OPINION OF ADVOCATE GENERAL

CAMPOS SÁNCHEZ-BORDONA

delivered on 18 November 2021(1)

Case C 140/20

G.D.

v

The Commissioner of the Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General

(Request for a preliminary ruling from the Supreme Court (Ireland))

(Reference for a preliminary ruling – Telecommunications – Processing of personal data – Confidentiality of communications – Electronic communications service providers – Directive 2002/58/EC – Article 15(1) – Article 4(2) TEU – Charter of Fundamental Rights of the European Union – Articles 7, 8, 11 and 52(1) – General and indiscriminate retention of traffic and location data – Access to retained data – Use of retained data as evidence in criminal proceedings)

1. This request for a preliminary ruling – to which can be added the requests in Joined Cases C 793/19, *SpaceNet*, and C 794/19, *Telekom Deutschland*, in which I am also delivering the Opinion (2) today – demonstrates, once again, the concern raised in some Member States by the Court's case-law on the retention of and access to personal data generated in the electronic communications sector.

2. In the Opinions in Cases C 511/18 and C 512/18, *La Quadrature du Net and Others*, (3) and C 520/18, *Ordre des barreaux francophones et germanophone and Others*, (4) I stated that the following were, at that time, the most important milestones in that case-law:

– the judgment of 8 April 2014, *Digital Rights Ireland and Others*, (5) which ruled that Directive 2006/24/EC (6) was invalid in that it entailed disproportionate interference with the rights recognised by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter');

– the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, (7) which held that Article 15(1) of Directive 2002/58/EC (8) precludes national legislation which, for the purpose of fighting serious crime, provides for the general and indiscriminate retention of all traffic and location data;

– the judgment of 2 October 2018, *Ministerio Fiscal*, (9) which confirmed the interpretation of Article 15(1) of Directive 2002/58, pointing out the importance of the principle of proportionality in that regard.

3. In 2018, a number of courts of certain Member States submitted requests for a preliminary ruling to the Court, expressing their uncertainties concerning whether those judgments (of 2014, 2016 and 2018) might deprive national authorities of a necessary tool for safeguarding national security and fighting crime and terrorism.

4. Four of those requests for a preliminary ruling resulted in the judgments in *Privacy International* (10) and *La Quadrature du Net and Others*, (11) both of 6 October 2020, which essentially confirmed the case-law laid down in the judgment in *Tele2 Sverige*, while introducing a number of supplementary qualifications.

5. As a result of their origin (the Grand Chamber of the Court of Justice), their content and their intention of explaining in detail, in a dialogue with the referring courts, the grounds which, nevertheless, justified the views set out therein, those two 'recapitulatory' judgments of 6 October 2020 might be expected to have resolved the debate. Any other request for preliminary ruling on the same subject would therefore warrant a reasoned order pursuant to Article 99 of the Rules of Procedure of the Court of Justice.

6. However, prior to 6 October 2020, the Registry of the Court had received three other requests for a preliminary ruling (in this case and in Joined Cases C-793/19 and C-794/19), which again called into question the case-law laid down in connection with Article 15(1) of Directive 2002/58.

7. The Court made each of the referring courts aware of the judgments of 6 October 2020, in case it should wish to withdraw its request for a preliminary ruling. When the referring court insisted on maintaining its request, as I shall explain below, (12) it was decided not to apply Article 99 of the Rules of Procedure and that the Grand Chamber of the Court of Justice would reply to it.

I. Legislative framework

A. European Union law. Directive 2002/58

8. According to Article 5(1) ('Confidentiality of the communications'):

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

9. Article 6 ('Traffic data') provides:

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

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

…'

10. Article 15 (‘Application of certain provisions of Directive 95/46/EC’) (13) provides in paragraph 1:

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

B. National law. Communications (Retention of Data) Act 2011 (‘the 2011 Act’)

11. The Supreme Court’s presentation of national law in paragraph 3 of its order for reference is as follows:

– ‘The 2011 Act was enacted with the express purpose of giving effect to … Directive [2006/54].

– … s. 3 of the Act requires all service providers to retain the “fixed network telephony and mobile telephony data” for a period of two years.

