Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 18 November 2021 [1]

Joined Cases C-793/19 and C-794/19

Bundesrepublik Deutschland
v
SpaceNet AG (C-793/19)
Telekom Deutschland GmbH (C-794/19)

(Requests for a preliminary ruling from the Bundesverwaltungsgericht (Federal Administrative Court, Germany))

(Reference for a preliminary ruling – Telecommunications – Processing of personal data and protection of privacy in the electronic communications sector – Directive 2002/58/EC – Article 15(1) – Article 4(2) TEU – Charter of Fundamental Rights of the European Union – Articles 6, 7, 8, and 11 and Article 52(1) – General and indiscriminate retention of connection data for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security)

1. These requests for a preliminary ruling, together with that in Case C-140/20, [2] highlight once again the concern raised in some Member States by the case-law of the Court on the retention of, and access to, personal data generated in the electronic communications sector.

2. In my 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 identified the following points as the most important milestones in that case-law to date:

— The judgment of 8 April 2014, *Digital Rights Ireland and Others*, [5] which declared Directive 2006/24/EC [6] to be invalid in so far as it entailed a disproportionate interference with the rights recognised in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

1 Original language: Spanish.

2 Case C-140/20, *Commissioner of the Garda Síochána and Others*, on which I also deliver my Opinion today.

3 'My Opinion in *La Quadrature du Net*' (EU:C:2020:6).

4 'My Opinion in *Ordre des barreaux francophones et germanophone*' (EU:C:2020:7).

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

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).

— The judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*,[7] which declared that Article 15(1) of Directive 2002/58/EC[8] precludes national legislation which, for the purpose of fighting serious crime, provides for general and indiscriminate retention of 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, noting the importance of the principle of proportionality in this regard.

3. In 2018, the courts of certain Member States made requests for preliminary rulings from the Court in which they questioned whether those judgments (of 2014, 2016 and 2018) could deprive national authorities of a necessary instrument in safeguarding national security and combating crime and terrorism.

4. Four of those requests for a preliminary ruling gave rise to the judgments in *Privacy International*[10] and *La Quadrature du Net and Others*,[11] both of 6 October 2020, which essentially endorsed the case-law of the judgment in *Tele2 Sverige*, while introducing some additional elements.

5. In view of the source of those judgments (the Grand Chamber of the Court of Justice), their content, and the pains taken to explain in detail, in discussion with the referring courts, the grounds which, in spite of everything, justify the position taken, those two 'synoptic' judgments of 6 October 2020 might have been expected to put an end to the debate. Any further request for a preliminary ruling on the same subject would therefore qualify for a reply by reasoned order as provided for in Article 99 of the Rules of Procedure of the Court of Justice.

6. However, before 6 October 2020, three further requests for preliminary rulings had been lodged with the Court (the two requests in the joined cases in these proceedings and the request in Case C-140/20) which once again questioned the case-law laid down in respect of Article 15(1) of Directive 2002/58.

7. The Court informed the referring courts of the judgments of 6 October 2020, in case they wished to withdraw their requests for a preliminary ruling. Since, as I shall explain below,[12] they persisted with the requests, it has been decided not to apply Article 99 of the Rules of Procedure and that the Grand Chamber of the Court of Justice should reply to them.

7 C-203/15 and C-698/15, EU:C:2016:970; 'the 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 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; 'the judgment in *La Quadrature du Net*'.

12 Point 30 of this Opinion.

I. Legislative framework

A. European Union law. Directive 2002/58

8. Paragraph 1 of Article 5 ('Confidentiality of the communications') provides as follows:

'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') stipulates that:

'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 thereof, that:

'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.'

[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).

B. National law

1. Telekommunikationsgesetz (Law on Telecommunications; 'the TKG')

11. Paragraph 113a(1) provides that:

'The obligations in respect of the retention, use and security of the traffic data defined in Paragraphs 113b to 113g apply to operators which provide publicly available telecommunications services to end users.'

12. Paragraph 113b provides that:

'(1) Operators to which Paragraph 113a applies shall retain data in national territory as follows:

1. for 10 weeks in the case of the data referred to in subparagraphs 2 and 3;

2. for four weeks in the case of the location data referred to in subparagraph 4.

(2) Providers of publicly available telecommunications services shall retain:

1. the telephone number or other identifier of the calling and called parties and of any other line used in the event of call switching or forwarding;

2. the date and time of the start and end of the communication, stating the time zone;

3. where different services can be used in the context of the telephone service, information on the service used;

4. and also, in the case of mobile telephony services,

   (a) the international mobile subscriber identity of the calling and called parties;

   (b) the international identifier of the calling and called terminals;

   (c) in the case of pre-paid services, the date and time of the initial activation of the service, stating the time zone;

5. and, in the case of internet telephony services, the IP (internet protocol) addresses of the calling and called parties and the allocated identification numbers.

