidence articulated in *O' Brien*).

118. Again, that argument is, in my view, misconceived. It may be that, in light of recent jurisprudence, and especially the decision of this Court in *Simpson v Governor of Mountjoy Prison* [2019] IESC 81, [2020] 3 IR 113, some aspects at least of the right to privacy are properly located in the express guarantee in Article 40.3.3 to protect and vindicate "*the person*" of citizens. But, whether that is so or not, it is wrong to suggest that unenumerated rights (or "*derived rights*", the term which this Court in *Friends of the Irish Environment v Ireland* [2020] IESC 49, [2020] 2 ILRM 233 suggested may more accurately reflect the true nature of rights which do not find expression in the text of the Constitution itself), are categorically less important and/or may be violated with greater impunity than express rights. Virtually all constitutional rights, express or derived, are to some extent liable to restriction and qualification. That is certainly true of the right to privacy: see *People (DPP) v Wilson* [2017] IESC 54, [2019] 1 IR 96 where this Court made it clear that the right was not absolute and may be outweighed by the exigencies of the common good, including the compelling public interest in the

investigation of serious crime (joint judgment of Clarke, Dunne and O' Malley JJ, at paras 32-33). But where evidence is found to have been obtained in breach of the constitutional right to privacy, there is no basis for discounting such a breach or treating it as inherently less serious than a breach of (say) Article 40.5. In both cases, admissibility is governed by *JC*. That is clear from *JC* itself in terms of the admissibility of real evidence and *Quirke (No 2)* makes it clear that *JC* in fact applies generally.

119. I also agree with the observations of Hogan J on this issue at paras 36 - 38 of his judgment.

The arguments as to whether JC is engaged by the breaches here

120. The principal (though not the only) issue in dispute under this heading relates to the proper characterisation of the Grand Chamber's decision in *GD* and the basis on which it concluded that the relevant provisions of the 2011 Act were incompatible with EU law. The Appellants (supported in this respect by IHREC) maintain that, in substance, the CJEU held that those provisions breached Articles 7, 8 and 11 and Article 52(1) of the Charter and, they say, the principle of equivalence requires that breaches of the Charter – which by virtue of Article 6(1) TEU has the same legal value as the Treaties – be regarded as equivalent to breaches of the Constitution and thus as engaging the *JC* test.

121. Mr Smyth criticised the approach taken by the Court of Appeal. The material on which the prosecution relied was, it was said, "*manifestly unlawfully retained and accessed*"

and instead of applying the domestic exclusionary rules of evidence, the Court of Appeal had engaged in a qualitative analysis of the gravity of this breach under the rubric of procedural autonomy of the Member States of the EU in a manner for which - so it was said - there was no precedent and which "*furthermore misunderstood and greatly simplified the principle of procedural autonomy.*" That principle did not afford national courts a free hand in determining how to deal with the consequences of breaches of EU rights. On the contrary, national courts were required "*to give full effect to the consequences of those breaches under the principle of effectiveness, and to do so in a manner which provides the same protection to rights under EU law as under domestic law in accordance with the principle of equivalence*". The SCC and the Court of Appeal were both said to have manifestly failed to give effect to these principles.

122. Mr McAreavey also emphasises that the procedural autonomy of Member States is limited by the principles of effectiveness and equivalence. The principle of equivalence required that the breach of EU rights here should be treated as equivalent to a breach of the constitutionally protected right to privacy. While that right was not absolute, where evidence was obtained in breach of that right *JC* governed the admissibility of that evidence.

123. The Director on the other hand argues that the CJEU in *GD* did not find that the relevant provisions of the 2011 Act were inconsistent with the Charter. Rather, the court's finding had been that those provisions were inconsistent with Article 15 of the ePrivacy Directive, read in light of Articles 7, 8, 11 and 52(1) of the Charter. The Director accepts that where the admissibility of evidence obtained in breach of a constitutional right is

at issue, the *JC* test applies. On the Director's case, however, there was no breach of any constitutional right here nor did the principle of equivalence require that the breach of EU law here be treated as the equivalent of the breach of a constitutional right or norm. The 2011 Act had been found by the CJEU not to comply with the conditions set out in Article 15(1). That, it is said, is "*much more reminiscent*" of a determination in Irish law that a measure was *ultra vires* a statutory power. Therefore, the Director says, the appropriate approach to the admissibility of the disputed evidence here is that applied in Irish law to evidence that has been illegally obtained, rather than that applicable to evidence obtained in breach of constitutional rights. On that basis, the Director says, the *JC* test is not engaged here.

124. IHREC's submissions focussed significantly on this issue. It supported the Appellants' argument that the breaches of EU law here were properly characterised as breaches of the Charter and not simply as breaches of Article 15(1) of the ePrivacy Directive. If the protections provided for in the ePrivacy Directive were breached, it necessarily followed that the underlying Charter rights were breached and, in any event, any interference with the Charter in such circumstances would not be "*provided for by law*" as required by Article 52(1) of the Charter. There was therefore a direct breach of the Charter. While rules relating to admissibility of evidence were subject to national procedural autonomy, that was subject to the duty of sincere co-operation and the principles of equivalence and effectiveness. According to IHREC, the principle of equivalence prevented a Member State from laying down less favourable procedural rules for actions for safeguarding rights that individuals derive from EU law than those that are applicable to similar domestic actions. The equivalence assessment takes place

at the level of the cause of action at issue (citing Case C-118/08 *Transportes Urbanos y Servicos Generales SAL v Administración del Estado* EU:C:2010:39 and Case C-234/17 *XC* EU:C:2018:853). In terms of "*essential characteristics*", no distinction could be drawn between a hearing to determine the admissibility of evidence gathered in breach of a Charter right and evidence gathered in breach of a constitutional right. IHREC also advanced a related but distinct argument to the effect that the principle of effectiveness required the application of *JC*. Where evidence was gathered in conscious or reckless breach of EU law protecting fundamental rights, or as a result of any "*seriously culpable*" breach of such rights, such evidence should be excluded, not just to ensure equivalence but as an aspect of the principle of effectiveness, so as to deter future breaches of EU law, ensure the primacy of EU law and uphold the rule of law, a foundational principle on which the Union is built. As already mentioned, IHREC relied on (inter alia) Case C-419/14, *WebMindLicences* EU:C:2015:832 in support of this submission.

125. IHREC also contended that a breach of the Charter is *ipso facto* a breach of the constitutional commitment to the Union in Article 29.4.4 of the Constitution. Any breach of Union law conflicts with that commitment and must there be treated as a breach of it, at least where (as here) the provision of EU law confers a "*foundational right*" on an individual having the same status as a Treaty right.

126. Finally, IHREC argued that the evidence at issue was in fact obtained in breach of the Appellants' constitutional right to privacy, citing the decision of the High Court (Hogan J) in *Schrems v Data Protection Commissioner* [2014] IEHC 310, [2014] 3 IR 75. In

Schrems – which concerned a challenge to the regime providing for the transfer of personal data from the EU to the USA, on the basis that such data was liable to unconstrained access by US security agencies – Hogan J observed that, as a matter of Irish law, the constitutional right to privacy was engaged by State measures to access private communications but such measures were not necessarily unlawful provided that "*appropriate safeguards*" were in place and the interference took place in a manner "*provided for by law*". On IHREC's case, neither of those requirements was satisfied here. The interference was not provided for by law in circumstances where the national legislation which authorised it violated EU law and the absence of any requirement for prior authorisation by an independent or judicial authority for access to the retained data meant that appropriate safeguards were not in place. A number of decisions of this Court – including *Damache v DPP* [2012] IESC 11, [2012] 2 IR 266 and *People (DPP) v Behan* [2022] IESC 23 – as well as decisions from the ECtHR, and the Supreme Courts of the United States and Canada were cited in support of the need for the "*independent authorisation safeguard.*"

127. The Director's arguments on the nature of the CJEU's findings in *GD* are not without force. They find some support in the terms of the *dispositif*. In addition, an important thread in the court's analysis (as it was in *La Quadrature du Net*) was that a regime of general retention was impermissible because it would turn the Article 15(1) exception into the rule: see, for example, at para 40. Even so, I am not persuaded that the judgment can properly be read as narrowly as the Director contends. It seems clear that the court ultimately concluded that the retention and access provisions of the 2011 Act exceeded the scope of permissible derogation under Article 15(1) of the ePrivacy Directive

precisely *because* those provisions gave rise to serious and unjustified interferences with the rights protected by Articles 7, 8 and 11 of the Charter. The substantive limits on the derogations permitted by Article 15(1) that were identified by the court in *GD* essentially derive from those Charter provisions. In substance, the retention and access provisions of the 2011 Act were condemned because they exceeded what the Charter permitted. That, in my opinion, was what the court meant when it referred to "*Article 15(1) [of the ePrivacy Directive] read in the light of Articles 7, 8 and 11 and Article 52(1) of [the Charter]*".

128. In this regard, the court characterised the ePrivacy Directive as the "*concrete expression*" of the rights set out in Articles 7 and 8 of the Charter (paras 36-37). Article 15(1) made it clear that measures taken by Member States had to comply with the general principles of EU law, including the principle of proportionality and "*ensure respect for the fundamental rights guaranteed by the Charter*" (para 42). Retention of traffic and location data was *per se* "*an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8*" (para 44). Retention of such data for policing purposes was liable, in itself, to infringe the rights enshrined in Article 7 and to deter users from exercising their freedom of expression guaranteed in Article 11, effects which were all the more serious given the quantity and breadth of the data involved (para 46). Article 15(1) permitted Member States to derogate from Articles 5, 6 and 9 of the Directive, reflecting the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter were not absolute rights (para 48). However, even the important objective of combatting serious crime did not justify general and indiscriminate retention of traffic and location data (para 65 and following).

The court's analysis of the access issue is somewhat briefer but in its substance it is clear that prior independent authorisation is necessary to ensure respect for, and protection of, the rights under Articles 7, 8 and 11 of the Charter.

129. It follows that the evidence at issue here must be regarded as having been retained and accessed in breach of the Charter. From that, it follows that the admissibility of that evidence falls to be assessed by reference to *JC*. To apply any less-exacting test would not be consistent with the principles of equivalence and effectiveness because it would effectively accord rights guaranteed by the Charter a lesser status than rights protected by the Constitution. That would not be consistent with the obligations of the State – and of this Court – to respect, and give full effect, to EU law, having regard, in particular, to Articles 4(3) and 6(1) TEU. The point is aptly stated in McGrath, *Evidence* (3rd ed; 2020):

> "*Given the primacy of EU law, it is difficult to see how a less protective approach could be applied to rights protected under the Charter than to rights protected under the Constitution.*" (para 7-135)

130. It is not, in my view, necessary here to engage in any extended discussion of the CJEU jurisprudence on the principle of equivalence. It is enough to observe that (adopting the language of the Grand Chamber in Case C-118/08 *Transportes Urbanos* EU:C:2010:39) an inquiry into the admissibility of evidence obtained in breach of the Charter has the same fundamental purpose and "*essential characteristics*" as an inquiry into the admissibility of evidence obtained in breach of the Constitution, such that they

must be regarded as similar: at para 35. That conclusion is not called into question by the later decision of the Grand Chamber in C-278/20 *Commission v Spain* EU:C:2022:503 insofar as the principle of equivalence is concerned. That decision would be relevant if there were EU rules on admissibility that prescribed a different threshold to *JC* but such is not the case.