– This is data which identifies the source, the destination, and the date and time of the start and end of a communication, the type of communication involved, and the type of and the geographic location of the communications equipment used. The content of communications does not fall within this type of data.

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

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

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

– At the times relevant to this investigation, all disclosure requests had to be approved in the first instance by a superintendent (or an inspector acting in that capacity) and were then sent to be processed by the TLU. Investigators were directed to include sufficient detail in the request to enable an informed decision to be made, and to bear in mind that the chief superintendent might have to justify the decision later in court or to the designated High Court judge. The TLU and the detective chief superintendent are required to verify the legality, proportionality and necessity of disclosure

requests sought by members of An Garda Siochana. Applications deemed not to comply with the requirements of the law or of internal garda protocols were returned for clarification or additional information. Under a Memorandum of Understanding issued in May 2011, service providers would not process requests for call related data that did not come through this process. The TLU is also subject to audit by the Data Protection Commissioner.'

12. Appendix I to the order for reference includes some additional information about the provisions of the 2011 Act. According to that information:

– Section 1 of the 2011 Act defines 'data' as 'traffic data or location data and the related data necessary to identify the subscriber or user'.

– Section 6(1) of the 2011 Act permits a Garda officer, in the terms set out above, to access such data if that officer considers that the data is required for: '(a) the prevention, detection, investigation or prosecution of a serious offence; (b) the safeguarding of the security of the State; and (c) the saving of human life'.

II. Facts, dispute and questions referred for a preliminary ruling

13. G.D. was sentenced in 2015 to life imprisonment for murder. During the appeal proceedings before the Irish Court of Appeal, he unsuccessfully contested the admissibility of certain incriminating evidence based on telephony data retained under national law.

14. In parallel to the criminal appeal, G.D. commenced *civil* proceedings (14) before the High Court (Ireland) in order to challenge the validity of a number of provisions of the 2011 Act, pursuant to which the telephony data concerned was retained and could be accessed.

15. By judgment of 6 December 2018, the High Court granted G.D.'s application seeking a declaration that Section 6(1)(a) of the 2011 Act was inconsistent with Article 15(1) of Directive 2002/58, in conjunction with Articles 7, 8 and 52(1) of the Charter.

16. The Irish Government appealed against that judgment to the Supreme Court (Ireland), which has referred the following questions to the Court of Justice for a preliminary ruling:

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

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

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

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

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

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

17. The Supreme Court states that evidence of the kind tendered in the criminal proceedings against G.D. is decisive for the detection and prosecution of certain categories of serious offence. It points out that, if the universal retention of metadata were not permitted, even with any conditions of access which may be in place, it would not be possible to identify or properly prosecute the perpetrators of many such offences.

18. In that connection, the Supreme Court has made the following findings:

– 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;

– 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;

– 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.

III. Procedure before the Court of Justice

19. The request for a preliminary ruling was received at the Registry of the Court on 25 March 2020.

20. Written observations were lodged by G.D., the Commissioner of the Garda Síochána, the Belgian, Czech, Cypriot, Danish, Spanish, Estonian, Finnish, French, Netherlands, Polish, Portuguese and Swedish Governments, and the European Commission.

21. The referring court was invited to state its views on the possible withdrawal of the reference for a preliminary ruling following the judgment in *La Quadrature du Net*, and it indicated, by letter received at the Registry on 27 October 2020, that it intended to continue with the reference. (15)

22. The hearing, held jointly with that in Joined Cases C 793/19, *SpaceNet*, and C 794/19, *Telekom Deutschland*, took place on 13 September 2021. It was attended by those who had lodged written observations (with the exception of the Belgian, Czech and Portuguese Governments) and the European Data Protection Supervisor.

IV. Analysis

A. Introductory observation

23. Most of the parties who have entered an appearance in the proceedings agree that the six questions referred for a preliminary ruling by the Supreme Court on the subject of Article 15(1) of Directive 2002/58 can be grouped together in three blocks, relating to:

– the lawfulness of a scheme of general and indiscriminate *retention* of data, of itself and in connection with the fight against serious crime (Questions 1, 2 and 4).

