EUROPEAN COMMISSION

Brussels, 4 August 2020
sj.f(2020)4720213

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

WRITTEN OBSERVATIONS

submitted pursuant to Article 23 of the Statute of the Court of Justice

by **the European Commission**,

represented by Saulius KALEDA, Herke KRANENBORG, Martin WASMEIER and Folkert WILMAN, all Members of its Legal Service, acting as agents, with an address for service, Greffe contentieux, BERL 1/169, 1049 Brussels, and consenting to service by e-Curia,

in Case C-140/20

G.D.

concerning the request for a preliminary ruling, laid down in the order for reference of 25 March 2020 (hereinafter: 'order for reference'), by the Supreme Court of Ireland (hereinafter: 'referring court') submitted pursuant to Article 267 of the Treaty on the Functioning of the European Union (TFEU)

on the interpretation of 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) (OJ L 201, 31.7.2002, p. 37) (hereinafter: 'Directive 2002/58'), read in conjunction with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union (hereinafter: 'the Charter').

1. INTRODUCTION

1. This case raises several questions relating to the interpretation of Article 15(1) of Directive 2002/58, read in conjunction with Articles 7, 8 and 52(1) of the Charter. The questions were referred to the Court of Justice so as to allow the referring court to determine the compatibility with Union law of certain provisions of Irish law on the retention and access of personal data.

2. As such, this case is the latest in a rather long line of cases of this kind. Those cases arose out of the annulment by the Court of Justice of Directive 2006/24/EC[1] in Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland*)[2] and subsequent judgments on the legal situation after that annulment, namely Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige, Watson*) and Case C-207/16 (*Ministerio Fiscal*).[3] Several cases are currently pending before the Court of Justice, specifically Case C-623/17 (*Privacy International*), Joined Cases C-511/18 and C-512/18 (*La Quadrature du Net a.o.*), Case C-520/18 (*Ordre des barreaux francophones and germanophone a.o.*), Case C-746/18 (*H.K.*) and Joined Cases C-793/19 and C-794/19 (*SpaceNet* and *Telekom Deutschland*).

3. Given the similarity of many of the issues at stake in those pending cases and the present case, the Commission is of the view that the questions raised in the present case can only be answered in a definitive manner after the issuance of the judgments in these pending cases, in particular in Joined Cases C-511/18 and C-512/18, and Case C-520/18.[4] Nonetheless, in the following, the Commission will set out its views on the questions now referred. It does so with reference to its observations in the pending cases.

---

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54) (Hereinafter: 'Directive 2006/24').

2 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, EU:C:2014:238.

3 CJEU Joined Cases C-203/15 and C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970 and CJEU Case C-207/16, *Ministerio Fiscal*, EU:C:2018:788.

4 The procedure in Joined Cases C-793/19 and C-794/19 was suspended awaiting the ruling in Joined Cases C-511/18 and C-512/18, and Case C-520/18.

4. Before setting out its views on the questions referred, the Commission will first give a brief overview of the applicable legal framework, the relevant facts and proceedings at national level, as well as the content of those questions.

2. LEGAL FRAMEWORK

2.1. Charter

5. Article 7 of the Charter reads as follows:

"*Article 7*

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications."

6. Article 8 of the Charter reads as follows:

"*Article 8*

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

7. Article 52(1) of the Charter reads as follows:

"*Article 52*

Scope and interpretation of rights and principles

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only

if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

2.2. Directive 2002/58

8. Article 15(1) of Directive 2002/58 reads as follows:

"*Article 15*

Application of certain provisions of Directive 95/46/EC

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."

2.3. National law

9. The national law principally at issue in the national proceedings is the Communications (Retention of Data) Act 2011 (hereinafter: 'the 2011 Act'). The 2011 Act was initially enacted in order to transpose into national law the provisions of Directive 2006/24, but has been retained after the annulment of that Directive by the Court of Justice in the aforementioned *Digital Rights Ireland* judgment.[5]

10. The Commission refers to the order for reference for a detailed overview of the provisions of the 2011 Act.[6] Its main elements are as follows.

11. The 2011 Act requires providers of telecommunication services to retain "fixed network telephony and mobile telephony data". This term refers to data identifying

---

5 CJEU Joined Cases C-293/12 and C-294/12.

6 See in particular section 3 of the order for reference, as well as its Appendix I.

the source; destination; data and time of the start and end of the communication; type of communication; and the type and geographic location of the communications equipment used (hereinafter jointly: 'traffic and location data'). The term and, consequently, the data retention obligations set out in the 2011 Act do not cover the content of the communications.