131. In concluding that the principles of equivalence and effectiveness require the application of the *JC* test, I have not overlooked the Court of Appeal's decision in *People (DPP) v O' Doherty* [2019] IECA 209. Giving the judgment of the court, Edwards J stated that nothing in Irish law suggested that, where a court is concerned with the admissibility of evidence obtained in breach of a fundamental personal right guaranteed to an accused under an instrument such as the Charter, which was not directly mirrored in the Constitution, such breaches were to be approached in the same way as breaches of rights guaranteed to the accused under the Constitution, or that they engaged the same exclusionary rules (at para 97). That was an avowedly *obiter* observation and it is apparent from the judgment that the issue was not argued. In contrast, this Court has had the benefit of elaborate argument on the point. In any event, the court in *O' Doherty* went on to indicate that, where it was alleged that evidence had been gathered in breach of the accused's right to privacy under Article 7 of the Charter, the constitutional exclusionary rule would arguably be engaged (para 120). That correctly states the position in my view.

132. In the circumstances, it is unnecessary to address the alternative arguments advanced by IHREC as to why *JC* should apply. The argument that a breach of the Charter is *ipso*

facto a breach of the constitutional commitment to the Union in Article 29.4.4 of the Constitution and is therefore to be regarded as a breach of the Constitution itself is novel and far-reaching. It is also, in my view, implausible. There can be no doubt that Article 29.4 of the Constitution permits the EU treaties to be made part of Irish law (their incorporation into domestic law is actually effected by the European Communities Act 1972 (as amended)) and immunises from constitutional challenge acts done and measures adopted by the State necessitated by membership of the EU. But it does not follow that Article 29.4, and Article 29.4.4 in particular (inserted into the Constitution by the 30th Amendment), effectively incorporates the treaties (including the Charter) into the Constitution, so that a breach of the former (at least in the area of fundamental rights) is to be regarded as a breach of the latter. The bland and innocuous language of Article 29.4.4 ("*Ireland affirms its commitment to the European Union within which the member states of that Union work together to promote peace, shared values and the well-being of their peoples*.") simply cannot bear such weight.

133. As to IHREC's argument that the manner in which the evidence here was obtained in breach of the Appellants' constitutional right to privacy, such an argument goes beyond the legitimate scope of its role as *amicus*. If such an argument was to be advanced, it was incumbent on the Appellants to do so. They have not. The Appellants' appeals are firmly based on the contention that the evidence at issue should be excluded because (and only because) it was obtained in breach of their *Charter* rights.

134. I would in any event observe that this Court's analysis in *Dwyer* strongly suggests that it considered that general data retention for the purposes of the investigation and

prosecution of serious crime was, in principle, constitutionally permissible: see the judgment of Clarke CJ at paras 6.2, 6.9, 6.10 & 6.14-6.16. It is less clear what view the Court might have taken as to the constitutionality of the statutory access regime, particularly in light of the decision in *Damache v DPP* [2012] IESC 11, [2012] 2 IR 266. As IHREC noted in its submissions, the approach taken in *Damache* is consistent with the approach taken in other jurisdictions as to the need for prior judicial/independent authorisation in similar contexts: see *R v Spencer* [2014] 2 SCR 212 (police access to IP addresses was unlawful in the absence of prior judicial authorisation); *Carpenter v United States* 138 S Ct 2206 (2018) (search warrant required to access location data held by telecoms providers) and *Benedik v Slovenia* (app no 62357/14) (July 2018) (access to IP addresses in breach of Article 8 ECHR *inter alia* because of absence of prior court order authorising access). But that issue did not fall for determination in *Dwyer*, given that the challenge to the 2011 Act was based solely on the Charter.

135. In any event, it is in my view clear that the admissibility of the evidence here falls to be determined by reference to *JC* on the basis that the evidence was obtained in breach of the Charter. Hogan J reaches the same conclusion in his judgment and I agree with his analysis also.

> *In considering the admissibility of the phone location and call data here, what is the significance (if any) of the fact that neither appellant asserted or accepted ownership of the 691 phone or the 773 phone?*

136. But, the Director says, the Appellants have not asserted or acknowledged ownership of the 691 and 773 numbers and therefore cannot assert any breach of their privacy rights. It follows – or so the Director says – that the Appellants cannot establish that any personal right of theirs (whether flowing from the Charter or otherwise) was interfered with by the retention and accessing of the traffic and location data associated with those phone numbers. That, the Director boldly suggests, is "*dispositive of the admissibility issue.*"

137. Mr Smyth and Mr McAreavey, supported by IHREC, suggest that the Director's argument runs counter to the entire structure of a criminal prosecution and to the onus of proof that rests on the prosecution. It would – so it is said - put the Appellants in a wholly invidious position if they were required to make admissions as to their use of the disputed numbers as a prerequisite to asserting a breach of their rights and/or contesting the admissibility of the traffic and location data that had been retained and accessed in breach of EU law. As it was put by IHREC, an accused should not have to forego the privilege against self-incrimination by making an admission that might assist the prosecution in order to rely on privacy rights nor should an accused have to forego reliance on privacy rights in order to rely on the privilege against self-incrimination.

138. In my view, the Director's argument must be rejected. The burden of proof here was at all times on the Director. Mr Smyth (and Mr McAreavey) were entitled to put the Director to proof in relation to all the elements of her case. The Director sought to rely on the traffic and call data relating to the 691 and 773 numbers on the basis that those

numbers had been, respectively, in the control and use of Mr Smyth and Mr McAreavey at all material times. In those circumstances, Mr Smyth and Mr McAreavey were entitled to object to the admissibility of that evidence on the basis that, *on the Director's case*, the traffic and call data constituted their personal data and that such data had been retained and accessed in breach of the Directive of the Charter.

139. In other words, Mr Smyth and McAreavey were entitled to adopt the position that, *if* the Director established that the 691 and 773 numbers should be attributed to them – such attribution being, of course, an essential prerequisite to establishing the relevance of the traffic and location data in the first place – *then* on that premise it followed that an issue arose as to its admissibility which required adjudication before such data could properly be admitted into evidence. They were not required to forego their fundamental rights as criminal defendants – and in particular their right not to incriminate themselves - by making an admission that the numbers were indeed theirs in order to object to the admissibility of the data, any more than an accused alleged to have made an incriminating statement in the course of an unlawfully intercepted phone call would first be required to admit that he was the person on the recording before being permitted to object to its admissibility, That would indeed place an accused in an invidious position, one which would be very difficult to reconcile with the provisions of Article 38 of the Constitution (or with Article 6 ECHR). In this regard I also note, and agree with, the observations of Hogan J at paras 18 and 19 of his judgment.

140. In my view therefore, the fact that Mr Smyth and McAreavey did not assert or accept ownership of the 691 phone or the 773 phone respectively does not have the

significance suggested by the Director. It is not, as she suggests, "*dispositive of the admissibility issue.*" To the extent that the SCC and the Court of Appeal considered otherwise, I respectfully differ from their analyses.

No privacy in the commission of criminal offences?

141. The Director also argues that there is, in any event, no or no significant right to privacy in communications or information that relate to or disclose the commission of a criminal offence. Such a sweeping proposition cannot be accepted. To do so would empty the right to privacy of any meaningful content in this context, as even in a case involving the most egregious breach of privacy – such as a knowingly unauthorised search of a dwelling house or interception of phones or correspondence - it might then be said that where any incriminating material was obtained as a result, then *ipso facto* it fell outside the scope of constitutional protection. Endorsing such an approach would incentivise inappropriate conduct by law enforcement agencies.

142. It is undoubtedly the case that as a matter of principle the investigation of serious crime may justify "*a degree of invasion of the right to privacy*": *People (DPP) v Wilson*, para 33. Thus, a search warrant may authorise incursion into private premises and the seizure of material that is "*undeniably private*" (*ibid*). Similarly, the interception of private phone communications or correspondence – acts which would otherwise violate the constitutional right to privacy as per *Kennedy v Ireland* [1987] IR 587 - may be

authorised in accordance with the provisions of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993. But as this Court explained in *Wilson*, such powers are "*of course subject to the requirement that they be exercised in accordance with law and in a manner proportionate to the purpose for which they are conferred"* (*ibid*). Where such acts are undertaken otherwise than in accordance with law, a breach of privacy occurs and it is no answer to say that, as a result of the breach, evidence relating to or disclosing the commission of a criminal offence has been obtained. That evidence may ultimately be admissible in a criminal trial but that does not take away from the fact that, in such circumstances, it was obtained in violation of the right to privacy. That is true of evidence obtained in breach of Articles 7 and 8 of the Charter as it is of evidence obtained in breach of the constitutional protection of privacy interests (which, in my view, encompasses the protection of the dwelling under Article 40.5, the protection of "*the person*" under Article 40.3.2 and the derived right to privacy protected by Article 40.3.1 recognised in *Kennedy v Ireland*).

143. That conclusion is consistent with the analysis of the former Court of Criminal Appeal in *People (DPP) v Dillon* [2002] 4 IR 501. In *Dillon*, an issue arose as to whether the actions of an Inspector in An Garda Síochána amounted to the "*interception*" of a phone call, in circumstances where no such interception had been authorised under the 1993 Act. The Inspector had come into possession of a mobile phone in circumstances leading him to believe that it was likely to be used for the purposes of arranging drug transactions. He answered a call from "*Joe*" – allegedly the accused – and, without revealing his true identity, held a conversation in which Joe made incriminating statements. The Court of Criminal Appeal held that this constituted an unauthorised

interception. That conclusion was reached *per incuriam* because the court applied the definition of "*interception*" contained in section 98 of the Postal and Telecommunications Services Act 1983, without adverting to the fact that the definition had been significantly amended by the 1993 Act: see *Geasley v DPP* [2009] IECCA 22. However, that error does not undermine the subsequent analysis in *Dillon*. The court noted that the DPP had submitted that "*the protection of privacy in telephone conversations, considered as a constitutional right, could not apply to a conversation which, it turns out, was for the purpose of furthering the commission of a crime*" (at page 513). Rejecting that argument, Hardiman J, giving the judgment of the court (the other members being Finnegan P and Ó Caoimh J) stated:

> *"It seems to us that the status of the interception must be determined as of the time of its commencement and cannot change on the basis of what develops during the conversation intercepted. An interception which is unlawful cannot become lawful on the basis of what is heard during it. Nor can an accused person be estopped from raising a question of admissibility of evidence based on unlawful interception on the basis of the illegal purport of the conversation intercepted. If that were permissible it would set at nought the detailed and specific statutory provisions relating to interception because it is only where a conversation evidences unlawful activity that it will be sought to introduce it in evidence. If a defendant could be so estopped, unlawful interception could take place within impunity so long as it yielded useful evidence and there would be no practical restriction on unlawful interception which did not yield such evidence because its occurrence would not become known."* (at 513)

Accordingly, the evidence of what was allegedly said by "*Joe*" was unconstitutional and its admissibility fell to be determined by the exclusionary rule in *Kenny* (*Dillon* obviously predated *JC*).