– the features required, where appropriate, of *access* to retained data (Question 3).

– the possible temporal limitation of the effects of any declaration of incompatibility with EU law of the national legislation in this field (Questions 5 and 6).

24. In my view, all those questions were answered in full in the judgments in *La Quadrature du Net*, and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*. (16)

25. In relation to the judgment in *La Quadrature du Net*, after that judgment was notified to it, the referring court was particularly laconic in its reply to the Court.

26. Having acknowledged that that judgment assists in clarifying EU law, the referring court merely stated that 'the type of case which underlies the proceedings in which the reference of the Supreme Court has been made differs significantly from the type of situations which underlay the proceedings giving rise to that judgment.' (17)

27. Those assertions of the referring court, made after its request for a preliminary ruling, do not call into question the case-law laid down in *La Quadrature du Net* (as some of the governments intervening in the proceedings have done) or seek clarifications concerning the content of that judgment.

28. Although the 'situations which underlay' (18) the proceedings giving rise to the judgment in *La Quadrature du Net* differed from that underlying this reference for a preliminary ruling, the important point is that the case-law laid down in general terms in that judgment by the Court of Justice applies *erga omnes* and is binding on all the courts of the Member States in relation to the interpretation of Directive 2002/58.

29. As regards access to retained data, I also believe that the judgment in *Prokuratuur*, which was given after the national court's decision to continue with the reference for a preliminary ruling, dispels the uncertainties raised in the reference.

30. In those circumstances, and unlike the approach I have taken in the Opinion in *SpaceNet* and *Deutsche Telekom*, (19) I shall confine myself in this Opinion to establishing the consequences for this reference for a preliminary ruling, as it was originally formulated, which flow from the judgments in *La Quadrature du Net* and *Prokuratuur*.

B. General and indiscriminate retention of traffic and location data (Questions 1, 2 and 4)

31. The referring court essentially asks:

– whether Article 15(1) of Directive 2002/58, interpreted in the light of the Charter, precludes a general data retention regime;

– whether, in examining national legislation which creates a regime for the general and indiscriminate retention of traffic and location data, subject to strict controls, it is relevant that service providers may lawfully retain those data for their own commercial purposes and that such retention may be required for reasons of national security;

– whether national legislation continues to be incompatible with Article 15 of Directive 2002/58 if that legislation requires the general retention of such data for the purposes of combating serious crime.

32. As I also argue in the Opinion in *SpaceNet* and *Telekom Deutschland*, (20) the answer to those questions cannot differ from the answer given by the Court in the judgment in *La Quadrature du Net*, which *reviewed* the case-law in that regard.

33. It is important to recall, first, the case-law laid down by the Court in that judgment, paragraph 168 of which summarises it as follows:

> 'Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that:
>
> – 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, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;
>
> – 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;
>
> – provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, 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;
>
> – provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;
>
> – allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, 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.'

34. The central idea of the Court's case-law in relation to Directive 2002/58 is that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise. (21)

35. Article 15(1) of Directive 2002/58 permits exceptions to the obligation to ensure the confidentiality of personal data and to the corresponding obligations. The judgment in *La Quadrature du Net* examines at length the balance struck between those exceptions and the fundamental rights whose exercise may be affected. (22)

36. According to the Court, the general and indiscriminate retention of traffic and location data can be justified only by the objective of safeguarding national security, the importance of which 'goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58'. (23)

37. In that case (national security), the Court held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, 'does not, in principle, preclude *a legislative measure which permits the competent authorities to order* providers of electronic communications services *to retain* traffic and location data of all users of electronic communications systems *for a limited period of time*, as long as 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'. (24)

38. Admittedly, those requirements lead to a more rigorous and stricter regime than that which follows from the case-law of the European Court of Human Rights (ECtHR) in relation to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). The fact that 'the meaning and scope' of the rights in the Charter which correspond to rights in the ECHR must be the same as those laid down by the ECHR does not prevent EU law from providing more extensive protection, in accordance with Article 52(3) *in fine* of the Charter.