12. Under the 2011 Act, the traffic and location data are to be retained for a period of two years.

13. The 2011 Act allows the traffic and location data to be accessed only by a member of the Irish police force not below the rank of chief superintendent. At the relevant time, as a matter of internal policy, disclosure requests were decided on by a single chief superintendent (namely, the head of the security and intelligence section of the Irish police force). The latter was supported by the Telecommunications Liaison Unit (TLU), which operated with a certain degree of independence. The chief superintendent and the TLU were charged with verifying the legality, proportionality and necessity of requests for access to the data. Under a memorandum of understanding of 2011, service providers would not process request for access to the data that did not come through this process.

14. The TLU is subject to audit by the Irish Data Protection Commissioner, which has been designated as the supervisory authority for the purposes of the 2011 Act.

15. According to the 2011 Act, the traffic and location data could be accessed where needed (inter alia) for the prevention, detection, investigation or prosecution of "serious offences". The latter term is defined as offences punishable by imprisonment for a term of five years or more, as well as certain other offences listed in the 2011 Act.

16. The 2011 Act requires the Irish police to report annually to the competent Irish ministry on all disclosure requests made. It also provides for a complaints procedure and it charges a designated judge with reviewing the operation of the 2011 Act's provisions.

3. FACTS AND NATIONAL PROCEEDINGS

17. As regards the proceedings at national level, two proceedings should be distinguished.

18. First, there is the criminal trial against a man, referred to in the order for reference as 'Mr. D.'. Mr. D. was accused of the murder of a woman (referred to as 'Ms. O'H.'). The latter disappeared in August 2012; her remains were discovered in September 2013. Investigations in that time period led to the identification of Mr. D as a suspect. Although the prosecution also relied on other evidence, the analysis of certain telecommunication data relating to Mr. D. (specifically, it appears, location data), retained and accessed in accordance with the 2011 Act, was a significant feature of the case against him.[7]

19. In the context of the criminal proceedings referred to in the previous paragraph, Mr. D. – who at all times denied guilt – unsuccessfully contested the admissibility of the aforementioned data as evidence in the case against him. In March 2015, Mr. D. was convicted and received a life sentence. His conviction is the subject of an appeal by Mr. D., which is pending before the Irish Court of Appeal.

20. Second, in a separate and parallel procedure, Mr. D. initiated civil proceedings against the relevant Irish authorities, in the course of which the present request for a preliminary reference has arisen. In these civil proceedings, Mr. D. seeks a declaration of invalidity of the 2011 Act for being incompatible with Union law, specifically Article 15(1) of Directive 2002/58. Mr. D. does so with a view to contending at the appeal against his conviction in the criminal case, referred to above, that the evidence of the telecommunication data relating to him is inadmissible.

21. In the civil proceedings, the Irish authorities contest that the 2011 Act is invalid for being incompatible with Union law.

22. It appears from the order for reference that the dispute between the parties to the civil proceedings specifically relates to three points: (a) whether it follows from the *Tele2 Sverige* case law of the Court of Justice that rules of national law providing for "universal" retention of personal data are *per se* contrary to Union law; (b) if not, whether the safeguards set out in the 2011 Act are sufficient, in particular as regards independent protection against undue access to the retained data; and (c) if not, whether the legal effects of the 2011 Act could be retained in the case at hand.

---

7 See in particular para. 3 of Appendix II to the order for reference.

4. QUESTIONS REFERRED

23. Against this background, the referring court raised the following questions to the Court of Justice for a preliminary ruling under Article 267 TFEU:

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

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

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

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

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

6 May a national court invited to declare the inconsistency of national legislation with Article 15 of the Directive 2002/58/EC, and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted

pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of the Directive 2006/24/EC issued by the CJEU on the 8th day of April, 2014?"

5. QUESTIONS 1, 2 AND 4

5.1. Preliminary remarks

24. By means of a first preliminary remark, the Commissions notes the close relationship between the issues raised in questions 1, 2 and 4. It therefore suggests assessing those three questions together.

