THE PRESIDENT AND MEMBERS OF THE
COURT OF JUSTICE OF THE EUROPEAN UNION

In **Joined Cases C-339/20 and C-397/20**

V.D. and S.R.

Applicants

WRITTEN OBSERVATIONS OF IRELAND

Ireland, represented by Maria Browne, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as Agent, accepting service by e-Curia and with an address at the Embassy of Ireland, 28 route d'Arlon, Luxembourg, and assisted by David Fennelly BL of the Bar of Ireland, has the honour to submit written observations in these proceedings, the subject of references for preliminary ruling from the *Cour de cassation* (France) lodged on 20 August 2020.

Dated 15 December 2020

I. Introduction

1. Ireland submits these Written Observations pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union.

2. In these References which have been joined for the purposes of the procedure and of the judgment, the *Cour de cassation* (France) ("**the Referring Court**") has asked a number of questions relating to the consistency of national data retention legislation with EU law and whether, in the event that the national legislation is found to be inconsistent with EU law, national courts have the power to maintain the effects of such legislation on a temporary basis in the interests of legal certainty.

3. Ireland will address the legal framework and the detailed questions in Sections III to V of its Observations. Before doing so, it is necessary to make the following preliminary observations on the broader context in which these questions are raised (Section II).

II. Preliminary Observations: the Necessity for the Court to Reconsider Its Case-Law on Targeted Retention

4. In referring these questions, the *Cour de cassation* joins the growing number of national courts, often national courts of final appeal, which have sought clarity from the Court of Justice on the compatibility of national data retention legislation with EU law in the wake of this Court's judgment in *Tele2 Sverige/Watson*.[1] It is apparent from these references that the Court's jurisprudence, particularly on the concept of so-called "*targeted retention*", is a source of serious concern for national courts across the Union.

5. What is novel about the present References is that the Referring Court raises these questions in the context of the national implementation of EU legislation on insider dealing and market abuse: Directive 2003/6/EC which has now been replaced by Regulation (EU) No. 596/2014. Under this legislation, national competent authorities

[1] C-207/16, *Ministerio Fiscal*; C-623/17, *Privacy International*; C-511/18, *Quadrature du Net & Others*; C-512/18, *French Data Network & Others*; C-520/18, *Ordre des barreaux francophones et germanophone*; C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*; C-793/19, *SpaceNet AG*; C-794/19, *Telekom Deutschland GmbH*; C-140/20, *Commissioner of the Garda Síochána and Others.*

must have, among their supervisory and investigatory powers to combat market abuse, the power to require *inter alia* existing data traffic records from telecommunications operators where there is a reasonable suspicion of infringement and where such records are relevant for the investigation of such infringement. As recital 65 of Regulation (EU) No. 596/2014 makes clear, existing recordings of telephone conversations and data traffic records – from investment firms, credit institutions and financial institutions or from telecommunications operators – "*constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation*". If such records were not retained and could not be accessed, the ability of national authorities to combat these criminal activities – proscribed in accordance with EU law – would be fundamentally undermined.

6. In the national proceedings, the Applicants have argued that – notwithstanding the relevant provisions of EU law on insider dealing and market abuse – national legislation providing for a system of general retention of telecommunications metadata is incompatible with Article 15(1) of Directive 2002/58, as interpreted in this Court's judgments in *Tele2 Sverige/Watson* and *Ministerio Fiscal*. For its part, the Indictment Division of the Court of Appeal of Paris considered that no invalidity could arise from the application of national provisions which themselves comply with a European regulation binding and directly applicable in the domestic legal order. It is from the decisions of the Indictment Division that the Applicants have brought their appeal to the *Cour de cassation*.