144. I agree with the analysis in *Dillon*. Adapting its language, if communications or information that relate to or disclose the commission of a criminal offence are *ipso facto* excluded from constitutional protection, the constitutional right to privacy would effectively be set at nought.

145. In passing I would also observe that it seems clear that in *Dillon* that the accused did not at any point admit that he was the "*Joe*" who had spoken to the Inspector. The prosecution alleged that he was and, it appears, satisfied the jury of that fact but nothing in the judgment of the Court of Criminal Appeal suggests that the accused admitted that he was the caller or that such an admission was a pre-requisite to challenging the admissibility of the Inspector's evidence of what was said on the call.

146. We were also brought to the decision of the Supreme Court of Canada in *R v Spencer* [2014] 2 SCR 212 in this context. In *R v Spencer* the police obtained from an Internet Service Provider the subscriber information associated with the IP address of a computer which the police had identified as having been used to access and store child pornography. The subscriber information was obtained without prior judicial authorisation. Armed with that subscriber information, the police obtained a search warrant to search the house where the defendant lived and seized his computer, which

contained illegal pornographic images. He was charged with and convicted of possession of child pornography. He argued that the police had conducted an unconstitutional search by obtaining the subscriber information and that the evidence obtained as a result should be excluded. That argument failed at trial and on appeal to the provincial court of appeal. Although taking the view that there had been an unconstitutional search, the Supreme Court of Canada dismissed the appeal on the basis that the exclusion of the evidence rather than its admission would bring the administration of justice into disrepute.

147. Cromwell J gave the sole judgment. In the course of it he considered the nature of the privacy interest potentially compromised by the State action. The court had, he noted, described three broad types of privacy interests - territorial, personal and informational (at para 35). He continued::

> *"[36] The nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought. To paraphrase Binnie J. in Patrick, the issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes: Patrick, at para. 32.*

[37] We are concerned here primarily with informational privacy. In addition, because the computer identified and in a sense monitored by the police was in Mr. Spencer's residence, there is an element of territorial privacy in issue as well. However, in this context, the location where the activity occurs is secondary to the nature of the activity itself. Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via smartphones, or portable devices. Therefore, here as in Patrick, at para. 45, the fact that a home was involved is not a controlling factor but is nonetheless part of the totality of the circumstances: see, e.g., Ward, at para. 90."

148. Cromwell J went on to hold that the defendant had a reasonable expectation of privacy in his subscriber information ([52] – [67]) and, on that basis, concluded that warrantless obtaining of that information was unlawful and a breach of Article 8 of the Charter: [68] – [74]. Turning to the admissibility of the evidence in such circumstances, Cromwell J applied the test set out in *R v Grant* [2009] 2 SCR 353, involving consideration of the following three factors: (1) the seriousness of the Charter-infringing conduct; (2) the impact of the breach on the Charter-protected interests of the accused and (3) society's interest in the adjudication of the case on its merits: [76]. As to (1), in the judge's view, the conduct could not be characterised as wilful or flagrant disregard of the Charter. The police officer had testified that he believed that the request to the ISP was authorised by law and, although the officer had also said that he was aware there were decisions "*both ways*" as to whether it was a legally acceptable practice, his belief was "*clearly reasonable"* in light of the fact that the trial judge and all three members of the Court of Appeal had concluded that the practice followed was

lawful: [77]. As to (2), the impact of the conduct on the defendant was serious as it had violated his anonymity and subjected him to police scrutiny. That weighed in favour of excluding the evidence: [78]. As to (3), society had both a strong interest in the adjudication of what were serious offences and also in ensuring that the justice system remained above reproach in its treatment of those charged with such offences. Exclusion of the evidence would leave the Crown with no case. The evidence was reliable and was admitted to constitute child pornography. Society "*undoubtedly has an interest in seeing a full and fair trial based on reliable evidence, and all the more so for a crime which implicates the safety of children*": [80]. Balancing the three factors, Cromwell J concluded that the exclusion of the evidence would bring the administration of justice into disrepute: [81].

149. *Spencer* is of wider interest but focussing at this stage on the observations made by Cromwell J at paragraphs [36] & [37], I agree with what is said there which appears to me to be consistent both with fundamental principle and with the approach taken by the Court of Criminal Appeal in *Dillon*. An unlawful search, unlawful interception or unlawful act of surveillance does not lose its unlawful character simply because it has yielded incriminating evidence. Any such principle would be wholly destructive of basic constitutional norms and the rule of law.

150. *Spencer* was referred to by the ECtHR in *Benedik v Slovenia* (Application no 62357/14) in which, in circumstances strikingly similar to those in *Spencer*, the Strasbourg court found that the manner in which the Slovenian police had obtained subscriber and traffic information from an ISP - leading to the seizure of the applicant's computer on which

files containing child pornography had been found - violated Article 8 ECHR. In the course of its judgment, the court observed that the issues concerning the applicability of Article 8 were " *to be answered independently from the legal or illegal character of the activity in question*" (para 99). No issue of admissibility arose in *Benedik v Slovenia* (that being solely a matter of national law in accordance with the settled jurisprudence of the ECtHR).

151. The authorities relied on by the Director in this context do not support any different approach. In *Idah v Director of Public Prosecutions* [2014] IECCA 3, the issue was the admissibility of evidence purportedly gathered pursuant to the Criminal Justice (Surveillance) Act 2009. The court ruled that, in fact, certain of the surveillance undertaken by An Garda Síochána fell outside the scope of the Act. Other evidence had been gathered purportedly pursuant to a District Court *authorisation* but the surveillance activity went beyond the scope of the authorisation. Section 14(4) of the 2009 Act expressly provided that such evidence could be admitted if the court decided that the officer had acted in good faith, that the failure was inadvertent and that the evidence ought to be admitted in the interests of justice. The trial judge admitted the evidence in dispute and the Court of Criminal Appeal did not consider it appropriate to interfere with that decision. However, the court held that other evidence gathered on foot of an *approval* issued by a senior Garda officer should be excluded on the basis that the circumstances of urgency justifying recourse to the approval regime did not exist and accordingly an application for judicial authorisation could and should have been made.

152. In the course of its judgment, the court observed that:

> *"37. There can be no doubt that the State may make incursions into the right of privacy in accordance with law. This is particularly the case in circumstances where the State is seeking to provide in relation to 'the investigation of arrestable offences, the prevention of suspected arrestable offences and the safeguarding of the State against subversive and terrorist threats'. Nevertheless that law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which public authorities are entitled to resort to such covert measures and it must provide necessary safeguards for the rights of individuals potentially affected. In the view of this court, that is precisely the intent and purpose of the Act of 2009."*

153. That passage is consistent with this Court's subsequent decision in *Wilson* and articulates the uncontroversial proposition that privacy rights are not absolute and that, accordingly, "*incursions*" into privacy may be authorised by law for (*inter alia*) the purposes of preventing and investigating crime. The suggestion that unauthorised incursions into privacy rights may be overlooked to the extent that they yield incriminating information is an entirely different proposition altogether and one for which *Idah* provides no support. Indeed, such a suggestion is inconsistent with fact that the court in *Idah* had no hesitation in excluding the (incriminating) evidence that had been gathered on foot of the ineffective "*approval*".

154. That understanding of the effect of *Idah* is confirmed by the observations of MacMenamin J (who gave the judgment of the court in *Idah*) in another case cited by the Director, *CRH v Competition and Consumer Protection Commission* [2017] IESC 34, [2018] 1 IR 521, at para 65.

155. The other Irish decision cited by the Director is *DPP v Doherty* [2019] IECA 209, to which I have already made reference. At para 127 of the court's judgment, Edwards J states that it is well-established that the right of privacy cannot extend to participation in criminal activity, a proposition characterised in Hogan et al, *Kelly: The Irish Constitution* (5th ed; 2018) as "*unremarkable*" (7.3.163, citing *inter alia Idah*). That is indeed so, provided that the proposition is properly understood as meaning, as per *Wilson*, no more than that significant incursions into the right of privacy may be *authorised by law* for the purpose of preventing or investigating crime.

The JC Test

JC

156. The decision in *JC* is too well-known to require extensive recitation. Three judgments were given on the majority side. In his judgment, O' Donnell J (as the Chief Justice then was) undertook a detailed survey of the comparative international jurisprudence as well as closely analysing the existing Irish jurisprudence. A consistent thread running through his judgment is that the issue of admissibility is not concerned solely with vindication of the rights breached (in *JC*, the Article 40.5 rights of the accused). That

is *not* the central issue. Rather, the central issue is the administration of justice, a central function of which is fact-finding and truth-finding. The exclusion of reliable evidence of guilt detracts from the truth finding function of the administration of justice and could bring it into disrepute (see paras 450, 452 and, particularly, 488). The question was at what point a trial would fall short of a trial in due course of law because of how evidence was obtained or, as he also put it, when did the admission of evidence itself bring the administration of justice into disrepute (para 488). A rule of near automatic exclusion extracts a heavy price in the exclusion of evidence obtained as a result of inadvertence, good faith or excusable error (para 489).

157. O' Donnell J was satisfied that *Kenny* was wrongly decided and should be over-ruled but was also satisfied that it would not be appropriate to allow the law to revert to that set out in *O' Brien* (essentially because the exclusionary rule formulated in *O' Brien* was too narrow and set the threshold for exclusion too high). As to what the appropriate test was, O' Donnell J indicated his agreement with the approach of Clarke J.

158. In his judgment, Clarke J identified two important, and potentially competing principles. On the one hand, there is "*a high constitutional value*" to be attached to the principle that all potentially relevant and probative evidence is considered at a criminal trial (para 824). The exclusionary rule, however, was not concerned with the probative value of the evidence - it was concerned with the circumstances in which the evidence was gathered. Exclusion of such probative evidence could only lead to the risk of an acquittal of guilty persons, without any corresponding reduction in the risk of the conviction of the innocent (para 826). On the other hand, there is also a "*significant*

constitutional value" in ensuring that investigative and enforcement agencies, such as An Garda Síochána, operate properly within the law. It followed that there should be significant consequences when the legal rules were broken (para 827).