39. Moreover, the case-law of the ECtHR in its judgments of 25 May 2021, *Big Brother Watch and Others v. United Kingdom* (25) and *Centrum för Rätvisa v. Sweden*, (26) and of 4 December 2015, *Zakharov v. Russia*, (27) concerns situations which, as was the prevailing view at the hearing, are not comparable to that at issue in this reference for a preliminary ruling. The solution to these must be sought by applying national provisions which are deemed to be consistent with the *exhaustive* rules laid down in Directive 2002/58, as interpreted by the Court.

40. Whatever the view regarding reliance on national security, in the judgment in *La Quadrature du Net*, as a ground for lifting, under certain conditions, the prohibition on the general and indiscriminate retention of traffic and location data (in my opinion, the limits set by the Court are excessively broad), the requirements set out in paragraphs 137 to 139 of that judgment must be met.

41. In any other circumstances, it will be necessary to consider whether the national legislation is underpinned by sufficiently *selective* criteria such that it complies with the conditions which, in accordance with the case-law of the Court, can justify a particularly serious interference with the fundamental rights concerned, such as the retention of data.

42. There would be a failure to respect the meaning of the judgment in *La Quadrature du Net* if the statements made therein concerning national security could be applied to offences, including serious offences, which do not threaten national security but rather public security and other interests protected by law.

43. This is why the Court carefully differentiated between national legislative measures which provide for the preventive, general and indiscriminate retention of traffic and location data in order to safeguard national security (paragraphs 134 to 139 of the judgment in *La Quadrature du Net*) and measures for combating crime and

safeguarding public security (paragraphs 140 to 151 of that judgment). The two types of measure cannot have the same scope or else that distinction would be rendered meaningless.

44. Measures providing for the retention of traffic and location data for the purposes of combating serious crime are, I repeat, set out in paragraphs 140 to 151 of the judgment in *La Quadrature du Net*. In addition to these, and having the same purpose, are measures authorising the preventive retention of IP addresses and of data relating to a person's civil identity (paragraphs 152 to 159 of that judgment) and the 'expedited retention' of traffic and location data (paragraphs 160 to 166 of that judgment).

45. The referring court asks, in particular, about the effect of 'the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of [Directive 2002/58]'.

46. The judgment in *La Quadrature du Net* links the data which those operators store for commercial purposes with the purpose for which the data were collected and only permits the 'expedited retention' of those data in the terms set out in paragraphs 160 to 166 of that judgment, cited above.

47. National security requirements permit, in the manner and subject to the guarantees and restrictions set out in the judgment in *La Quadrature du Net*, the general and indiscriminate retention of traffic and location data. However, the same does not occur in relation to the aim of prosecuting offences, including serious offences, as referred to in Section 6(1)(a) of the 2011 Act, with which the reference for a preliminary ruling is concerned.

48. As regards the difficulties created by the *targeted retention* of traffic and location data, (28) I refer, in addition, to points 43 to 50 of my Opinion in *SpaceNet* and *Telekom Deutschland*.

49. Since the Court cannot be asked to take on a regulatory role and spell out which categories of data can be retained and for how long, (29) nor would it be appropriate for the Court, when interpreting Article 15(1) of Directive 2002/58, to take on the role of legislature by inserting into that provision intermediate categories between national security and public security, in order to apply to the latter the requirements attached to the former.

50. As the Court has held, 'the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives'. (30)

51. The proposal that the Commission put forward at the hearing (31) (the introduction of a *tertium genus* of infringements) would extend to the point of uncertainty the sole ground capable of justifying the general and indiscriminate retention of traffic and location data (national security), placing threats to national security on the same footing as threats resulting from serious crime.

52. The difficulties which were made clear when this was debated at the hearing, in relation to defining the offences that could make up that *tertium genus*, confirm that that is not a task to be carried out by a court.