25. In the second place, the Commission recalls that, in a situation such as the one at issue in the main proceedings, Article 15(1) is not the only relevant provision of Directive 2002/58. Article 15(1) permits, subject to certain conditions, Member States to restrict the scope of rights and obligations set out in certain other provisions of that Directive. That means that Article 15(1) is only relevant if there is such a restriction.

26. In the case at hand, it appears that the other relevant provisions of Directive 2002/58 are, in particular, Articles 5 on the confidentiality of communications, Article 6 on the processing and storage of traffic data, as well as Article 9 on location data other than traffic data.[8] The referring court seems to assume that the 2011 Act restricts the scope of rights and obligations set out in those provisions. That being so, and considering that the order for reference contains no specific information and questions in this regard, the Commission makes a similar assumption. It therefore concentrates on the interpretation of Article 15(1).

27. Finally, whilst the questions referred mention the Charter in general, it is clear from other parts of the order for reference that the referring court is of the view that the relevant provisions of Directive 2002/58 should be read in conjunction with, more specifically, Article 7, 8 and 52(1) of the Charter.[9]

28. The Commission agrees with that view.[10] After all, the rights and freedoms enshrined in the Charter are the main point of reference for the purposes of

---

8 Cf. CJEU Joined Cases C-203/15 and C-698/15, para. 84-87.

9 See in particular point 2.3 of the order for reference.

10 Although other articles can be relevant too, such as Article 11 on the freedom of expression. Cf. CJEU Joined Cases C-203/15 and C-698/15, para. 92-93.

applying the condition set out in the last sentence of Article 15(1) of Directive 2002/58.[11] Moreover, the national law at issue evidently restricts the exercise of the fundamental rights to respect for private life and to protection of personal data.[12]

5.2. Substance

29. With questions 1, 2 and 4, the referring court essentially inquires whether Article 15(1) of Directive 2002/58, read in conjunction with the Charter, should be interpreted in such a manner that a national law providing for a universal data retention regime, such as the 2011 Act, is *per se* incompatible with Union law.

30. More specifically, the referring court inquires whether the conclusion of incompatibility should be drawn even if: (a) the national law in question involves restrictions on retention and access, which the referring court considers stringent; (b) the data concerned may anyway be retained lawfully by the service providers for their own commercial purposes; (c) the data concerned may be retained for reasons of national security, which according to the referring court are reasons falling outside the scope of Directive 2002/58; and (d) the national court seized considers that the retention of the data concerned is both essential and strictly necessary for achieving the objective of combating serious crime.

31. The Commission notes that the questions are based on the view of the referring court that the 2011 Act qualifies as a "*general/universal*" regime on the retention of certain types of personal data.[13] It is evident from the order for reference that, by using this term, the referring court intends to refer to rules of national law providing for "*general and indiscriminate retention*" of personal data within the meaning of the *Tele2 Sverige* case law.[14]

32. Having regard to the description of the 2011 Act in the order for reference, as briefly outlined above, the Commission sees no reason to question that qualification by the referring court.

33. In paragraphs 104 to 107 of the *Tele2 Sverige* ruling, the Court made clear that national legislation which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as traffic data,

---

11 CJEU Joined Cases C-203/15 and C-698/15, para. 91.

12 Cf. CJEU Joined Cases C-203/15 and C-698/15, para. 93-94.

13 In addition to the preliminary questions at issue here, see also para. 6.3 of the order for reference.

14 CJEU Joined Cases C-203/15 and C-698/15, para. 97.

and which provides for no differentiation, limitation or exception according to the objective pursued exceeds the limits of what is strictly necessary and cannot be justified within a democratic society. It therefore follows from the *Tele2 Sverige* ruling that a general and indiscriminate retention scheme, such as the retention scheme in place in the case at issue, for the purpose of fighting serious crime, is *per se* incompatible with Union law.[15]

34. Whether the four elements put forward by the referring court could have any bearing on this position of the Court of Justice, will be discussed in turn below.

a) Relevance of "stringent restrictions on retention and access" (question 1)

35. The Irish Court refers to the possible relevance of restrictions in Irish law on both retention and access, which it considers to be stringent. However, from the order for reference it follows that this should rather be understood as referring to restrictions to *access* only. The question emerged from a debate between the applicant in the national case and the Irish State on whether the conditions for *access* to the retained data should be taken into account when assessing the permissibility of the retention measure.[16]