159. Clarke J then discussed how these competing considerations should be balanced. After a lengthy discussion of what the elements of the test for admissibility should be, at para 871 of his judgment he summarised that test as follows:

> *"[871] In summary, the elements of the test are as follows:-*
>
> *(i) the onus rests on the prosecution to establish the admissibility of all evidence. The test which follows is concerned with objections to the admissibility of evidence where the objection relates solely to the circumstances in which the evidence was gathered and does not concern the integrity or probative value of the evidence concerned;*
>
> *(ii) where objection is taken to the admissibility of evidence on the grounds that it was taken in circumstances of unconstitutionality, the onus remains on the prosecution to establish either:-*
>
> *(a) that the evidence was not gathered in circumstances of unconstitutionality; or*
>
> *(b) that, if it was, it remains appropriate for the court to nonetheless admit the evidence.*

The onus in seeking to justify the admission of evidence taken in unconstitutional circumstances places on the prosecution an obligation to explain the basis on which it is said that the evidence should, nonetheless, be admitted AND ALSO to establish any facts necessary to justify such a basis;

(iii) any facts relied on by the prosecution to establish any of the matters referred to at (ii) must be established beyond reasonable doubt;

(iv) where evidence is taken in deliberate and conscious violation of constitutional rights then the evidence should be excluded save in those exceptional circumstances considered in the existing jurisprudence. In this context deliberate and conscious refers to knowledge of the unconstitutionality of the taking of the relevant evidence rather than applying to the acts concerned. The assessment as to whether evidence was taken in deliberate and conscious violation of constitutional rights requires an analysis of the conduct or state of mind not only of the individual who actually gathered the evidence concerned but also any other senior official or officials within the investigating or enforcement authority concerned who is involved either in that decision or in decisions of that type generally or in putting in place policies concerning evidence gathering of the type concerned;

(v) where evidence is taken in circumstances of unconstitutionality but where the prosecution establishes that same was not conscious and deliberate in

the sense previously appearing, then a presumption against the admission of the relevant evidence arises. Such evidence should be admitted where the prosecution establishes that the evidence was obtained in circumstances where any breach of rights was due to inadvertence or derives from subsequent legal developments;

(vi) evidence which is obtained or gathered in circumstances where same could not have been constitutionally obtained or gathered should not be admitted even if those involved in the relevant evidence gathering were unaware due to inadvertence of the absence of authority."

160. Addressing the element of the test directed to evidence taken in conscious and deliberate breach of rights (sub-para (iv) above), Clarke J explained that an inquiry into whether evidence was so gathered would require an analysis of the conduct or state of mind not only of any individuals "*at the coal face*" but also of any other senior official or officials within the relevant enforcement or investigation authority who were involved in a material way in the process. Thus a senior investigating garda who was well aware that An Garda Síochána did not have authority to conduct a particular search could not escape the consequences simply by procuring a less experienced or less informed member to carry out the search. In addition, if there was a systematic failure in the sense that senior gardaí were aware of and condoned practices which, to their knowledge, were likely to lead to breaches of constitutional rights, the fact that individual members involved in evidence gathering did not have the same knowledge would not justify a

finding that there was no deliberate and conscious breach in the circumstances. (para 850)

161. As to the rule providing for the admission of evidence where any breach of rights "*was due to inadvertence or derives from subsequent legal developments*", the facts in *JC* were illustrative. As a result of a subsequent decision of the courts (*Damache v Director of Public Prosecutions* [2012] IESC 11, [2012] 2 IR 266) it had become clear that a particular form of search warrant was invalid. That legal fact was not known at the time the evidence in *JC* was gathered. While it was true that some doubts had been expressed over the constitutional validity of the relevant measure (section 29 of the Offences Against the State Act 1939) "*it remained on the statute book and enjoyed the presumption of constitutionality.*" In those circumstances, Clarke J asked rhetorically, how could it be said that it would encourage enforcement and investigation authorities to remain within the boundaries of their legal power if "*evidence is to be excluded by reference to legal decisions not even taken at the time when the power in question was exercised?*" (para 853)

162. Clarke J returned to this question later in his judgment when applying the *JC* test to the facts. The disputed evidence in *JC* was, he noted, gathered before *Damache* was decided. It followed that the warrant was issued on foot of a statutory provision which was presumed constitutional and which, at the relevant time, had not been the subject of any judicial determination concerning its constitutional validity. It was possible that different considerations might arise in a case where there had been a decision of the High Court or Court of Appeal which, if correct, would render the warrant invalid –

even if such a decision was under appeal it would represent the law as understood at the time (para 873). He went on:

> *"[874] It is true that there had been some suggestions made in legal debate over the years which might have questioned the validity of the type of warrant used in this case and also in Damache v. Director of Public Prosecutions [2012] IESC 11, [2012] 2 I.R. 266. However, it does not seem to me that such debate can influence the proper approach to an assessment of the circumstances in which the warrant in this case was granted and executed. The substance of the factual underlay to this case is that the evidence in question was gathered on foot of a warrant which was prima facie valid on the basis of the law as it stood when that warrant was issued, and where the warrant was issued in furtherance of a statutory provision which enjoyed the presumption of constitutionality. In those circumstances, it seems to me that this case comes clearly within the category of case where the evidence should properly be admitted on the basis of the test which I propose. On that basis, it seems to me that, while the trial judge was, of course, bound by The People (Director of Public Prosecutions) v. Kenny [1990] 2 I.R. 110, her decision to exclude the evidence in question was necessarily erroneous in the sense in which that term is used in section 23. I would, therefore, so find."*

163. Clarke J also emphasised that, in formulating the test in the manner he did, inadvertence (which, he explained, did not include reckless or grossly negligent conduct) was not being elevated to the status of a lawful excuse for unconstitutional action. Inadvertence

did not excuse the breach. Any sanction applying in the civil or criminal law for that breach would continue to apply (Clarke J gave the example of a claim in trespass). Whether evidence obtained as a result of a breach should thereby be excluded was "*an entirely different question*". The focus of a trial was not, or not primarily, on whether the evidence was properly gathered (at least in the absence of any suggestion that the circumstances in which the evidence was gathered affected its probative value). The focus was on whether the accused was guilty or innocent and the admission of evidence that was not properly gathered did not excuse any breach of rights but simply recognised that, notwithstanding the circumstances in which was gathered, the evidence remained probative and cogent (para 860).

164. One further aspect of Clarke J's judgment should be noticed, relating to sub-paragraph (vi) of the *JC* test. Clarke J explained that it was important to distinguish between evidence gathered in circumstances where it "*could not have been constitutional in any circumstances"* and evidence gathering which was capable of being lawful and which would have been lawful but for the absence of the appropriate form of authorisation specific to the case, or where there was some defect in the authorisation granted. In that context, he continued, there was a difference "*between prosecuting authorities being able to rely, on the one hand, on evidence, the gathering of which was not authorised, but which could have been authorised, and where the absence, inaccuracy or invalidity of or in the relevant authorisation was not adverted to, and, on the other hand, evidence gathering which could never have been authorised at all*." (para 862). That "*backstop*" (as it was characterised at the hearing of the appeal and as the Court characterised it in *Quirke (No 2)*) will be the subject of detailed discussion later.

165. The third and final majority judgment was given by MacMenamin J (Denham CJ agreed with all three judgments). He agreed with the approach to admissibility proposed by Clarke J, which sought to give due recognition to the rights of protection, the duty of deterrence and the considerations of public policy and the rights of all citizens (paras 907-908). The rights involved were not just the rights of the accused but encompassed a broader range of interests and rights, including the right of the community to have crimes prosecuted and the victims of crime (para 954). While it should not be said that there should not be an exclusionary rule, the threshold of "*deliberate and conscious*" breach "*should not, and cannot encompass steps properly taken on foot of Acts of the Oireachtas, or otherwise, in a bona fide, genuine and well-founded belief as to their legality*" (para 958). In MacMenamin J's view, the bar set by the majority, which he noted was "*significantly higher*" than that to be found anywhere else in the common-law world, redressed the balance so as to "*encompass community interests while ensuring that egregious breaches of a suspect's rights and police misconduct are checked*" (para 959).

166. The exclusionary rule formulated in *JC* is not an absolute rule of exclusion. It does not follow from the fact that evidence has been obtained in circumstances of unconstitutionality that it must be excluded. That is, in essence, because (i) the issue of admissibility of evidence is a separate issue, following on from but also distinct from the issue of the lawfulness of the circumstances in which the evidence is obtained and (ii) the issue of admissibility engages compelling interests in addition to (and potentially in opposition to) the interests of the accused. It follows from *JC* that the effective

protection of constitutional rights does *not* require the exclusion of unconstitutionally obtained evidence in all or nearly all cases. That, it seems to me, is the fundamental tenet of *JC*.

167. Constitutional (and Charter) rights may be vindicated by means other than the exclusion of evidence – by way of declarations of unconstitutionality, damages for breach of constitutional rights and so on. Here, the Charter rights of Mr Smyth and Mr McAreavey have arguably been vindicated by the decision of the CJEU in *GD* and the consequent order of this Court effectively invalidating the data retention and access provisions in the 2011 Act. This is particularly so because the nature of the breach identified – general and indiscriminate retention - is of general application and arguably requires a general remedy, by invalidation. As regards their particular position, their rights are further vindicated by this Court holding (as it does) that their Charter rights were breached by the manner in which their data was retained and accessed. In addition, they may have a *Francovich* damages claim against the State arising from the breach of their EU law rights, including their Charter rights. In any event, it is clearly not the case that exclusion of the evidence here is the only means of recognising and vindicating such rights.

168. *JC* was, of course, the first time that the *JC* test was applied. Notably, the Court did not consider it necessary either to conduct any specific factual inquiry itself or to send the proceedings back to the Circuit Criminal Court for that purpose. It did not consider or make any reference to the *subjective* state of mind of the members of An Garda Síochána involved in the unlawful search. Instead, the Court focussed on the *objective*

position and, in particular, the fact that the evidence had been "*gathered on foot of a warrant which was prima facie valid on the basis of the law as it stood when that warrant was issued, and where the warrant was issued in furtherance of a statutory provision which enjoyed the presumption of constitutionality."* It was solely by virtue of a subsequent development in the law – this Court's decision to strike down section 29 of the Offences Against the State Act 1939 in *Damache* – that the breach of rights occurred in *JC* and, on that basis, the evidence was admissible.

Quirke (No 2)

169. *JC* was considered and unanimously affirmed by this Court in *Quirke (No 2)*, which was decided after the hearing of this appeal. The sole judgment was given by Charleton J (O' Donnell CJ, Dunne, O' Malley, Baker, Woulfe and Murray JJ agreeing). The Court had earlier ruled that the seizure of computers from the accused home was unlawful as it had not been authorised by the search warrant issued by the District Court judge (*People (DPP) v Quirke* [2023] IESC 5, [2023] 1 ILRM 225). An issue then arose as to the admissibility of the evidence obtained from the computers, which had been a "*significant element of the prosecution case*" (para 15). The appellant contended that a *JC* enquiry had to be undertaken and that it could only be carried out by the Central Criminal Court on a retrial. The Director argued that *JC* could be applied by this Court without the need for a retrial and that the evidence was admissible by reference to *JC*.

170. Having referred in detail to *JC*, as well as a number of international authorities, Charleton J articulated the following compendium of applicable principles (at para 53):

"(1) The decision in JC reverses The People (DPP v Kenny). On this analysis, that decision can no longer be regarded as having any binding effect as an authority.

(2) That decision in JC does not simply reinstate the decision of the Court in The People (AG) v O'Brien insomuch as that case held that evidence obtained in a deliberate and conscious breach of the Constitution, in the sense of an intentional breach rather than merely where the action leading to the breach was itself was deliberate, must be excluded; but subject to extraordinary excusing circumstances. For the reasons set out in the majority judgment and discussed in the judgments of O'Donnell J at [423–431], Clarke J at [823] and MacMenamin J at [956–960] of the report in JC, that test, while a significant advance at the time, did not constitute a final analysis. Accordingly, while the test in JC restates the rule that evidence obtained in deliberate and conscious breach of constitutional rights must be excluded save in extraordinary excusing circumstances, that is now only a component of the applicable rules.