The Judgments of 6 October 2020

7. Since the lodging of the References, this Court has delivered, on 6 October 2020, its judgments in Case C-623/17, *Privacy International* and Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*.[2] In its judgment in *La Quadrature du Net and Others*, the Court has – with limited exceptions – maintained the position laid down in *Tele2 Sverige/Watson* that EU law precludes national legislation providing for the "*general and indiscriminate retention*" of traffic and

[2] Judgments of the Court of 6 October 2020: *Privacy International*, C-623/17, EU:C:2020:790; *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791.

location data of telecommunications users but that EU law does not prevent Member States from adopting legislation permitting, as a preventive measure, "*the targeted retention of traffic and location data*" for the purposes of *inter alia* combating serious crime.[3]

8. The Court has recognised, however, that national legislation could allow, for the purposes of safeguarding national security, "*recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable*" subject to certain further conditions being fulfilled.[4] The Court has also stated that national legislation could – for the purposes of safeguarding national security, combating serious crime, and preventing serious threats to public security – provide for 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*" and of "*data relating to the civil identity of users of electronic communications systems*".[5] In addition, the Court has concluded that national measures could provide for recourse to an instruction to service providers to undertake, subject to certain conditions, "*the expedited retention of traffic and location data*".[6]

9. What is the source of these evolving and increasingly elaborate principles in the Court's case-law? According to the Court, they derive from Article 15(1) of Directive 2002/58/EC ("**the ePrivacy Directive**"), interpreted in light of Articles 7, 8, 11 and 52 of the Charter of Fundamental Rights. It is true that Article 15(1) of the ePrivacy Directive permits Member States to adopt legislative measures restricting the rights and obligations laid down in the Directive for certain stated purposes, including national security, defence, public security and law enforcement purposes, and, to this end, to adopt *inter alia* "*legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph*". It is also true that such

[3] *La Quadrature du Net and Others*, paras. 141-147.
[4] *La Quadrature du Net and Others*, para. 168.
[5] *La Quadrature du Net and Others*, para. 168.
[6] *La Quadrature du Net and Others*, para. 168.

measures must be in accordance with the general principles of Community law, which include fundamental rights now enshrined in the Charter. However, Article 15(1) does not provide, and was never intended to provide, a detailed framework for the regulation of data retention at EU level in the manner in which it is now being developed in the case-law of the Court. Despite this, the Court has divined in Article 15(1) of the ePrivacy Directive the evolving and increasingly elaborate principles identified above.

The fundamental difficulty with targeted retention

10. The fundamental difficulty with the Court's approach in this regard is that, in order to be effective as a law enforcement or security tool and thus meet the first step of any proportionality analysis, data retention must be general in scope at the retention regime. As Ireland and many other parties have previously submitted to the Court, the model of targeted retention – first identified by the Court in *Tele2 Sverige/Watson* and since elaborated upon in *La Quadrature du Net & Others* – is not only unworkable in practice but is also deeply problematic in principle. This is not merely a matter of legal submission. It has been confirmed by the findings of fact of the Supreme Court of Ireland in the pending reference in Case C-140/20, *Commissioner of the Garda Síochána and Others.*

11. This fundamental difficulty is borne out by the experience on the ground since the Court's judgment in *Tele2 Sverige/Watson*. While the law on data retention has been under review and subject to change across Member States, no Member State has been able to design and bring forward national legislation providing for a model of targeted data retention of the kind envisaged by this Court in its case-law. Nor has the European Commission proposed any such data retention legislation. The reason for this is simple: it is not possible to do so. Any such regime would be ineffective in achieving its intended purpose and would in itself give rise to serious fundamental rights concerns.

12. It follows that, far from bringing clarity to these issues, the Court's recent judgment in *La Quadrature du Net & Others* has only served to underline the difficulties with the Court's case-law in this field. These difficulties arise not merely at the level of principle; they have very significant and ongoing practical consequences for the work

of law enforcement and security authorities and for national courts across the Member States.

13. In the circumstances, Ireland respectfully asks that the Court re-consider its conclusion on targeted retention in light of the evidence which has now been put before it. If the Court's case-law were to stand in its present form, it would have very grave and detrimental implications for the fight against serious crime and the fight against threats to public and national security across the Member States and would represent a significant impediment to European integration in these critically important and extremely sensitive fields. This is a matter of deep concern to Ireland and other Member States.