36. The same issue was also discussed during the written and oral proceedings in the *Tele2* Sverige case before the Court of Justice. Since the position of the Court on this matter did not follow clearly from the preceding ruling in *Digital Rights Ireland*, the issue was considered as not yet decided. The discussion on this point in the *Tele2 Sverige* proceedings is described and commented upon in paragraphs 189 to 215 of the Opinion in that case of Advocate-General Saugmandsgaard Øe.[17]

37. The Advocate-General's reading of *Digital Rights Ireland* was that the Court held that a general data retention obligation wend beyond the bounds of what was strictly necessary where it was not accompanied by stringent safeguards concerning access to the data, the period of retention and the protection and security of the

---

15 In its observations in the pending cases the Commission developed the view that a general and indiscriminate data retention scheme might be justified for certain *particularly* serious crimes (section 3.2.5 of the observations of the European Commission in Joined Cases C-511/18 and C-512/18, and section 3.2.4 of the observations in Case C-520/18). See also para. 56 et seq. of the present observations.

16 See point 6.2 of the order for reference.

17 See Opinion AG Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15, EC:EU:2016:572, para. 189-215.

data. The Advocate General suggested the Court to conclude that a general data retention obligation did not, in itself, necessarily go beyond the bounds of what was strictly necessary for the purposes of fighting serious crime, provided it was accompanied by safeguards concerning access to the data, the retention period and the protection and security of the data.[18]

38. The Court of Justice did not take over the reasoning of the Advocate-General. On the contrary, it dealt with the issues of retention and data protection separately. When answering the second question of the Swedish referring Court – whether a general retention scheme that was found incompatible with Union law, could 'nevertheless' be permitted if there were strict rules on access in place – the Court considered that the rules on access should be assessed 'irrespective' of the obligation to retain the data.[19]

39. It follows from the ruling in *Tele2 Sverige*, having in mind also the discussions during the proceedings, that restrictions on access by competent authorities to the retained data did not prevent the Court from concluding that a general and indiscriminate retention scheme, for the purpose of fighting serious crime, is in itself incompatible with Union law.

b) Relevance of "the fact that data may be retained lawfully by the service providers for their own commercial purposes" (question 2)

40. The referring court asks whether a national court, when considering the inconsistency of a national data retention measure with Union law, is entitled to have regard to the fact that the same data may also be lawfully retained by service providers for their own commercial purposes.

41. In the Commission's view the fact that Directive 2002/58 allows providers, subject to further restrictions, to retain certain telecommunications data for specifically indicated commercial purposes, is not relevant for the assessment of the compatibility with Union law of a national data retention scheme for the fight against serious crimes.

42. The lawfulness of retention of data should always be assessed in relation to the specific objective pursued. This follows from Article 52(1) of the Charter and the

---

18 *Ibid*., para. 205.

19 CJEU Joined Cases C-203/15 and C-698/15, resp. para. 51 and 113.

principles of purpose limitation, data minimisation and storage limitation as laid down in Article 5(1)(b), (c) and (e) of Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR).[20]

43. That the lawfulness of retention by providers for their own commercial purposes must be assessed independently from the lawfulness of a retention requirement for law enforcement purposes, and vice versa, also follows from the structure of Directive 2002/58.

44. The lawfulness of retention for commercial objectives has to be considered in the light of Articles 5, 6 and 9 of Directive 2002/58/EC. These provisions regulate the conduct of the providers, and in fact allow, subject to further conditions, general and indiscriminate storage of certain telecommunication data relating to their costumers for certain specified purposes, such as billing purposes.

45. The retention of telecommunications data for the objective of prevention, investigation, detection and prosecution of criminal offences, on the other hand, is only possible as a derogation from the substantive provisions of Directive 2002/58 on the basis of Article 15 of Directive 2002/58. This provision allows Member States, by law and subject to further conditions, to restrict the scope of certain provisions of Directive 2002/58. In that respect, the Court of Justice considered in *Tele2 Sverige*, that the system put in place by Directive 2002/58 requires the retention of data for the objectives listed in Article 15(1) to be the exception, and not the rule.[21] This consideration was at the basis of the Court's conclusion that a general and indiscriminate retention scheme, for the purpose of fighting serious crimes, exceeded the limits of what is strictly necessary.