(3) The majority judgments in JC expressly approve the decisions given in respect of unlawful detention in breach of a right to liberty in The People v Madden (which was clearly stated in 1977), The People v O'Loughlin (which followed Madden in 1979), and in The People (DPP) v Healy (reaffirming the relevant principles in 1990). In JC the applicability of the exclusionary principle in those cases was described as "plainly correct, and ... examples of

the court performing the function of ensuring that constitutional rights are respected, upheld and vindicated" at [429]. Those cases rejected explanations that gardaí were, for example, unaware that a period of detention had expired. The proposition that to admit evidence in such circumstances would, as McCarthy J observed in The People (DPP) v Healy, "put a premium on ignorance, indeed ignorance of the law by law enforcement officers" was expressly approved in JC [431]. Such matters as not knowing that there is a legal obligation or not making genuine efforts to abide by the law cannot be considered as mere "inadvertence".

(4) The first limb of the test in JC therefore, restates the approach in The People (AG) v O'Brien, which is that of exclusion of evidence where there has been a deliberate and conscious breach in gathering it, but the full test as set out in JC, goes further.

(5) Hence, where evidence is obtained in breach of a constitutional right, even though the breach is not deliberate and conscious in The People (AG) v O'Brien sense, there is a presumption that such evidence must be excluded; see Clarke J at [871](v).

(6) Such evidence can only be admitted when the breach can be excused. Such admission can occur either (1) where the breach has been occasioned in consequence of a subsequent legal developments, or (2) has occurred due to inadvertence. Reality demands the adoption of the rule in this form, through

acknowledging that Garda officers or other persons conducting searches or obtaining evidence cannot be expected to anticipate the future decisions of the courts. Law enforcement officials are entitled to take the law as it stands as of the time of their actions. Factual errors and understandable human errors fall under the heading of the second class of case. Both classes of case can be understood by reference to the decided case law. JC itself was an example of subsequent legal development; namely the ruling in Damache. The evidence there had been obtained pursuant to a warrant which was valid according to the law as it then stood and it was only because of the subsequent decision of this Court in Damache, that it could be contended that the warrant was invalid. The gardaí and other law enforcement officials are entitled, and in some instances obliged, to take the law as it stands. Consequently, evidence obtained as a result may be admitted. The decision in The People (AG) v O'Brien illustrates the second category. The difference between Cashel Road and Captain's Road, was clearly a simple human error, indicative that there had been an honest attempt to obtain a warrant, but that this was a process required to be undertaken sometimes under pressure of circumstances that can lead to error. The decision is explicable as an instance where there had been a clear intention to respect the constitutional rights involved and to obtain a warrant in respect of the premises and no objection was made when the warrant was executed.

(7) JC also establishes the principle that even where evidence is obtained illegally, without breach of constitutional rights, there is an obligation on the

Court to consider whether it is necessary to exclude the evidence because otherwise if to admit it would render the trial unfair. An example is The People (DPP) v Lawless where the premises searched on a warrant that was in error was not that of the accused but was the dwelling of another person. Hence, there had been an illegality but not a breach of the accused's right to the inviolability of what was not his constitutionally protected dwelling.

(8) JC is authority that any rule of exclusion should "also exclude evidence obtained in reckless or grossly negligent disregard of the Constitution" [487]. Hence, the law does not support a systemisation where inadvertence may be deliberately chosen, as in seeking out an officer, in execution of a warrant or an arrest or the extension of detention, who knows nothing of the investigation, or in flagrant disregard of legal rules, or in doing what suits through advertent blindness to what is required. In considering any question of inadvertence, or deliberate and conscious breach of a constitutional right, consequently, the state of mind under consideration is not only that of individuals, as it were, at the coalface, [850], but also of any other senior official or officials within the relevant enforcement or investigation authority who are involved in a material way in the process. The test also, therefore, necessarily looks to any question of systemic failure within an investigating team and not just the absence of any deliberate and conscious breach on the part of the executing officer.

(9) Finally, the test under which evidence obtained in breach of constitutional rights may be admitted, does not permit the evidence to be admitted if it could

never have been lawfully obtained; see [863]. This, it should be understood, is a further qualification on the admission of evidence. It would be a significant misunderstanding of the test in JC to invite a court merely to consider whether the evidence could have been lawfully obtained, and if so, to admit the evidence. To do so assumes compliance with the Constitution, when the issue arises precisely because there has been a breach. This is, therefore, a backstop test, and a further qualification which may usefully be understood as addressed to circumstances that where evidence was obtained in breach of constitutional rights, and although there was inadvertence or a subsequent legal development, it would nevertheless render the trial unfair to admit such evidence."

171. I emphasise Charleton J's statements that gardaí and law enforcement officers are entitled – if not indeed obliged - to "*take the law as it stands*". Earlier in his judgment, he observed that "*since abiding by the law, even in the investigation of crime, is a paramount consideration, and since the doctrine of precedent and secure reliance on existing legislation are the central supports for legal certainty, where an existing statute is overturned or modified as to its application by judicial decision, as in [Damache], or where the common law develops so as to recognise privacy rights as requiring protection in a previously overlooked area, as in Quirke no 1, there can be no deliberate disregard of the legal order in law-enforcement officers standing on the firm ground of what the law then was"* (para 45). That, he said, was recognised in *JC*, adding that what *"is beyond advertence is the prediction that a section of a statute may be struck down or that the common law will develop in reliance on existing authority, here as to privacy and the security of the dwelling, into a new sphere, here the digital space. Hence, what*

can and should be excused are what is not realisable because the breach at a particular time "derives from subsequent legal developments" which have yet to occur."

172. *Quirke (No 2)* provides further guidance as to the nature of the "*backstop test*" in para 871(vi) of *JC*. The *JC* test does not permit the admission of evidence "*if it could never have been lawfully obtained"* (para 53(9)) or, as Charleton J put it earlier, "*if there is no constitutional path to obtaining the evidence*" the evidence must be excluded (para 51). That is so even if the evidence would otherwise be admissible under *JC* (thus the characterisation of this element of the *JC* test as a "*backstop*"). But, as Charleton J makes clear (see again para 53(9), as well as para 55) it would be to significantly misunderstand this aspect of *JC* to read it as meaning that, provided only that the disputed evidence could have been lawfully obtained, it should therefore be admitted into evidence. That the evidence could have been lawfully obtained does not make it admissible. Admissibility is determined by reference to para 871(ii)-(v) of *JC*. Evidence obtained in deliberate and conscious breach of rights, or in reckless or grossly negligent disregard of the Constitution is inadmissible and is not rendered admissible simply because there was a "*constitutional path*" to obtaining it.

173. Mr Smyth (and Mr McAreavey) and IHREC contend that the SCC (whose analysis on this point was endorsed by the Court of Appeal) gave undue weight to the fact that, even if access to retained traffic and location data had at the relevant time been regulated by an independent authority, the authority would inevitably have permitted access in the circumstances here. Mr Fitzgerald SC characterised that as a "*missing step analysis*" whereby a failure to take an essential step for the lawful gathering of evidence – such

as obtaining a valid search warrant or other necessary authorisation - is wrongly disregarded on the basis that had that step been taken, the warrant or authorisation *would* have been granted. Such an approach, IHREC says, is "*highly corrosive of the very essence of JC*". I see the force in these submissions but, as I have explained, *JC* and *Quirke (No 2)* make it clear that the fact that unconstitutionally obtained evidence might have been constitutionally obtained does *not* mean that such evidence is admissible. The possibility that the evidence could have been obtained lawfully is a necessary but not sufficient condition to its admissibility under *JC*. Nothing in this Court's decision in *People (DPP) v Behan* [2022] IESC 23 suggests any different approach.

Can a JC Inquiry be undertaken by this Court or must there be a retrial?

174. As *JC* and *Quirke (No 2)* illustrate, this Court can undertake a *JC* inquiry on appeal even where no such inquiry was carried out in the trial court. No doubt, as O' Malley J observed in *Behan*, in many appeals it may be difficult for an appellate court to be certain what might have transpired if a *JC* inquiry had been conducted at trial because it will not have the necessary evidence before it (at para 71). But whether that is so in any given appeal depends on the nature of the issues and the nature and scope of the inquiry involved.

175. What factual inquiry is said to be required here? As the Appellants emphasise, this is not a case involving an error on a warrant or the like. Unlike the position in *Quirke (No 2)*, where the state of mind of the Gardaí who had applied for the search warrant was relevant insofar as it might be suggested that they had deliberately concealed from the

District Judge their desire to search the suspect's "*digital space*", Mr Smyth and Mr McAreavey do not argue that the state of mind of the individual Garda officers involved in making the particular access requests here is relevant. The problem here, on their case, was not at the level of individual retention or access under the 2011 Act; the problem was systemic and involved the entire statutory retention and access regime established by that Act.

176. That may well be so. But it is less clear what Mr Smyth and Mr McAreavey say should follow in terms of evidential inquiry. If – as they accept – the state of mind of the individual Garda officers involved in operating the 2011 Act regime is not relevant (and, in any event, there is unchallenged evidence as to their state of mind) whose state of mind ought then to be the focus of inquiry and what would an appropriate *JC* inquiry look like?

177. IHREC, and at times Mr Smyth and Mr McAreavey also, appeared to contend for some wide-ranging inquiry into the state of mind of An Garda Síochána and the State, along the line of the inquiry undertaken by the Central Criminal Court in *Cervi*.

178. In my opinion, such an inquiry is neither mandated by *JC* nor constitutionally appropriate. The subjective state of mind of members of An Garda Síochána, the state of mind of the Government and/or of the Oireachtas and its individual members and the state of mind of the service providers subject to the 2011 Act are not relevant to the application of *JC* here. The assessment that must be undertaken here is an objective one, as indeed Mr Smyth and Mr McAreavey appeared to accept in argument. It follows

in my opinion that there would seem to be no obstacle to this Court conducting the *JC* inquiry arising here.

179. There are, in my view, a number of significant difficulties with the analysis in *Cervi*, not least that Murphy J appears to have attached no weight whatever to this Court's judgments in *Dwyer* and, in particular, the views expressed by all members of the Court that, notwithstanding the CJEU's decision in *Tele2*, the general retention regime provided for in the 2011 Act was, in principle, compatible with the Charter. No reference is made to the fact that, after the CJEU's decision in *Tele2*, numerous further references had been made to the CJEU, indicating a widespread view amongst courts of the different Member States that the issues around general traffic and location data retention and access had not been settled by *Tele2.* Most fundamentally, the ruling in *Cervi* fails to explain how the views of officers of An Garda Síochána, however senior (including the Commissioner) as to the validity of the 2011 Act should have determinative weight in this context. An Garda Síochána exercise neither legislative nor judicial powers in our constitutional order. It is bound by the law enacted by the body to whom exclusive legislative competence is granted by the Constitution – the Oireachtas - subject to the exercise by the body to whom the Constitution entrusts the judicial power – the Article 34 courts – of its power to strike down such legislation or enjoin its operation *pro tem*. In my view – and contrary to the views stated by Murphy J – neither An Garda Síochána as a body, nor the individual members of it, were entitled, less still obliged, to disapply the 2011 Act on the basis of their views as to its consistency with the EU law. Furthermore – and significantly – the inquiry in *Cervi* appears to have been limited to documents passing between An Garda Síochána and the

Department of Justice. The court did not have sight of the legal advice available to those bodies or to the Government, particularly in the context of the proceedings in *Dwyer*. At best, the inquiry in *Cervi* gave only a very limited insight into the state of mind of the State (even if that was the appropriate focus of inquiry, which in my view it was not).