53. It should also be noted that, in describing 'activities capable of seriously destabilising the … structures of a country' and which, to that extent, jeopardise 'the essential functions of the State and the fundamental interests of society', the Court has referred to 'the fundamental constitutional, political, economic or social structures' of that country. (32)

54. On that basis, the Irish legislation described by the referring court does not differ significantly from the legislation examined in the proceedings giving rise to the judgment in *La Quadrature du Net*. Whatever the rules for access to data laid down in the 2011 Act (which are the subject of Question 3) are, the rules on data retention laid down in that Act are similar to those analysed in that judgment and therefore they also infringe Article 15(1) of Directive 2002/58.

55. The Irish legislation, for reasons which go further than those attached to the safeguarding of national security, allows the preventive, general and indiscriminate retention of the traffic and location data of all subscribers for a period of two years.

56. In summary, I suggest that Questions 1, 2 and 4 referred by the Supreme Court should be answered in the same terms as the ruling given by the Court in *La Quadrature du Net*.

C. Access to retained data (Question 3)

57. The referring court asks what criteria it should take into account in order to determine whether the national rules on access to retained data provide for the prior scrutiny required by the case-law of the Court, or whether an *ex post* judicial or independent scrutiny would suffice.

58. The judgment in *Prokuratuur* also responded to that question. In order to ensure compliance with the conditions to be satisfied by legislation governing access to retained data, (33) 'it is essential that access of the competent national authorities to retained data be subject to a *prior review* carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime'. (34)

59. The Court held that 'one of the requirements for that prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access'. (35)

60. If the prior review is entrusted to an independent authority, that authority 'must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence'. (36)

61. Specifically, 'the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review … means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field, … the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings'. (37)

62. According to the description of the Irish provisions provided by the referring court, access to retained data does not appear to be subject to prior review by a court or an independent authority and is instead at the discretion of a Garda officer of a certain rank, who decides whether or not to submit the request to the service providers.

63. It is for the referring court to examine whether the officer to whom the national legislation entrusts the prior review of access to retained traffic and location data has the status of an 'independent authority' and the nature of a 'third party', as required by the case-law of the Court of Justice.

64. In conducting that examination, the competent court must bear in mind that, in the judgment in *Prokuratuur*, it was held that a public prosecutor's office of a Member State does not have the attributes of independence or of a 'third party' where it also carries out investigative functions in criminal proceedings.

65. As regards the possibility of conducting the review mentioned by the referring court *ex post*, the judgment in *Prokuratuur* also provides the (negative) answer:

– ‘the lack of a review by an independent authority may [not] be made up for by a subsequent review carried out by a court as to whether a national authority’s access to traffic and location data was lawful’;

– ‘the independent review must take place before any access, except in the event of duly justified urgency, in which case the review must take place within a short time’. (38)

D. The possibility of limiting in time the effects of a declaration of incompatibility of the national provision with EU law (Questions 5 and 6)

66. Lastly, the Supreme Court asks whether:

– it is entitled to limit the temporal effect of a declaration of incompatibility of the national provision with Article 15 of Directive 2002/58, where failure to do so would result in ‘chaos and damage to the public interest’;

– it may, having been invited to disapply the national provision enacted to transpose the provisions of a directive, refuse to do so or limit its declaration to the period after the judgment of the Court of Justice of 8 April 2014, (39) which declared that Directive 2006/24 was invalid.

67. The answers to those questions are, once again, found in the judgment in *La Quadrature du Net*, which followed the traditional case-law in that respect.

68. In Case C 520/18, the Cour Constitutionnelle (Constitutional Court, Belgium) referred to the Court of Justice a question similar to that referred by the Irish Supreme Court in this reference for preliminary ruling. (40)

69. In responding to that question in the judgment in *La Quadrature du Net*, the Court, after recalling the requirements flowing from the principle of the primacy of EU law (paragraphs 214 and 215), reproduced its statement of the law regarding the limitation of the effects of its judgments: ‘Only the Court may, 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. Such a restriction on the temporal effects of the interpretation of that [EU] law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested’. (41)

70. Immediately afterwards, the Court stated that, ‘unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph. Maintaining the effects of national legislation such as that at issue in the main proceedings 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.’ (42)

71. On that basis, the Court concluded that ‘the referring court cannot apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of the national legislation at issue in the main proceedings’. (43)

72. Those considerations are fully applicable to Questions 5 and 6 referred by the Supreme Court.

73. First, it is immaterial that the national legislation at issue was enacted for the purpose of transposing Directive 2006/24 into national law. What matters in that regard is that the national provision complies in terms of its content with EU law as a whole, which is not the case here.