46. It should be noted that the Court has made clear that access of public authorities to personal data that is retained by providers – either for their own commercial reasons or on the basis of a law requiring the retention for the fight against serious crime – constitutes an interference with the fundamental rights to respect for private life and protection of personal data which in itself – so separately from the

---

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 199, 4.5.2016, p. 1). The provisions of Directive 2002/58/EC particularise and complement the GDPR with respect to the processing of personal data in the electronic communication sector, see Art. 1(1) and (2) of Directive 2002/58/EC.

[21] *Ibid*., para. 89 and 104.

retention – must be justified and proportionate in relation to the objective pursued, in line with Article 15(1) of Directive 2002/58.[22]

c) Relevance of "the fact that [data] may be required to be retained for reasons of national security excluded from the provisions of Directive 2002/58/EC" (question 3)

47. This third element brought forward by the referring court triggers two further issues which are subject to extensive debate in several of the cases currently pending in Court, namely (1) whether a retention scheme for the objective of safeguarding national security falls within the scope of Directive 2002/58 and, if so, (2) whether a general and indiscriminate retention scheme would be justified if the objective is safeguarding national security rather than the prevention, investigation, detection and prosecution of serious criminal offences.

48. For providing a meaningful answer to the referring court, the Commission does not consider it necessary to discuss again these two issues. For a further explanation of the Commission's position that a retention obligation on providers for national security purposes falls within the scope of Directive 2002/58, and that a general and indiscriminate retention scheme could, subject to certain further conditions, be justified for such purposes, the Commission respectfully refers to Court to its observations in Case C-623/17, Joined Case C-511/18 and C-512/18, and in Case C-520/18.[23]

49. The Commission is of the view that the fact that general and indiscriminate retention of personal data might be justified for reasons of national security is, as such, not relevant for the assessment of the compatibility with Union law of a national data retention scheme for the fight against serious crimes.

50. It is true that there can be a certain overlap between objectives pursued in the interest of national security and 'ordinary' law enforcement objectives. In particular, the prevention of acts of terrorism might relate to both prevention of criminal offences and prevention of threats to national security. However, the national law at

---

22 CJEU Case C-207/16, *Ministerio Fiscal*, para. 51-57.

23 See section 3.1 of the observations of the European Commission in Case C-623/17, section 3.2.4 of the observations in Joined Cases C-511/18 and C-512/18, and section 3.2.3 of the observations in Case C-520/18.

issue applies to the fight against serious crime in general and there appears to be no particular relation to the objective of national security.

51. The Commission again underlines that the lawfulness of retention of data should be assessed in relation to the specific objective pursued. This follows from Article 52(1) of the Charter and the principles of purpose limitation, data minimisation and storage limitation as laid down in Article 5(1)(b), (c) and (e) of the GDPR.[24] It is not because data might be lawfully required to be retained for one purpose, it is also justified to retain that data for other purposes.

52. It should thereby be concluded that if data is retained (only) on the basis of a law for a specific purpose in the public interest as listed in Article 15(1), access by competent national authorities to the retained data should also be limited to that purpose.

d) Relevance of the national court's conclusion that the general retention is "both essential and strictly necessary to the achievement of the objective of combating serious crime" (question 4)

53. With this fourth element, the referring court seems to directly challenge the finding of the Court of Justice in the *Tele2 Sverige* that a general and indiscriminate retention scheme for the purpose of fighting serious crime is not in compliance with Union law. It considers that alternative, targeted forms of retention, as suggested by the Court of Justice in *Tele2 Sverige*[25], are ineffective and unworkable.[26]

54. In *Tele2 Sverige*, the Court of Justice has indeed interpreted Article 15(1) of Directive 2002/58, read in the light of the Charter, as precluding any national legislation which, for the purpose of fighting serious crime, provides for a general and indiscriminate data retention scheme.

---

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 199, 4.5.2016, p. 1). The provisions of Directive 2002/58/EC particularise and complement the GDPR with respect to the processing of personal data in the electronic communication sector, see Art. 1(1) and (2) of Directive 2002/58/EC.

[25] CJEU Joined Case C-203/15 and C-698/15, para. 106 and 108-111.

[26] See point 8.5 with reference to points 7.2-7.6 of the order for reference.

55. The 2011 Act as a whole would not pass the proportionality test, as it extends the scheme to any "serious offence" punishable by imprisonment for a term of five years or more, as well as certain other offences listed. Therefore, to the questions as asked by the referring court in the abstract, the Commission can only reply that a general and indiscriminate retention scheme, for the purpose of fighting serious crime, is *per se* incompatible with Union law. In this respect, there is no room for a national court to substitute the Court's finding by its own assessment.