Subparagraph 1 above shall apply *mutatis mutandis*

1. to SMS, multimedia messaging or similar services; in such cases, the information referred to in item 2 of subparagraph 1 shall be replaced by the time of despatch and receipt of the message;

2. to unanswered calls or calls that are unsuccessful due to intervention on the part of the network manager …

(3) Providers of publicly available internet access services shall retain:

1. the IP address allocated to the subscriber for the purposes of using the internet;

2. the clear identifier of the connection that provides access to the internet and the allocated network identification number;

3. the date and time of the start and end of internet use from the allocated IP address, stating the time zone.

(4) Where mobile telephony services are used, the designation of the cell sites used at the start of the communication by the caller and the recipient must be retained. In the case of mobile usage of publicly available internet access services, the designation of the cell sites used at the start of the internet connection must be retained. Any data that enable identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question should also be retained.

(5) The content of the communication, data on internet sites visited and data from email services may not be retained pursuant to this provision.

(6) Data underlying the communications referred to in Paragraph 99(2) may not be retained pursuant to this provision. This applies, *mutatis mutandis*, to telephone communications originating from the entities referred to in Paragraph 99(2). The second to seventh sentences of Paragraph 99(2) apply *mutatis mutandis*. [14]

…'

13. Paragraph 113c provides as follows:

'(1) Data retained pursuant to Paragraph 113b may be:

1. disclosed to a law enforcement authority, where the authority so requests under a statutory provision which authorises it to collect the data referred to in Paragraph 113b for the purposes of prosecuting particularly serious criminal offences;

2. disclosed to a security authority of the *Länder*, where the authority so requests under a statutory provision which authorises it to collect the data referred to in Paragraph 113b for the purposes of preventing a specific risk to life and limb or a person's freedom or to the existence of the federal State or the *Land*;

3. used by the provider of publicly available telecommunications services in order to supply information pursuant to the third sentence of Paragraph 113(1).

[14] The communications referred to in Paragraph 99(2) of the TKG are communications with persons, authorities and organisations of a social or religious nature offering telephone assistance in psychological or social emergencies to callers who in principle remain anonymous, which are subject to specific confidentiality obligations. Under the second to fourth sentences of Paragraph 99(2) of the TKG, this exemption is conditional on inclusion on a register held by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Agency for Electricity, Gas, Telecommunications, Post and Rail Networks; 'the Federal Network Agency'), for which proof of the nature of the services provided is required in the form of a certificate issued by an entity, body or foundation governed by public law.

(2) Data retained pursuant to Paragraph 113b may not be used by persons who are subject to the obligations established in Paragraph 113a(1) for purposes other than those provided for in subparagraph 1.

…'

14. Paragraph 113d provides as follows:

'A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that the data retained pursuant to the retention obligation in Paragraph 113b(1) are protected by state-of-the-art technical and organisational measures against unauthorised access and use. These measures shall include, in particular:

1. use of a particularly secure encryption method;

2. storage in separate storage facilities that are separate from those designated for normal operational tasks;

3. storage that provides a high level of protection against cyber-attacks, in isolated data processing systems;

4. measures to ensure that access to the data processing facilities is restricted to persons who have been specially authorised by the obliged party; and

5. a requirement for at least two persons who have been specially authorised by the obliged party to be involved when the data are accessed.'

15. Paragraph 113e provides as follows:

'(1) A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that all access, in particular the reading, copying, alteration, deletion and blocking of data retained pursuant to the retention obligation under Paragraph 113b(1), is logged for data protection control purposes. The following data must be logged:

1. the time of access;

2. the persons accessing the data;

3. the purpose and nature of the access.

(2) The log data may not be used for purposes other than data protection control.

(3) A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that the log data are deleted after one year.'

2. Strafprozessordnung (Code of Criminal Procedure; 'the StPO')

16. Paragraph 100g provides as follows:

'…

(2) Where there is prima facie evidence that someone has been the perpetrator of or an accessory to one of the particularly serious criminal offences referred to in the second sentence or, in those cases where an attempted offence is punishable, that someone has attempted to commit the offence in question and it is a particularly serious instance of the offence, the traffic data retained pursuant to Paragraph 113b of the [TKG] may be collected if the investigation of the facts or the determination of the whereabouts of the person under investigation would otherwise be significantly impeded or impracticable and the collection of the data is proportionate to the importance of the matter.

…

(4) Traffic data may not be collected pursuant to subparagraph 2 … where the data in question may lead to information about which the person in question could decline to give evidence …'

17. Paragraph 101a(1) establishes that judicial authority is required for the collection of traffic data pursuant to Paragraph 100g of the StPO. Paragraph 101a(2) of the StPO stipulates that the judicial decision must assess whether the measure is necessary and appropriate in the specific circumstances; those involved in the communication must be informed of the measure (Paragraph 101(6) of the StPO).