III. Legal Framework

14. In addition to Article 15(1) of the ePrivacy Directive which has been referred to above, the Referring Court has made reference to certain provisions of Directive 2003/6/EC ("**the 2003 Directive**") on insider dealing and market manipulation and its successor, Regulation (EU) No 596/2014 ("**the 2014 Regulation**") on market abuse. It appears from the References that the criminal investigations in the underlying cases commenced prior to the coming into force of the 2014 Regulation.

15. The 2003 Directive required the Member States to prohibit in national law insider dealing, market manipulation and related practices, and to designate a single administrative authority with competence to ensure that the provisions of the 2003 Directive were applied. According to Article 12 of the 2003 Directive, the competent authority "*shall be given all supervisory and investigatory powers that are necessary for the exercise of its functions*". These powers were to be exercised in conformity with national law and included at least the right to *inter alia*: (a) have access to any document in any form whatsoever, and to receive a copy of it; and (d) require existing telephone and existing data traffic records.

16. For its part, the 2014 Regulation, which replaced the 2003 Directive with effect from 3 July 2016, provides in Article 23(2) that the competent administrative authority for the

purposes of the Regulation "*shall have, in accordance with national law, at least the following supervisory and investigatory powers*":

> *....(g) to require existing recordings of telephone conversations, electronic communications or data traffic records held by investment firms, credit institutions or financial institutions*
>
> *(h) to require, insofar as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of an infringement and where such records may be relevant to the investigation of an infringement of point (a) or (b) of Article 14 or Article 15; ....*

17. It follows that, in order to enable competent national authorities to investigate and prosecute insider dealing, market abuse and related practices, the EU legislature required that such authorities would have the power to require existing data traffic records held by a telecommunications operator where there is a reasonable suspicion of an infringement of the provisions of the Regulation and the records are relevant to the investigation of that infringement. Without access to such evidence, national authorities would be unable to effectively discharge their duties. This is reflected in recital 65, quoted above, which recognises that the evidence referred to in paragraphs (g) and (h) of Article 23(2) "*constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation*".

18. As the Referring Court has observed, "*the inside information likely to form the material element of unlawful market practices was essentially verbal and secret*".[7] Indeed, by their very nature, offences of this kind will tend to be carried out under the veil of secrecy, with every effort being taken to avoid detection. In these circumstances, if national authorities were unable to access existing data traffic records in accordance with national law, they would be deprived of a critical source of evidence. It is against this backdrop that the Referring Court's questions must be considered.

IV. The Referring Court's First Question

[7] Reference in C-397/20, para. 37; Reference in C-339/20, para. 38.

19. By its first question, the Referring Court asks in essence whether the relevant provisions of the 2003 Directive and the 2014 Regulation cited above imply that the national legislature must be able to require electronic communications operators to retain connection data on a temporary but general basis in order to enable the competent administrative authority to exercise its powers under the 2003 Directive and 2014 Regulation where there are grounds to suspect persons of being involved in conduct proscribed in accordance with those legislative instruments.

20. It is significant in this regard that both the 2003 Directive and the 2014 Regulation refer to "*existing data traffic records*". In its first question, the Referring Court is concerned specifically with the exercise by national authorities of their powers "*in cases where there are grounds to suspect that the records so linked to the subject matter of the investigation may prove relevant to the production of evidence of the actual commission of the breach, to the extent, in particular, that they offer a means of tracing the contacts established by the persons concerned before the suspicions emerged*".

21. According to the Court's judgment in *Tele2 Sverige/Watson*, Article 15(1) of Directive 2002/58/EC, interpreted in light of the Charter, precludes national legislation providing for general and indiscriminate retention of traffic and location data but EU law does not preclude "*a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary*".[8] The Court continued:

> *...the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public*

[8] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 108.

security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.[9]

The Court's notion of targeted retention is therefore premised on it being possible to identify in advance "*a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences*", for example by setting limits using a geographical criterion.

22. In its recent judgment in *La Quadrature du Net & Others*, the Court has further elaborated upon these statements in the following passages:

149 In that regard, it must be made clear that the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned.

150 The limits on a measure providing for the retention of traffic and location data may also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences (see, to that effect, judgment of 21 December 2016, Tele2, C‑203/15 and C‑698/15, EU:C:2016:970, paragraph 111). Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.