56. That being said, in the pending cases, the Commission has proposed that a general and indiscriminate retention scheme could be considered necessary and proportionate with regard to the fight against the most serious forms of crime affecting the essential interests of the society, and where it is the only effective instrument to achieve this objective.[27] Those forms of crime can be referred to as "particularly serious crime".

57. If the Court of Justice, in these pending cases, were to accept that national law could foresee data retention for the fight against certain types of particularly serious crime, then another question, of a procedural nature, might arise, namely whether the referring court might, under national procedural law, have any margin to deny declaratory relief as sought by a particular applicant, considering the particular case and the circumstance that this applicant was convicted for a crime which could be viewed as a particularly serious one.

58. Provided all other conditions set out by the Court in its case law are met, in particular in relation to access to the retained data (see section 6 below), the national court could possibly have a margin to consider that the relevant national law would not be incompatible with Union law in as far as it sets up such a scheme with regard to particularly serious crime. It could then come to the conclusion that the retention scheme could only not be applied for the fight against crimes that are *not* considered particularly serious.

59. Alternatively, again provided that the other conditions set out by the Court are met, the national court might have some discretion to deny declaratory relief in certain cases[28]. If so, it might be open to decide not to grant declaratory relief in the

---

[27] In that regard, the Commission refers, in particular, to its observations in Case C-520/18, para. 64-70 (see esp. para. 67).

[28] See the description of declaratory relief in Irish law of civil procedure in pending case C-64/20.

particular case of an applicant, given the particular circumstances. Ultimately, these are however procedural questions for the referring court to consider.

60. To conclude on questions 1, 2 and 4, it follows from the foregoing that the four elements put forward by the referring court do not alter the conclusion that a general and indiscriminate retention scheme, for the purpose of fighting serious crime, not being limited to certain forms of particularly serious crime, is *per se* incompatible with Union law.

61. Therefore, the Commission respectfully suggests to the Court to provide the following answer to questions 1, 2 and 4, taken together:

> "Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights must be interpreted as precluding national legislation which, for the purpose of fighting serious crime as such and without it being limited to the fight against certain types of particularly serious crime, provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."

6. QUESTION 3

62. The Court of Justice considered in *Tele2 Sverige* that as a general rule, except in cases of validly established urgency, access of the competent authorities to retained data should be subject to prior review carried out by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities.[29]

63. In the case at issue, access to the retained data by the Irish law enforcement authorities is not subject to prior control by a court. The referring court therefore explores whether the internal system set up by the Garda Commissioner, which includes the involvement of a single chief superintendent and a small "independent unit" known as the Telecommunications Liaison Unit (TLU)[30], could qualify as prior review by an independent administrative authority in the meaning of the *Tele2 Sverige* ruling.

---

29 CJEU Joined Case C-203/15 and C-698/15, para. 120.

30 See points 3.4-3.5 of the order for reference.

64. In particular, the referring court wants to know what criteria should be applied in considering the independence of an authority responsible for the prior review of requests for access to retained data and whether the existence of *ex post* judicial or independent scrutiny has any relevance in that respect.

65. The question against what criteria the independence of an authority should be measured, was also raised in the still pending Case C-746/18. For a full description of its position, the Commission respectfully refers the Court to the observations of the Commission in that case.[31]

66. In short, the Commission underlined that the independent administrative authority must be able to decide on access in an objective and impartial manner. The Commission suggested the Court to consider the following two elements to be taken into account for assessing the independence of the administrative authority:

    a. whether the authority is protected against any direct or indirect external influence, in particular political;

    b. whether the authority is independent from the authority that requests access to the retained data in order to ensure a correct balance between, on the one hand, the rights to private life and the protection of personal data and, on the other hand, the legitimate law enforcement interest sought by the requesting authority.

67. The information provided by the referring court allows the Commission to conclude that in particular the second of the above criteria is not met in the present case.

68. The internal control mechanism, which includes the detective chief superintendent and the TLU, does not ensure an objective and impartial review of requests for access to retrained data. The TLU and the detective chief superintendent are required to verify the legality, proportionality and necessity of disclosure request sought by members of the Garda Commissioner. However, the detective chief superintendent, who is the head of the security and intelligence section of the Garda Commissioner, ultimately decides whether to issue a request for disclosure to the service providers. The TLU provides support to the functions of the detective chief superintendent and acts as the single contact point for service providers.