Applying JC Here

180. The starting point for analysis is the 2011 Act. It was enacted by the Oireachtas in exercise of its legislative competence under Article 15.1 of the Constitution. That the Act was enacted to give effect to the Retention Directive does not alter its fundamental constitutional status as a matter of Irish law. Unless and until repealed or amended by the Oireachtas, or struck down by a court of competent jurisdiction, the 2011 Act declared the law and An Garda Síochána and service providers alike were bound by, and entitled to rely on, its provisions.

181. In our constitutional democracy, founded on the rule of law, neither private persons (including private companies) nor public bodies or agencies, including the Government itself, are free to determine which enactments of the Oireachtas to be bound by or free to disregard the law enacted by the Oireachtas: see for example *Duggan v An Taoiseach* [1989] ILRM 710. Acts of the Oireachtas are presumed valid and, in the event of a challenge to the validity of such an Act, it is a matter for the courts, and for the courts alone, to adjudicate on that challenge. In fact, Article 34 of the Constitution vests the jurisdiction to determine the constitutional validity of laws enacted by the Oireachtas

in the High Court, the Court of Appeal and, ultimately, this Court, to the exclusion of all other courts. Even where the constitutional validity of an enactment is challenged, it remains in force and continues to operate, unless and until a competent court enjoins its enforcement by interlocutory order. A high threshold applies to the making of any such order, precisely because of the presumption of constitutionality: *Carrigaline Community Television Broadcasting Limited v Minister for Transport, Energy and Communications* [1994] 2 IR 359 and *MD (a minor) v Ireland* [2009] IEHC 206, [2009] 3 IR 690.

182. Thus, as a matter of Irish law, it is clear that, as long as the 2011 Act remained on the statute book, service providers within the meaning of section 1(1) – including the telecommunications service providers to whom access requests were directed here and who complied with such requests - were *required* to retain the data specified in section 3 and schedule 2 of the Act and were *required* by section 7 of the Act to comply with access requests made to them by (*inter alia*) a member of the Garda Síochána not below the rank of Chief Superintendent in accordance with section 6. As a matter of Irish law, a service provider could not lawfully have declined to retain Schedule 2 data, or refused to provide access to such data to An Garda Síochána, on the basis that it considered and/or had been advised that the Act was unconstitutional or otherwise invalid. If a service provider considered that the 2011 Act was invalid, it was open to it to bring proceedings to challenge it. It could then have sought an injunction suspending the operation of the Act pending the resolution of that challenge. But, absent such an injunction, it would nonetheless have been bound to continue to comply with the Act. Of course, no such challenge was in fact brought by any service provider.

183. While the 2011 Act may not have imposed any express *duties* on An Garda Síochána, one of An Garda Síochána's core functions is *"bringing criminals to justice, including by detecting and investigating crime"* (section 7(1)(f) of the Garda Síochána Act 2005). In seeking to discharge that function, members of An Garda Síochána were entitled to rely on the provisions of the 2011 Act, unless and until a competent court determined otherwise. They were, as this Court made clear in *Quirke*, "*entitled to take the law as it stands as of the time of their actions*" (para 53(6)).

184. The position here is thus on all fours with *JC*. That there may have been doubts as to the validity of the 2011 Act does not affect the proper approach to assessing the circumstances in which the traffic and location data evidence was obtained. That evidence was retained "*on the basis of the law as it stood"* and accessed in accordance with an authorisation *"issued in furtherance of a statutory provision which enjoyed the presumption of constitutionality*" (Clarke J, at para 874). Here, as in *JC,* the steps taken by the relevant members of An Garda Síochána were "*properly taken on foot of [an Act] of the Oireachtas … in a bona fide, genuine and well-founded belief as their legality"* (MacMenamin J, at para 958).

185. But the position here is said to be different because it was apparent from at least the CJEU's decision in *Tele2* (if not its earlier decision in *Digital Rights Ireland*) that the 2011 Act was invalid. Furthermore, it is said, the nature of that invalidity alters the paradigm: whatever the position under Irish law, An Garda Síochána were under an EU law obligation to *disapply* the 2011 Act and their continued reliance on the Act in such

circumstances means that they were guilty of a "*deliberate and conscious breach*" of the Appellant's rights.

186. The basic premise of that argument - the contention that the 2011 Act was clearly contrary to the Charter and that its continued operation therefore involved a "*deliberate and conscious breach*" of the Charter – collides head-on with this Court's decision in *Dwyer*. That decision is fundamentally inconsistent with any suggestion that it was clear from *Digital Rights Ireland* and/or *Tele2* that the retention and/or access provisions of the 2011 Act were contrary to EU law. I do not, in this context, overlook the High Court's decision in *Dwyer* in December 2018. But this Court took a very different view of the impugned provisions of the 2011 Act – particularly the retention provisions - than the High Court did. As already explained, the Court was unanimously of the view that general retention was in principle permissible, though it also considered (Charleton J dissenting) that the issue was not so clear as to exclude the need for a reference. While it took a somewhat different view of the access regime – inclining to the view that the safeguards in the 2011 Act were not sufficiently robust - again it did not regard the issue as clear.

187. Accordingly, the argument that it was clear, or ought to have been clear, to An Garda Síochána (or the Government or the Oireachtas) that the 2011 Act was invalid at any point prior to the CJEU's decision in *GD* must be rejected in light of our decision in *Dwyer*.

188. In this context, it is neither necessary nor appropriate to look behind this Court's decision in *Dwyer*. But, even if one was to do so, it appears to me that the references made in, and the decisions of the CJEU in, *La Quadrature du Net* and *Prokuratuur*, as well as the CJEU's decision in *GD* itself, are fundamentally at odds with the suggestion that the legal position was clear from *Digital Rights Ireland* or *Tele2.*

189. I do not overlook the *Report of the Law on the Retention of and Access to Communications Data* prepared by the late John Murray (April 2017) ("*the Murray Report*"). But, while the views of the former Chief Justice (and former judge of the CJEU) are naturally worthy of the greatest respect, they cannot be given primacy over the views reached by this Court, on the basis of extensive evidence and argument, in *Dwyer*.

190. Assessed objectively, *JC* compels the conclusion that the breach of the Charter here was not "*deliberate and conscious*" in the *JC* sense. The 2011 Act was on the statute-book when the data at issue in this appeal was retained and accessed (between June and December 2017). By analogy with *JC* itself (where the search warrant had been issued pursuant to a statutory provision that was subsequently struck down in *Damache*), the illegality here arose as a result of a "*subsequent legal development*", namely the combined effect of the CJEU's judgment in *GD* and the declaration subsequently granted by this Court when the proceedings came back before it.

191. The argument that An Garda Síochána ought to have *disapplied* the 2011 Act on the basis that it was clearly contrary to EU law faces a further and distinct difficulty in my

view. The decision of the CJEU (Grand Chamber) in Case C-378/17 *Minister for Justice and Equality v Workplace Relations Commission* EU:C:2018:979 was cited in support of the contention that An Garda Síochána were entitled – indeed obliged – to disregard the Act if they were of the view – as it is said they were or ought to have been - that it conflicted with the Charter.

192. *Minister for Justice and Equality v Workplace Relations Commission* was a reference from this Court: [2017] IESC 43, [2020] 2 IR 244. The point at issue was whether EU law required that the Workplace Relations Commission (WRC) should, in the exercise of its statutory adjudicative functions, have the power to "*disapply*" a provision of national law, even where, as a matter of Irish law, such a power could only be exercised by the High Court (or, on appeal, by the Court of Appeal and/or this Court). The point arose in related age discrimination claims brought before the WRC in circumstances where the applicants had been excluded from recruitment to An Garda Síochána by virtue of being older than the maximum age for recruitment established by regulations made by the Minister for Justice under the Garda Síochána Act 2005. The Minister contended that the WRC lacked jurisdiction to entertain the complaints as it was bound by the regulations. The WRC nonetheless decided to proceed. The Minister and the Commissioner then brought judicial review proceedings seeking to prohibit the WRC from adjudicating on the complaints. The High Court made an order of prohibition.

193. On the WRC's appeal, this Court (per Clarke J, MacMenamin, Laffoy, Dunne and O'Malley JJ. agreeing) held that, as a matter of national law, tribunals such as the WRC did not have, and could not constitutionally be conferred with, the power to set aside or

disapply enacted legislation (there was, in Clarke J's view, no real distinction between a power to set aside and a power to disapply national law in this context): paras 26-29. That position stemmed "*from fundamental constitutional provisions which require that important or significant legal questions are determined by courts established under the Constitution rather than by statutory bodies or tribunals*" (para 30). Nevertheless, the Court considered it appropriate to make a reference to the CJEU directed to the issue of whether EU law required that the WRC should have such a jurisdiction.

194. The CJEU (Grand Chamber) held that EU law, in particular the principle of primacy, precludes national legislation under which a national body established by law in order to ensure enforcement of EU law in a particular area lacks jurisdiction to decide to disapply a rule of national law that is contrary to EU law (Judgment, para 52). Such a power arose only in a "*specific case*" and did not involve a power to strike down legislation, such that it was no longer valid for any purpose (Judgment, para 33). A key element in the Court's analysis was that the WRC had been established by the legislature for the purpose of complying with Ireland's obligations under Article 9 of Directive 2000/78. As a body conferred with the power to ensure enforcement of the principle of non-discrimination in employment and occupation, if a discrimination dispute was before the WRC, then the principle of primacy required it to ensure that EU law was fully effective (Judgment, para 45). The fact that the WRC was a "*court or tribunal*" within the meaning of Article 267 TFEU, so that it could refer questions to the CJEU, was a further factor relied on by the court (Judgment, para 47).

195. In my view, there is no meaningful analogy with *Minister for Justice and Equality v Workplace Relations Commission* here. There appears to me to be a significant distinction between the function and application of specific EU legislative measures such as Directive 2000/78 on the one hand and that of the Charter on the other. In the first place, the Charter applies to Member States only when implementing EU law. The investigation of crime under the 2005 Act is not generally an EU law function or one governed by EU law. Furthermore, while it is clear from *Minister for Justice and Equality v Workplace Relations Commission* and the caselaw referred to at para 30 of the Court's judgment that the principle of primacy is not limited in its application to courts and tribunals but also applies to all organs of the State, including administrative bodies, it could not be the case that EU law requires that every administrative body should be empowered to act as a quasi-constitutional court, entitled – indeed, on this theory, obliged – to disapply provisions of national law, based on its – inexpert - assessment of complex questions as to the meaning and effect of the Charter. Such a scenario is entirely remote from that at issue in *Minister for Justice and Equality v Workplace Relations Commission* where the WRC was a "*court or tribunal*" within the meaning of Article 267 TFEU, constituted by law as an expert body in the specific area of employment law, authorised by law to adjudicate on discrimination claims and subject to review by the courts. A scenario where individual members of An Garda Síochána, or individual Districts or even An Garda Síochána as a whole could decide to "*disapply*" an enactment of the Oireachtas based on their view that it was contrary to the Charter would fundamentally undermine legal certainty and the rule of law.