[9] Judgment of 21 December 2016 in *Tele2 Sverige/Watson*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111.

Lack of evidence that targeted retention is feasible or effective

23. However, in neither judgment has the Court identified any evidence in support of its conclusion that such a model of targeted retention – based on personal and/or geographical profiling – would be effective for the purposes of fighting serious crime.

24. While, in its most recent judgment, the Court has specified that geographical targeting must be based on "*objective and non-discriminatory factors*", it remains entirely unclear how such a form of geographical targeting could be implemented and/or effective to combat crime in practice. Such a regime would be readily circumvented by criminals and other persons who pose a serious threat to public and national security. Indeed, in his Opinion in *La Quadrature du Net & Others*, Advocate General Campos Sánchez-Bordona acknowledged the significant problems with the Court's approach in *Tele2 Sverige/Watson*, relying *inter alia* on the submissions of the European Data Protection Supervisor.[10]

25. The regime proposed by the Court in *Tele2 Sverige/Watson* and more recently *La Quadrature du Net & Others* simply does not correspond to the real world of law enforcement and safeguarding public and/or national security. If it were possible to identify in advance the persons and/or areas likely to be implicated in serious crime or threats to public or national security, such crimes and threats could be prevented and access to retained telecommunications data would not be necessary for the purposes of investigating and prosecuting such matters. However, the experience of Member States confirms that, in very many cases, it is simply not possible to identify such persons in advance, particularly in the context of many forms of serious crime and serious threats to public security.

A model of targeted retention would fundamentally undermine the investigation and prosecution of the crime of insider dealing

[10] Opinion of Advocate General Campos Sánchez-Bordona dated 15 January 2020, *Ordre des barreaux*, EU:C:2020:7, paragraphs 88, 89 and 92.

26. The very value and utility of retained telecommunications metadata is that it enables the authorities to identify persons suspected of such crimes and threats to security who are not otherwise known to the authorities. The offences at issue in the national proceedings provide a vivid practical example of this issue. By their nature, insider dealing and other market abuse offences are carried out in a covert and secret fashion, designed to evade detection. The persons engaged in such offences are unlikely to come to the attention of law enforcement authorities or to live or work in areas with a high incidence of serious crime or particular vulnerability to such crime.

27. For this reason, as the EU legislature has stated in recital 65 to the 2014 Regulation, access to existing data traffic records is often a crucial and in some cases the only source of evidence. If national authorities were limited to retention of such data on a prospective basis once suspicions emerged, it would not be possible in many cases to detect, investigate and prosecute such offences. The national authorities would be deprived of an essential source of evidence.

28. Moreover, in a context such as this, it is difficult to conceive how a system of targeted retention of the kind envisaged by the Court in its judgments – whether by reference to a particular group of persons (for example, members of a particular profession) or a geographical area (for example, parts of a city where such professionals are based) – could work in practice, let alone be justifiable in principle.

29. It follows that, if it were not permissible for Member States to provide for the general retention of data traffic records by telecommunications service providers, the competent authorities in Member States would not be able to carry out their functions effectively under the 2003 Directive and now the 2014 Regulation and, as a result, the conduct which must be prohibited under those instruments would, in many cases, not be amenable to investigation and/or prosecution. Article 15(1) of the ePrivacy Directive does not compel such a conclusion. It would be a direct consequence of the Court's judgments in *Tele2 Sverige/Watson* and *La Quadrature du Net & Others.*

Evidence before the Court confirms that data retention is only effective if it is general scope at the retention stage

30. This problem is of course not confined to the offences proscribed in accordance with the 2003 Directive and/or the 2014 Regulation. Similar challenges arise in the detection, investigation and prosecution of serious crime generally. This includes both well-established forms of serious crime in which telecommunications play an increasingly significant role and other forms of serious crime, such as complex organised crime and cybercrime which will be an ever-more prominent feature of law enforcement in the digital age.