---

[31] See section 3.3 of the observations in Case C-746/18.

69. In those circumstances, it cannot be concluded that access of the competent authorities to retained data is subject to prior review carried out by an independent administrative body.

70. The fact that other *ex post* independent judicial and administrative control mechanisms are in place, does not lift the mandatory prior review by a court or independent administrative body.[32] This follows from the *Tele2 Sverige* ruling itself, in which the Court, *in addition* to the requirement of prior authorisation, insisted on supervision by an independent authority and notification of the data subject, in order to enable persons affected to exercise their right to a legal remedy.[33]

71. The essence of prior review is that it aims to *prevent* unlawful disclosures of retained data. *Ex post* review and remedies cannot compensate the preventive safeguard that is ensured by prior review. The only exception to prior review, the Court considered, was in cases of validly established urgencies.

72. On the basis of the foregoing, the Commission respectfully suggests the Court to provide the following answer to question 3:

> "Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights, must be interpreted as requiring, except in cases of validly established urgency, that access of the competent authorities to retained traffic and location data be subject to prior review carried out by a court, or by an independent administrative body which should be free from any direct or indirect external influence, and should be independent and impartial in relation to the authority that formulated the request for access to the retained data."

7. QUESTIONS 5 AND 6

73. Questions 5 and 6, which the Commission suggests addressing together, are based on the premise that a national law such as the 2011 Act is incompatible with Union law, in particular Article 15(1) of Directive 2002/58. The questions focus on whether there is any scope for the national court seized to limit the temporal effect of any declaration to that effect (or otherwise refuse the relief sought on that basis),

---

[32] The requirement of prior review was repeated in CJEU Opinion 1/15, *EU-Canada PNR Agreement*, EU:C:2016:656, para. 202.

[33] See CJEU Joined Case C-203/15 and C-698/15, para. 121 and 123.

in particular in a situation where (a) the national court is of the view that such limitation is needed to avoid chaos and damage to the public interest and (b) the national law in question had been enacted, in accordance with Article 288 TFEU, to faithfully transpose into national law the provisions of Directive 2006/24, which has subsequently been annulled by the Court of Justice, whilst the application of that national law in the case at hand took place prior to that annulment.

74. Under the principle of sincere cooperation laid down in Article 4(3) TEU, Member States are required to nullify the unlawful consequences of an infringement of Union law. Competent national authorities have to take all necessary measures, within their sphere of competence, to remedy the situation.[34] This obligation is also incumbent on national courts before which an action against a national measure has been brought. The detailed procedural rules applicable to such actions are a matter for the domestic legal order of each Member State, under the principle of procedural autonomy of the Member States, provided that they comply with the principle of equivalence and the principle of effectiveness.[35]

75. According to settled case law, only the Court of Justice may, in exceptional cases, for overriding considerations of legal certainty, allow temporary suspension of the ousting effect of a rule of Union law with respect to national law that is contrary thereto. If national courts had the power to give provisions of national law primacy in relation to Union law contravened by those provisions, even temporarily, the uniform application of Union law would be undermined.[36]

76. The Court of Justice has exceptionally authorised a national court, subject to specific conditions, to make use of a national provision empowering it to maintain certain effects of a national measure which was found contrary to Union law, given the existence of an overriding consideration relating to the environment and because there was a risk that the annulment of that measure could create a legal vacuum that was incompatible with the Member State's obligation to adopt measures to transpose another act of Union law concerning the protection of the environment.[37] The Court of Justice also authorised a national court to temporarily

---

34 CJEU, Case C-411/17, *Inter-Environnement Wallonie ASBL*, EU:C:2019 :622, para. 170.

35 *Ibid*., para. 171.

36 CJEU Case C-409/06, *Winner Wetten*, EU:C:2010:503, para. 66-67 and CJEU Case C-379/15, *Association France Nature Environnement*, EU:C:2016:603, para. 33.