196. Furthermore, it was not suggested that the principle in *Minister for Justice and Equality v Workplace Relations Commission* might, on any view, extend to service providers – who, under the 2011 Act, were subject to the data *retention* obligation.

197. It was said in argument that *JC* should not be interpreted as effectively giving *carte blanche* to the admissibility of evidence where its unlawfulness results from unconstitutional or invalid legislation, rather than any narrower issue such as an error in a warrant or some other flawed procedural step. But that submission appears to rest on a misunderstanding of the essential purpose of the exclusionary rule. It is not directed at the legislature. It is (at least in the criminal law context) directed at investigating and enforcement agencies, primarily (though not exclusively) An Garda Síochána. The constitutional value that it serves (and which justifies the exclusion of otherwise relevant and probative evidence) is the need to ensure that such agencies operate properly within the law and that evidence is gathered within the limits prescribed by law (*JC*, at para 827). The admission of evidence obtained otherwise than in accordance with law may, at least in certain circumstances, be seen to condone misconduct and may bring the administration of justice into disrepute. The admission of evidence that was obtained in accordance with the law as it stood at the time, but where such law was subsequently struck down, does not raise the same issues. That no doubt is what MacMenamin J had in mind when making the observations he did in *JC*, para 958, which have been set out already.

198. It may be that there could be circumstances in which An Garda Síochána (or other such law enforcement agency) could not properly rely on an existing legislative power, even

in the absence of a court order striking it down. For instance, if in the aftermath of this Court's decision in *Damache* striking down section 29 of the Offences Against the State Act 1939, An Garda Síochána relied on an identically worded provision in another statute to obtain a search warrant, a significant question might then arise as to the admissibility of evidence obtained on foot of such a warrant. But that is not this case. Nor is this a case where the disputed evidence was obtained after the High Court had declared the relevant provisions of the 2011 Act invalid. In his judgment in *JC* (para 873) Clarke J tentatively suggested that it was possible that different considerations might arise in such a scenario. But, again, that is not this case – the traffic and location data at issue here was accessed in 2017, well before the first High Court decision in *Dwyer*. In any event, the declaratory orders made by the High Court were subsequently stayed pending appeal and, on that basis, there would appear to be a strong argument that An Garda Síochána was entitled to continue to rely on the 2011 Act pending the resolution of that appeal. However, as the issue does not arise here it would not be appropriate to express any concluded view on it. But it is in any event significant that Clarke J contemplated a *judicial* determination by a court of competent jurisdiction in this context and expressly excluded any weight being given to public debate or controversy questioning the validity of an Act (para 874).

199. For the reasons just set out, there was no conscious or deliberate breach of Charter rights here. Any breach of the Appellants' Charter rights derived from subsequent legal developments, as that expression was used in *JC* and *Quirke (No 2)*, namely the decision of the CJEU in *GD* and this Court's subsequent Order of 26 May 2022.

200. Hogan J reaches a different view in his judgment. I readily acknowledge the force of his analysis but nonetheless disagree with it. In my respectful view, it does not give sufficient weight to the fact that the issue of admissibility here arises from a finding of invalidity of legislation enacted by the Oireachtas, rather than any narrower issue such as an error in a warrant or some other flawed procedural step. For the reasons set out above, and in particular in para [199] above, that is in my view a very significant distinction in this context. Furthermore, as will be evident from the discussion above, I take a different view of this Court's decision in *Dwyer* than my colleague does. In particular, I differ from my colleague in the weight that I would accord the stated view of this Court that a general data retention regime for the purposes of combatting serious crime was, in principle, compatible with EU law and its view that, while the compatibility of the access regime in the 2011 Act was more questionable, it was *not* clear.

201. The admissibility of the evidence here does not turn on whether, viewed objectively, the continued use of the 2011 Act was "*perfectly legal*". Such a threshold is not suggested by or consistent with *JC* or *Quirke (No 2).* Nor is it supported by the decision of the Supreme Court of Canada in *R v Fearon*. *R v Fearon* did not involve any issue of a search conducted within the four corners of a statutory regime subsequently declared to be invalid; rather it involved a decision by law enforcement officers to search a mobile phone without first seeking a warrant. Warrantless searches of mobile phones were subsequently held to be unlawful but the evidence obtained was nonetheless held to be admissible because in Cromwell J's words (at para 95), the "*police simply did some thing that they believed on reasonable grounds to be lawful*

and were proven wrong, after the fact, by developments in the jurisprudence." Here, of course, the Gardaí involved in authorising access to the traffic and location data all give evidence that they believed that the 2011 Act was valid and that it was lawful to proceed as they did. But that evidence of subjective belief aside, for the reasons set out already, it was objectively reasonable – and therefore it was not objectively negligent or reckless - for the Gardaí to continue to rely on the 2011 Act while it remained on the statute-book and in the absence of a decision of a court of competent jurisdiction striking it down. That is not inconsistent with *JC*. As I have explained, *JC* makes it clear that special considerations apply where (as here) issues of admissibility of evidence arise consequent on the subsequent striking down of legislation where that evidence was gathered in accordance with that legislation. That there may have been doubts as to the validity of the 2011 Act and/or that, objectively, there was a risk that its provisions might ultimately be struck down does not alter the application of the *JC* test or point to the exclusion of the evidence at issue here. On the contrary, in *JC* this Court acknowledged that doubts had been expressed about the validity of section 29 but made it clear that such doubts or uncertainties did not warrant the exclusion of evidence obtained on foot of a search conducted on foot of a warrant granted under that section. The threshold is not one of doubt or risk.

202. But *JC* and *Quirke (No 2)* present a further issue that must be addressed before the admissibility of the traffic and location data here can be determined. It concerns the application of the so-called "*backstop*". It is apparent from *JC* that this aspect of the test is intended to ensure that evidence that has, in fact, been obtained unconstitutionally should not be admitted, whatever the mitigating circumstances, if it could not have been

obtained in a constitutional manner or, in the words of Charleton J in *Quirke (No 2)* "*if there [was] no constitutional path to obtaining the evidence.*" As Charleton J emphasised in *Quirke (No 2)*, this part of the *JC* test does *not* mean that unconstitutionally obtained evidence should be admitted provided only that it could have been obtained in a constitutional manner. That the evidence could have been obtained constitutionally is a necessary but not sufficient, condition for its admissibility. It is important to re-iterate that position here in light of the concerns expressed both by the Appellants and IHREC on this point.

203. *Quirke (No 2)* suggests that the backstop may usefully be understood as addressed to circumstances where the admission of evidence that is otherwise admissible by reference to the *JC* test would nonetheless render the trial unfair (para 53(9)). *JC* and *Quirke (No 2)* otherwise provide very limited guidance as to the concrete application of the backstop, though the manner in which the test was initially formulated in *JC* suggests that it is primarily concerned with cases of inadvertent constitutional breach, rather than cases in which the unconstitutionality arose because of a subsequent legal development. This is, of course, a subsequent legal development case.

204. The application of the backstop necessarily requires engagement in a counterfactual exercise. In some cases, that may be straightforward. In *JC*, it was clear to this Court that, if section 29 had not been there, a search warrant could and would have been granted by a court pursuant to some different statutory provision authorising searches. That was also the case in *Behan*. In *Quirke (No 2)*, it was clear that a search warrant encompassing a search of the suspect's "*digital space*" could validly have been granted

to the Gardaí, whether pursuant to section 10 of the Criminal Justice (Miscellaneous Provisions) Act 1997 (as amended) or, alternatively, pursuant to some other statutory provision.

205. That counterfactual is more difficult where – as here – the subsequent legal development involves the striking down of a previously applicable statutory regime making special provision for the retention of, and access to, a particular category of evidence. As of 2017 – when the traffic and location data at issue in this appeal was retained by the relevant service providers and subsequently accessed by An Garda Síochána – the rules for retention and access were those set out in the 2011 Act. There was no parallel statutory regime. Some 4½ years later, the operative provisions of the 2011 Act were struck down.

206. I do not read *JC* as requiring the Director to retrospectively identify a hypothetical alternative legislative regime that could have been in place in 2017 in lieu of the 2011 Act, on the basis of which the court can be satisfied that the specific data at issue here *would* have been lawfully retained and accessed. There is too much uncertainty and contingency for any such exercise to be meaningful or reliable. Rather, it seems to me that this aspect of the *JC* test is intended to exclude evidence otherwise admissible in accordance with *JC* which *could* never have been obtained lawfully – in other words evidence obtained by a method and/or in circumstances irreconcilable with fundamental constitutional norms. As was discussed at the hearing, evidence obtained in breach of an operative privilege such as legal professional privilege or marital privilege would

appear to fall into this category. So would evidence gathered by inherently unconstitutional means – such as by oppression, intimidation, torture or duress.[19]

207. It is clear that traffic and location data has no privileged status under either the Constitution or the Charter. It may lawfully be gathered, retained and accessed by a variety of actors in a variety of circumstances. Its retention is not inherently unconstitutional or contrary to the Charter. Although the general retention of such data is generally impermissible under the ePrivacy Directive and the Charter, there are nonetheless many circumstances in which such data may properly be retained. Traffic and location data may be subject to general retention for purposes of national security (*La Quadrature du Net*). It is true of course that the circumstances in which such data may be retained for the purposes of the investigation and prosecution of serious crime are significantly more restricted. Even so, *La Quadrature du Net*, *GD* and *Skynet* all emphasise that there are many circumstances in which such data may be retained consistently with the Charter, including circumstances where such data may be retained (and thereafter accessed) on a general basis by reference to geographic criteria, not linked to any particular suspicion of individual communication services users and also circumstances where such data may be retained on the basis of "*expedited retention*" (or as this Court referred to it in *Dwyer*, "*quick freeze*"). *Skynet* emphasises that the category of circumstances in which traffic and location data may lawfully be retained for criminal investigation purposes is not closed (subject always to the exclusion of any regime of general and indiscriminate retention for that purpose).

[19] See Charleton & McDermott, para 4.15.

208. That being so, it appears to me that the traffic and location data at issue here *could* have been *retained* in a manner compatible with the Charter (and the Constitution). That, in my view, is all that the backstop requires. It does not require the court to hypothesise an alternative legislative regime and to hypothesise how that regime might have operated in 2017 and whether, in particular, its operation *would* have led to the retention of the traffic and location data at issue here.

209. As for *access*, it is clear that such data *could* have been accessed in a manner compatible with the Charter. Access here was sought for the purpose of investigating a very serious crime. There was a substantial basis for considering that the data sought was relevant to the investigation and the access requests were narrowly-tailored. In the event that access had been subject to a regime of prior independent authorisation, there can be no doubt that access *could* have been authorised consistently with the Charter.