31. In this context, it is relevant to refer to the findings of fact of the Supreme Court of Ireland in the pending reference in Case C-140/20, *Commissioner of the Garda Síochána and Others*. For the first time, in this reference, the Court of Justice has the benefit of findings of fact on the different forms of data retention and their feasibility which are based on evidence properly adduced before the national court. In its reference, the Supreme Court found as follows:

    (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.

    In the words of the Supreme Court, "*it is not possible to access that which has not been retained*".[11]

32. These conclusions are consistent with the findings of a detailed study recently carried out on behalf of the European Commission.[12] This study once again confirms that data

[11] Reference in Case C-140/20, paragraph 8.5.
[12] European Commission/Milieu, *Study on the retention of electronic communications non-content data for law enforcement purposes* – Final Report, December 2020.

preservation or quick freeze is not a suitable alternative to general data retention. This was already clear at the time the EU's own Data Retention Directive was initially proposed.[13] Notwithstanding this position, in *Tele2 Sverige/Watson*, the Court proposed a model of targeted retention which is similar in character to data preservation. In its recent judgment in *La Quadrature du Net & Others*, the Court has gone further, re-characterising the model of expedited data preservation provided for in Article 16 of the Budapest Convention on Cybercrime as a form of "*expedited retention of traffic and location data for the purpose of combating serious crime*" permissible under EU law subject to certain conditions.[14] While data preservation may complement data retention in the investigation of serious crime (including cybercrime), it is not an effective alternative to or substitute for data retention.[15]

33. In summary, not only is there no evidence which supports the feasibility or effectiveness of the Court's proposed model of targeted retention, such evidence as there is before the Court demonstrates that data retention is only effective as a law enforcement and security tool if it is general in scope at the retention stage and that a model of targeted retention would not be effective to achieve the objectives of fighting serious crime or safeguarding public or national security.

34. The Court's judgment in *La Quadrature du Net & Others* does recognise the force of this position but only to a limited extent in the context of retention for national security purposes and the retention of data relating to IP addresses and the civil identity of users. In light of the evidence referred to above, it is incumbent on the Court to reconsider its position in respect of generalised retention of traffic and location data for the purposes of fighting serious crime and threats to public security.

[13] In proposing this legislation, the Commission had considered but rejected alternative measures such as data preservation or 'quick freeze' systems: see Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, SEC(2005) 1131, at 13.

[14] *La Quadrature du Net and Others*, paras. 160-165.

[15] See e.g. Centre for Strategy and Evaluation Studies, *Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries* (November 2012).

35. The facts of the present case underline why it is important for the Court to do so. If it were not possible to access existing data records held by telecommunications service providers, as required under the 2003 Directive and the 2014 Regulation, it would not be possible to conduct an effective investigation and prosecution into the crime of insider dealing and there would be a very real and significant risk that these crimes – proscribed in accordance with EU law – would go unpunished.

36. More generally, in the investigation of serious crime and security threats, it is frequently the traffic and location data which are of most value to national authorities. If such data are not retained, they will simply not be available for the national authorities in cases where it emerges that they may be highly relevant, even critical, to the investigation and/or prosecution of a serious crime or security threat. As a result, it may not be possible to identify appropriate leads or evidence which are necessary for the effective investigation and prosecution of such conduct.

37. In its judgment in *La Quadrature du Net & Others* the Court has expressed the view that whether or not retained data are subsequently used is "*irrelevant*" because access to retained data is a separate interference with fundamental rights.[16] However in truth the degree of interference which data retention entails can only be properly assessed and understood in light of the conditions governing access to such data.

38. Although the Court has expressed the view in *La Quadrature du Net & Others* that it is for the Court to "*strike a balance between the various interests and rights at issue*",[17] in Ireland's submission, this is first and foremost the role of the legislature, whether at EU or national level, which has access to the full range of evidence and information on the appropriate policy and legislative options. The Court's judgments in *Tele2 Sverige/Watson* and *La Quadrature du Net & Others* demonstrate the very real difficulties that can arise – both at the level of principle and in practice – when the Court develops detailed rules governing a complex policy area in the absence of an appropriate legislative framework and evidential basis.