37 CJEU Case C-41/11, *Inter-Environnement Wallonie ASBL and Terre wallonne ASBL v Région wallonne*, EU:C:2012:103, para. 58.

maintain the effect of a national provision if otherwise there would be a genuine and serious threat of disruption to the electricity supply of the Member State at issue.[38]

77. The Commission observes that this case law, at least partly, takes into account the fact that national measures adopted in breach of *procedural* requirements of EU law are not necessarily contrary in substance to EU law, and therefore, in some situations, the possibility of their regularisation could be allowed by the Court as a matter of exception.[39] Such reasoning could not be extended to the national legislation which contravenes the substantive provisions of Directive 2002/58, the latter giving expression to the fundamental rights enshrined in the Charter.

78. Moreover, as the Commission already stipulated in its observations in the pending Case C-520/18, with reference to *Nelson a.o.*[40], the interpretation the Court of Justice gives to a rule of Union law 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 entry into force.[41] Restricting the temporal effects of such an interpretation may be allowed only in the actual judgment ruling upon the interpretation requested. According to the Court in *Nelson a.o.* that principle guarantees the equal treatment of the Member States and of other persons subject to Union law. Equally, a declaration of invalidity of an Union act by the Court of Justice applies retroactively (*ex tunc*) and also the temporal effects of such a declaration can only be restricted in the ruling itself.

79. The national law at issue in the present case constituted a transposition of Directive 2006/24 and, after the invalidation of that Directive by the Court of Justice in *Digital Rights Ireland*, was subsequently based on Article 15(1) of Directive 2002/58, a provision which, in relation to national measures on data retention, was clarified by the Court of Justice in the *Tele2 Sverige* ruling. Neither in *Digital Rights Ireland*, nor in *Tele2 Sverige*, did the Court of Justice put any restrictions on the temporal effects of its rulings.

---

38 CJEU Case C-411/17, para. 179 and CJEU Case C-24/19, *A and others*, EU:C:2020:503, para. 92-95.

39 CJEU Opinion of Advocate General Kokott, C-411/17, *Inter-Environnement Wallonie ASBL*, EU:C:2018:972, point 209; Opinion of Advocate General Campos Sánchez-Bordona, C-24/19, *A and others*, EU:C:2020:503, point 129.

40 CJEU Case C-581/10 and C-629/10, *Nelson a.o.*, EU:C:2012:657, para. 87-94.

41 See pt. 100 of the observations of the European Commission in Case C-520/18, *Ordre des barreaux francophones and germanophone a.o.*

80. Against this background, the Commission does not see why in the present case, it would be justified to allow a limitation of the temporal effects of the future ruling of the referring court, while it concerns the same subject matter and the same provisions of Union law as in the *Tele2 Sverige* ruling. According to the Commission, questions 5 and 6 must therefore be answered in the negative.

81. As a last remark, in relation to the point indicated by the referring court that the absence of a limitation in time would result in 'chaos and damage to the public interest', the Commission wishes to point at the standing case law of the Court of Justice that Union law does not require a national court to disapply domestic rules of procedure conferring finality on a decision, even if to do so would enable it to remedy an infringement of Union law by the decision at issue.[42]

82. On the basis of the foregoing, the Commission respectfully suggests the Court to provide the following answer to questions 5 and 6, taken jointly:

> "A national court is not permitted to limit the temporal effect of a declaration of inconsistency of national legislation which governs the retention of, and access to, telecommunications metadata by national authorities in the course of the detection, investigation and prosecution of serious crime with Article 15 of Directive 2002/58/EC, as interpreted by the Court of Justice."

8. CONCLUSION

83. In view of the foregoing, the Commission has the honour to suggest answering the preliminary questions referred in the present case as follows:

> 1. Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights must be interpreted as precluding national legislation which, for the purpose of fighting serious crime as such and without it being limited to the fight against certain types of particularly serious crime, provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.
>
> 2. Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights, must be interpreted as requiring, except in cases of validly established urgency, that access of the competent

[42] CJEU Case C-234/04, *Rosemarie Kapferer*, EU:C:2006 :178, para. 21.

authorities to retained traffic and location data be subject to prior review carried out by a court, or by an independent administrative body which should be free from any direct or indirect external influence, and should be independent and impartial in relation to the authority that formulated the request for access to the retained data.

3. A national court is not permitted to limit the temporal effect of a declaration of inconsistency of national legislation which governs the retention of, and access to, telecommunications metadata by national authorities in the course of the detection, investigation and prosecution of serious crime with Article 15 of Directive 2002/58/EC, as interpreted by the Court of Justice.

Saulius KALEDA Herke KRANENBORG Martin WASMEIER Folkert WILMAN

Agents of the Commission