210. It follows that the backstop does not require the exclusion of the traffic and location data evidence here.

211. If, as *Quirke (No 2)* seems to suggest, the backstop is properly understood as being directed at more general considerations of fairness, it is, in my view, equally clear that no basis for excluding the evidence arises here. Critically, the reliability of the evidence has never been disputed. The gravity of the "*structural*" breaches of EU law involved here, as identified by the CJEU in *GD*, is fully reflected by the application of the *JC* test. The breaches to which the Appellants, as individuals, can point to are not, in my

view, of such dimensions as to mandate exclusion. Certainly, their personal/private information was retained unlawfully. But such retention took place in accordance with an enactment of the Oireachtas. Furthermore, only a limited amount of personal/private information was accessed and then only for the purposes of investigating a very serious criminal offence. Although access was not governed by a system of prior independent authorisation, it was not unregulated either. The 2011 Act limited access for the purpose of the investigation of a "*serious offence*" (as well as the protection of State security and the saving of human life) and there were administrative arrangements in place intended to operate as a filter on access requests.

212. I accept that the *JC* test is the product of a balancing of rights. Evidence obtained as a result of a conscious or reckless breach of the Constitution is inadmissible; evidence obtained as a result of an inadvertent breach or a subsequent legal development may be admitted. As IHREC argued, where evidence has been obtained as a result of a conscious or reckless breach of the Constitution (or, here, the Charter), *JC* requires its exclusion (at least in the absence of extraordinary excusing circumstances). *JC* does not permit any further balancing exercise whereby such evidence is admitted because of its probative effects, because of the seriousness of the offence or because of the weight to be given to the rights of the community or victims of crime. But that is not the position here. The evidence at issue here was *not* obtained in conscious or reckless breach of the Charter. The question being addressed here is not whether, if the *JC* test for admissibility is not met, the circumstances are such that the court can or should decide to *admit* the evidence anyway; rather, it is whether, even if the conditions for

admissibility set out in *JC* are satisfied - as in my view they are satisfied here - the court should nonetheless exercise a discretion to *exclude* the evidence.

213. Nor, in my view, would it bring the administration of justice into disrepute or undermine the integrity of the court to admit the evidence here. In his judgment in *JC*, O' Donnell J accepted that there may be circumstances in which the *admission* of unconstitutionally obtained evidence could bring the administration of justice into disrepute. But, as he also emphasised, the *exclusion* of reliable evidence is apt to impair the truth finding function of the administration of justice and to bring it into disrepute. The Canadian jurisprudence provides useful guidance in this context. Section 24(2) of the Canadian Charter of Rights and Freedoms provides that evidence obtained in breach of the Charter shall be excluded if, in all the circumstances, its admission would bring the administration of justice into disrepute. I have already referred to the test articulated in *R v Grant*, which was applied in *R v Spencer* [2014] 2 SCR 212. *R v Grant* was also discussed in *JC* and *Quirke (No 2)*. Making all due allowance for the nature of the unlawfulness here and its impact on the interests of Mr Smyth and Mr McAreavey, it appears to me that the community's interest in the adjudication of the case against them on its merits weighed decisively in favour of the admission of the evidence and it is the *exclusion* of that evidence rather than its *admission* that would bring the administration of justice into disrepute. The considerations I have mentioned above – including the nature and probative value of the evidence, the fact that it was gathered in accordance with the 2011 Act, the view taken by this Court in *Dwyer* of the lawfulness of the retention regime created by the Act, the gravity of the crime being investigated and the

limited and targeted nature of the access obtained - are all significant factors in this context.

214. For these reasons, which differ from the reasoning of the SCC and the Court of Appeal, I would hold that the traffic and location data evidence was properly admitted at trial. Issue 1(c) above must therefore be answered no – the SCC did not err in admitting the evidence.

CONCLUSIONS

215. I shall briefly summarise my principal conclusions:

(1) The question of the admissibility of the traffic and location data here is governed by Irish law, subject to the principles of equivalence and effectiveness.

(2) The test for the admissibility of evidence obtained in breach of constitutional rights is that set out in *JC* and *Quirke (No 2).*

(3) That is so whether the constitutional right at issue is expressly provided for in the Constitution or is an unenumerated or derived right.

(4) The traffic and location data at issue here must be regarded as having been retained and accessed in breach of the Charter and not merely in breach of the ePrivacy Directive.

(5) The admissibility of the traffic and location data evidence therefore falls to be assessed by reference to *JC* as to apply any less-exacting test would not be consistent with the principles of equivalence and effectiveness in that it would effectively accord rights guaranteed by the Charter a lesser status than rights protected by the Constitution. Such would not be consistent with the obligations of the State – and of this Court – to respect, and give full effect to, EU law.

(6) The answer to the first admissibility issue is, therefore, that the test for admissibility is indeed that set out in *JC*.

(7) The fact that Mr Smyth and McAreavey did not assert or accept ownership of the 691 phone or the 773 phone respectively does not have the significance suggested by the Director. The Director sought to rely on the traffic and call data relating to the 691 and 773 numbers on the basis that those numbers had been, respectively, in the control and use of Mr Smyth and Mr McAreavey at all material times. In those circumstances, Mr Smyth and Mr McAreavey were entitled to object to the admissibility of that evidence on the basis that, on the Director's case, the traffic and call data constituted their personal data and that such data had been retained and accessed in breach of the Directive of the Charter.

(7) The answer to the second admissibility issue is therefore that, in considering the admissibility of the phone location and call data here, the fact that neither Mr Smyth or Mr McAreavey asserted or accepted ownership of the 691 phone or the 773 phone is not material.

(8) The application of *JC* here does not involve or require any factual inquiry or investigation but, rather, an objective assessment of whether it was reasonable for An Garda Síochána to rely on the provisions of the 2011 Act or whether such reliance involved a "*deliberate or conscious*" breach of the Charter. This Court is in a position to carry out that assessment.

(9) *JC* compels the conclusion that the breach of the Charter here was not "*deliberate and conscious*" in the sense used in *JC*. The 2011 Act was on the statute-book when the data at issue in this appeal was retained and accessed (between June and December 2017). An Garda Síochána was entitled to rely on it. Even if there may be circumstances where a law enacted by the Oireachtas is so manifestly unconstitutional (and/or contrary to the Charter) that, even in the absence of an order of a court of competent jurisdiction declaring that law invalid, it could be reckless or negligent for a law enforcement body to rely upon it – and *JC* suggests not – such is not the position here. This Court's decision in *Dwyer* is wholly inconsistent with the argument that, as of 2017, the 2011 Act was so clearly contrary to the Charter that it could not properly or reasonably be relied on by An Garda Síochána.

(9) By analogy with *JC* itself (where the search warrant had been issued pursuant to a statutory provision subsequently struck down in *Damache*), the illegality here arose as a result of a "*subsequent legal development*", namely the combined effect of the CJEU's judgment in *GD* and the declaration subsequently granted by this Court when the proceedings came back before it.

(10) In the circumstances, the traffic and location data at issue here was *prima facie* admissible under *JC*.

(11) As regards the so-called *JC* "*backstop*", the traffic and location data at issue here *could* have been retained and accessed in a manner compatible with the Charter. Access

here was sought for the purpose of investigating a very serious crime. That is all that the backstop requires. It does not require the court to hypothesise an alternative legislative regime and to hypothesise how that regime might have operated in 2017 and whether, in particular, its operation *would* have led to the retention of the traffic and location data at issue here.

(12) If, as *Quirke (No 2)* seems to suggest, the backstop is properly understood as being directed at more general considerations of fairness, no basis for excluding the evidence arises here. The community's interest in the effective adjudication of the case against Mr Smyth and Mr McAreavey on its merits weighed decisively in favour of the admission of the evidence and it is the *exclusion* of that evidence rather than its *admission* that would bring the administration of justice into disrepute. Considerations including the nature and probative value of the evidence, the fact that it was gathered in accordance with the 2011 Act, the view taken by this Court in *Dwyer* of the lawfulness of the retention regime created by the Act, the gravity of the crime being investigated and the limited and targeted nature of the access obtained are all significant factors weighing in favour of the admission of the evidence.

(13) It follows – to address the third and final admissibility issue – that the SCC did not err in admitting the traffic and location evidence.

216. Mr Smyth's appeal must therefore be dismissed.

APPENDIX

CHRONOLOGY

Date	Event
5 May 2010	High Court (McKechnie J) gives judgment in *Digital Rights Ireland* making a reference to the CJEU ([2010] IEHC 221, [2010] 3 IR 251)
13 December 2013	Opinion of AG Cruz Villalón in *Digital Rights Ireland* (C-293/12) EU:C:2013:845
8 April 2014	Judgment of the CJEU (Grand Chamber) in *Digital Rights Ireland* EU:C:2014:238
15 April 2015	Supreme Court decision in *People (DPP) v JC* [2015] IESC 31, [2017] 1 IR 417
17 July 2015	EWHC (Divisional Court) decision in *Watson* ([2015] EWHC 2092 (Admin))
20 November 2015	Court of Appeal of England and Wales's decision in *Watson* ([2015] EWCA Civ 1185, [2017] 1 All 63)
19 July 2016	Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698 *Tele2 Sverige* & *Watson* EU:C:2016:572
21 December 2016	CJEU (Grand Chamber) Judgment in Joined Cases C-203/15 and C-698 *Tele2 Sverige* & *Watson* EU:C:2016:970

Date	Event
April 2017	Report of former CJ Murray – *Review of the Law on the Retention of and Access to Communications Data*
10 May 2017	Shooting of James Gately
June – December 2017	Various Section 6 access request sent to telecommunications service providers re (*inter alia*) the 691 and 773 numbers
6 December 2018	First High Court decision in *Dwyer* v *Commissioner of An Garda Síochána* [2018] IEHC 685, [2019] 1 ILRM 461
11 January 2019	Supplemental High Court decision in *Dwyer* (form of order/stay) [2019] IEHC 48, [2019] 1 ILRM 523
15 January 2020	Opinion of Advocate General Sánchez-Bordona in Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and others* EU:C:2020:6
24 February 2020	Supreme Court decision in *Dwyer* [2020] 1 ILRM 389- Court decides (Charleton J dissenting) to make a reference to the CJEU
6 October 2020	Judgment of the CJEU (Grand Chamber) in Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and others* EU:C:2020:791
9 October 2020 – 5 November 2020	Trial in the Special Criminal Court
5 January 2021	Special Criminal Court gives judgment finding both accused guilty
2 March 2021	Judgment of the CJEU (Grand Chamber) in Case C-746/18

Date	Event
	HK v Prokuratuur EU:C:2021:152
18 November 2021	Opinion of Advocate General Sánchez-Bordona in Case C-140/20 *GD v Commissioner of An Garda Síochána (Dwyer)* EU:C:2022:258
10 February 2022	Court of Appeal hears appeals in *Smyth & McAreavey*
5 April 2022	Judgment of the CJEU (Grand Chamber) in *Dwyer*.
26 May 2022	Supreme Court makes formal Order dismissing appeal in *Dwyer* and affirming the declaration granted by the High Court
28 July 2022	Court of Appeal gives judgment dismissing appeals [2022] IECA 182
16 December 2022	Supreme Court gives leave to appeal