74. Where the Court has declared a directive to be invalid on the grounds that it is incompatible with substantive provisions of the Treaties, that incompatibility with primary EU law also applies to national

provisions which merely give effect to that directive.

75. The referring court states that the 2011 Act was enacted to comply with Article 288 TFEU, by transposing Directive 2006/24 into Irish law. Nobody disputes that this is the case but, as I have just observed, what is relevant here is that that directive was invalid from the outset (this was the finding in the *Digital Rights* judgment), since it amounted to disproportionate interference with the rights recognised by Articles 7 and 8 of the Charter, and that the retention of traffic and location data must be governed by Directive 2002/58, as interpreted by the Court of Justice.

76. Second, it is well known that preliminary rulings on interpretation given by the Court of Justice produce effects from the time when the provision of EU law interpreted came into force. (44)

77. While the temporal limitation of the effects of the interpretation of EU law given by the Court of Justice can be allowed only in the judgment ruling on the interpretation sought, it should be recalled that that did not occur in the *Digital Rights* judgment, which the referring court cites.

78. Nor did it occur in:

– the judgment in *Tele2 Sverige*, given on 21 December 2016, which interpreted Directive 2002/58, declaring that it precluded national legislation which, for the purpose of fighting serious crime, provides for general and indiscriminate retention of traffic and location data;

– the judgment in *La Quadrature du Net*, which, on 6 October 2020, again confirmed the interpretation of Directive 2002/58, in the manner described above.

79. Third, this reference does not address the difficulties linked to the exclusion of evidence in criminal proceedings brought against an individual who was convicted of murder. Rather, this case concerns *civil* proceedings (as the Supreme Court describes them) which have to be resolved by an objective comparison of national law with EU law.

80. This is emphasised by the national court: 'In the appeal currently before this Court [the Supreme Court], the only issue is whether the High Court was correct in determining that s. 6(1)(a) of the [2011 Act] is inconsistent with EU law'. (45)

81. The reply to the 'only issue' is that Section 6(1)(a) of the 2011 Act does not comply with EU law and that there are no reasons to delay the effects of the judgment which must make that finding.

V. Conclusion

82. In the light of the foregoing considerations, I suggest that the Court of Justice reply as follows to the Supreme Court (Ireland):

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, 11 and 52(1) of the Charter of Fundamental Rights of the European Union and Article 4(2) TEU, is to be interpreted as meaning that it precludes national legislation which:

– requires providers of publicly available electronic communications services to retain, on a preventive, general and indiscriminate basis, the traffic and location data of end users of those services for purposes other than the safeguarding of national security against a threat which is shown to be genuine and present or foreseeable;

– does not make access by the competent authorities to retained traffic and location data subject to a prior review carried out either by a court or by an independent administrative body.

2. A national court may not limit in time the effects of a declaration of illegality of domestic legislation which imposes on suppliers of electronic communications services, with a view to, inter alia, safeguarding national security and combating crime, an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights.

---

1 Original language: Spanish.

---

2 'Opinion in *SpaceNet* and *Telekom Deutschland*'.

---

3 (EU:C:2020:6).

---

4 'Opinion in *Ordre des barreaux francophones et germanophone*' (C 520/18, EU:C:2020:7).

---

5 Cases C 293/12 and C 594/12, EU:C:2014/238; 'the *Digital Rights* judgment'.

---

6 Directive of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

---

7 Cases C 203/15 and C 698/15, EU:C:2016:970; 'judgment in *Tele2 Sverige*'.

---

8 Directive 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).

---

9 Case C 207/16, (EU:C:2018:788).

---

10 C 623/17, EU:C:2020:790.

---

11 C 511/18, C 512/18 and C 520/18, EU:C:2020:791; 'judgment in *La Quadrature du Net*'.

---

12 Point 25 et seq. of this Opinion.

---

13 Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

---

14 See point 80 of this Opinion.

15 Point 25 et seq. of this Opinion.

16 Case C 746/18, EU:C:2021:152; 'judgment in *Prokuratuur*'. That judgment was discussed at the hearing.

17 Those were the words used by the Supreme Court in the letter received by the Registry on 27 October 2020, in reply to the Court of Justice's formal letter asking it to state whether it was continuing with the request for a preliminary ruling following the judgment in *La Quadrature du Net*.