[16] *La Quadrature du Net and Others*, para. 116.
[17] *La Quadrature du Net and Others*, para. 127.

39. In circumstances where, on the evidence before the Court, only a model of general data retention (and not a model of targeted retention) would be effective to achieve the objectives of fighting serious crime and safeguarding public and/or national security, neither Article 15(1) of the ePrivacy Directive nor any other provision of EU law ought to be interpreted as preventing Member States from adopting legislative measures providing for the general retention of telecommunications metadata for those purposes subject to appropriate safeguards governing access to such retained data. Any other conclusion would seriously prejudice Member States' capacity to fight serious crime and security threats within the Union and would compel Member States to adopt a model of data retention which could not be justified on the available evidence.

40. For all these reasons, in answer to the Referring Court's first question, Ireland submits that the relevant provisions of the 2003 Directive and the 2014 Regulation do indeed imply that the national legislature must be able to require electronic communications operators to retain connection data on a temporary but general basis.

V. The Referring Court's Second and Third Questions

41. By its second question, the Referring Court asks whether – in the event that the Court's answer to the first question is such as to prompt the Referring Court to form the view that the French legislation on the retention of connection data is not consistent with EU law – the effects of that legislation could be "*temporarily maintained in order to avoid legal uncertainty and to enable data previously collected and retained to be used for one of the objectives pursued by that legislation*". For the reasons set out above, Ireland's primary submission is that, in view of the answer to the Referring Court's first question, it may not be strictly necessary for the Court to answer this question. However, without prejudice to that submission, Ireland makes the following observations.

42. Similarly, by its third question, the Referring Court asks whether a national court may temporarily maintain the effects of legislation enabling the officials of an independent administrative authority responsible for investigating market abuse to obtain connection data without prior review by a court or another independent administrative authority. In this regard, Ireland notes that the *Conseil constitutionnel* found that the

relevant French legislation was contrary to fundamental rights guaranteed under French constitutional law. As Ireland has submitted in Case C-140/20, the concept of an independent administrative authority is not one defined in either the EU Treaties or in EU legislation and accordingly is not an autonomous concept of EU law. For present purposes, however, the sole issue raised by the Referring Court is the power of national courts to maintain on a temporary basis the effects of legislation inconsistent with EU law.

43. In its judgment of 6 October 2020, the Court addressed this issue in its answer to the third question raised by the Belgian Constitutional Court in Case C-520/18, *Ordre des barreaux*. Having reaffirmed the principle of the primacy of EU law, it held that only the Court of Justice could "*in exceptional cases, on the basis of overriding considerations of legal certainty*" allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto.[18] According to the Court, maintaining the effects of national legislation contrary to Article 15(1) of the ePrivacy Directive, read in light of the Charter, "*would mean that the legislation would continue to impose on providers of electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data has been retained*".[19] On this basis, the Court concluded that the referring court in that case could not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality.[20] Indeed, the Court went even further, laying down certain principles applicable to the admissibility of evidence obtained in breach of EU law, notwithstanding its recognition that this was a matter properly for the national courts.[21]

The Lack of Legal Certainty arising from the Court's Evolving Case-Law

44. In Ireland's submission, the Court's approach in *La Quadrature du Net & Others* fails to have any regard to the fact that the primary source of the lack of legal certainty in this field – which has had such far-reaching implications for national law enforcement

[18] *La Quadrature du Net & Others*, para. 216.
[19] *La Quadrature du Net & Others*, para. 219.
[20] *La Quadrature du Net & Others*, para. 220.
[21] *La Quadrature du Net & Others*, paras. 221-227.

and security authorities – lies in the changing and still uncertain principles of European Union law governing this issue.

45. In this regard, it is important to recall that, up until 8 April 2014 when the Court delivered its judgment in *Digital Rights Ireland & Others*,[22] EU Member States were required – as a matter of EU law – to have in place a system of general retention of telecommunications metadata. Indeed, the Commission brought infringement proceedings against a number of Member States, including Ireland, for failure to transpose the Data Retention Directive into national law.