18 In the absence of another explanation, those 'situations' must be taken to be those relating to the facts adjudicated on and the applicable national provisions.

19 The Bundesverwaltungsgericht (Federal Administrative Court, Germany) explained the differences between German national law and the national law examined in the judgment in *La Quadrature du Net* and asked the Court of Justice to give a ruling in the light of those differences.

20 Points 33 to 41 below reproduce the corresponding points of that Opinion.

21 Judgment in *La Quadrature du Net*, paragraph 109.

22 Ibid., paragraphs 111 to 133.

23 Ibid., paragraph 136.

24 Ibid., paragraph 137 (italics added). The Court goes on to state that that is the case 'even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection … with a threat to the national security of that Member State', in which case it must 'be considered that the existence of that threat is, in itself, capable of establishing that connection' (loc. ult. cit.).

25 CE:ECHR:2021:0525JUD005817013.

26 CE:ECHR:2021:0525JUD003525208.

27 CE:ECHR:2015:1204JUD004714306.

28 Judgment in *La Quadrature du Net*, paragraph 147: 'Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the *targeted retention* of traffic and location data for the purposes of combating serious crime, preventing serious threats to public security and equally of safeguarding national security, provided that such retention 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'. Italics added.

---

29 Opinion in *Ordre des barreaux francophones et germanophone* (C 520/18, EU:C:2020:7, point 101).

---

30 Judgment in *La Quadrature du Net*, paragraph 112 and the case-law cited.

---

31 Supported by many of the governments which entered an appearance.

---

32 Paragraph 135 of the judgment in *La Quadrature du Net*.

---

33 Legislation which 'must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities'. Judgment in *Prokuratuur*, paragraph 50.

---

34 Judgment in *Prokuratuur*, paragraph 51, italics added. That paragraph states that, in line with the judgment in *La Quadrature du Net*, paragraph 189, 'in cases of duly justified urgency, the review must take place within a short time'.

---

35 Ibid., paragraph 52.

---

36 Ibid., paragraph 53.

---

37 Ibid., paragraph 54.

---

38 Ibid., paragraph 58.

---

39 The *Digital Rights* judgment.

---

40 Paragraph 213 of the judgment in *La Quadrature du Net* summarises the wording of the third question referred for a preliminary ruling in Case C 520/18 as follows: 'the referring court seeks, in essence, to ascertain whether a national court may apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of national legislation imposing on providers of electronic communications services – *with a view to, inter alia, pursuing the objectives of safeguarding national security and combating crime* – an obligation requiring the general and indiscriminate retention of traffic and location data, owing to the fact that that legislation is incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.' Italics added.

---

41 Judgment in *La Quadrature du Net*, paragraph 216.

42 Ibid., paragraph 217.

43 Ibid., paragraph 220.

44 According to settled case-law, the interpretation which the Court gives to a rule of EU law, in the exercise of the jurisdiction conferred upon it by Article 267 TFEU, clarifies and defines the meaning and scope of that rule as it must be, or ought to have been, understood and applied from the time of its coming into force. It follows that the rule as thus interpreted may and must be applied by the courts to legal relationships arising and established before the judgment ruling on the request for interpretation, provided that in other respects the conditions for bringing before the courts having jurisdiction an action relating to the application of that rule are satisfied (judgments of 3 October 2019, *Schuch-Ghannadan*, C 274/18, EU:C:2019:828, paragraph 60, and of 16 September 2020, *Romenergo and Aris Capital*, C 339/19, EU:C:2020:709, paragraph 47).

45 Order for reference, paragraph 6 of Appendix II, *in fine*.