46. In the intervening period, very significant uncertainty has prevailed in respect of the status and validity of national data retention regimes:

    (i) In its judgment of 21 December 2016 in *Tele2 Sverige/Watson*, as noted above, the Court held that EU law precluded national measures providing for general and indiscriminate data retention for the purpose of fighting serious crime but did not prevent the adoption, as a preventive measure, of a "*targeted retention*" regime, a concept which was entirely unknown in the law of the Union and its Member States.

    (ii) In its judgment of 2 October 2018 in *Ministerio Fiscal*, the Court concluded that Article 15(1) of the ePrivacy Directive did not preclude national authorities from accessing mobile phone subscriber data for the purposes of preventing, investigating, detecting and prosecuting criminal offences.[23]

    (iii) In its judgment of 6 October 2020 in *La Quadrature du Net & Others*, as discussed above, the Court has laid further and more detailed principles governing the nature and form of national data retention measures which may be adopted in accordance with Article 15(1) of the ePrivacy Directive.

[22] Judgment of 8 April 2014, *Digital Rights Ireland & Others*, C-293/12 and C-594/12, EU:C:2014:238.
[23] Judgment of 2 October 2018, *Ministerio Fiscal*, Case C-207/16, EU:C:2018:788.

(iv) At present, in addition to these References, four further references are pending before the Court at various stages of the procedure: C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*; C-793/19, *SpaceNet AG*; C-794/19, *Telekom Deutschland GmbH*; C-140/20, *Commissioner of the Garda Síochána and Others.*

47. The long line of references from national courts demonstrates that the principles of European Union law in this field have been anything but "*clear and precise*", as the Court itself requires of national rules in this field.[24] On the contrary, those principles – which have little if any textual basis in Article 15(1) of the ePrivacy Directive itself – have evolved considerably, often in significant and unexpected ways, in response to the questions referred by national courts.

The Consequences of the Lack of Legal Certainty

48. Moreover, for the reasons identified above, the practical effect of the Court's evolving case-law – and, in particular, its concept of targeted retention – has been that neither national legislatures nor the EU legislature have been able to bring forward, still less adopt, data retention measures which would be consistent with this case-law. This is a matter of grave and growing concern for Ireland and other Member States.

49. In particular, the resultant lack of legal certainty has had very significant adverse consequences for the ability of national law enforcement and security authorities to discharge their responsibilities in the fight against serious crime and threats to public and national security. It has also had far-reaching implications for past and present criminal investigations and prosecutions, casting doubt over the admissibility of evidence based on retained telecommunications metadata in national legal systems.

50. All of this underlines the vital necessity of the Court reconsidering its case-law so that Member States and/or the EU legislature can bring forward data retention legislation which is compatible with the requirements of EU law. For so long as the Court maintains its jurisprudence on targeted retention, it will remain impossible for the

[24] See e.g. *La Quadrature du Net & Others*, paras. 132 and 168.

Member States and/or the EU legislature to bring forward appropriate amending legislation.

51. For these reasons, Ireland submits that overriding considerations of legal certainty require that Member States courts be permitted to maintain the effects of national data retention legislation which is found to be inconsistent with EU law on a temporary basis pending the adoption of revised legislation.

VI. Conclusion

52. For these reasons, Ireland submits that the Court should respond as follows to the first question referred by the *Cour de cassation* (France):

> **With respect to the first question**, in accordance with Article 12(2)(a) and (d) of the 2003 Directive and Article 23(2)(g) and (h) of the 2014 Regulation, national legislatures must be able to require electronic communications operators to retain connection data on a temporary but general basis.
>
> **With respect to the second and third questions**, overriding considerations of legal certainty require that Member States courts be permitted to maintain the effects of national data retention legislation which is found to be inconsistent with EU law on a temporary basis pending the adoption of revised legislation.
>
> Dated 15 December 2020

Signed: Tony Joyce
Agent for Ireland
on behalf of Maria Browne, Chief State Solicitor.

Signed: Juliana Quaney
Agent for Ireland
on behalf of Maria Browne, Chief State Solicitor.