II. Facts, proceedings and questions referred

18. SpaceNet AG and Telekom Deutschland GmbH are companies that provide publicly available internet access services in Germany.

19. The two companies lodged actions with the Verwaltungsgericht (Administrative Court, Germany), objecting to the obligation set out in Paragraph 113a(1) in conjunction with Paragraph 113b of the TKG to store customers' telecommunications traffic data as from 1 July 2017.

20. In each case, after the companies' applications were upheld at first instance, the Federal Network Agency filed an appeal with the Bundesverwaltungsgericht (Federal Administrative Court) which, in each of the two proceedings, has ordered the following question to be referred for a preliminary ruling before giving judgment:

'In the light of Articles 7, 8 and 11 and Article 52(1) of the Charter …, on the one hand, and of Article 6 of the Charter … and Article 4 [TEU], on the other hand, is Article 15 of Directive 2002/58/EC to be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services where:

— that obligation does not require a specific reason in terms of location, time or region;

— the following data are the subject of the storage obligation in the provision of publicly available telephone services – including the transmission of short messages, multimedia messages or similar messages and unanswered or unsuccessful calls:

— the telephone number or other identifier of the calling and called parties as well as, in the case of call switching or forwarding, of every other line involved;

— the date and time of the start and end of the call or – in the case of the transmission of a short message, multimedia message or similar message – the times of dispatch and receipt of the message, and an indication of the relevant time zone;

— information regarding the service used, if different services can be used in the context of the telephone service;

— and also, in the case of mobile telephone services:

— the International Mobile Subscriber Identity of the calling and called parties;

— the international identifier of the calling and called terminal equipment;

— in the case of pre-paid services, the date and time of the initial activation of the service, and an indication of the relevant time zone;

— the designations of the cells that were used by the calling and called parties at the beginning of the call;

— in the case of internet telephone services, the Internet Protocol addresses of the calling and the called parties and allocated user IDs;

— the following data are the subject of the storage obligation in the provision of publicly available internet access services:

— the Internet Protocol address allocated to the subscriber for internet use;

— a unique identifier of the connection via which the internet use takes place, as well as an allocated user ID;

— the date and time of the start and end of the internet use at the allocated Internet Protocol address, and an indication of the relevant time zone;

— in the case of mobile use, the designation of the cell used at the start of the internet connection;

— the following data must not be stored:

— the content of the communication;

— data regarding the internet pages accessed;

— data from electronic mail services;

— data underlying links to or from specific connections of persons, authorities and organisations in social or ecclesiastical spheres;

— the retention period is 4 weeks for location data, that is to say, the designation of the cell used, and 10 weeks for the other data;

— effective protection of retained data against risks of misuse and against any unlawful access to that data is ensured, and

— the retained data may be used only to prosecute particularly serious criminal offences and to prevent a specific threat to life and limb or a person's freedom or to the continued existence of the Federal Republic or of a Federal *Land*, with the exception of the Internet Protocol address allocated to a subscriber for internet use, the use of which data is permissible in the context of the provision of inventory data information for the prosecution of any criminal offence, maintaining public order and security and carrying out the tasks of the intelligence services?'

21. The referring court explained that regulation of the disputed obligation was amended by a Law of 10 December 2015, [15] which became necessary following:

— the judgment of the Bundesverfassungsgericht (Federal Constitutional Court, Germany) of 2 March 2010, [16] which declared the previous provisions governing data retention to be unconstitutional; and

— the declaration that Directive 2006/24, which those provisions had been enacted in order to implement, was invalid.

22. The referring court considers that the disputed storage obligation restricts the rights provided for in Articles 5(1), 6(1) and 9(1) of Directive 2002/58. In its opinion, such a restriction would be justified only if it were covered by Article 15(1) of the directive.

23. In the view of the referring court, notwithstanding the case-law established by the judgment in *Tele2 Sverige*, Article 15(1) of Directive 2002/58 could provide a basis for the obligation at issue in the proceedings for the following reasons:

— The applicable national provisions do not require storage of all telecommunications traffic data of *all* users and subscribers in relation to *all* means of electronic communication.

— Those provisions have significantly reduced the storage period (to a maximum of 10 weeks) as compared with the period provided for in the legislation examined in the judgment in *Tele2 Sverige* and that provided for in Directive 2006/24, thus making it harder to establish profiles.

— Strict limits have been imposed regarding protection of stored data and access to and use of those data.

[15] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Law introducing a storage obligation and a maximum storage period for traffic data).

[16] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (DE:BVerfG:2010:rs20100302.1bvr025608).

— The legislature has restricted itself to complying with the duties to act entailed by the right to security (Article 6 of the Charter). [17]

— If, as a general rule, it is not possible to rely on Article 15(1) of Directive 2002/58 as a basis for the storage of data 'without a reason' [18] (in other words, if the form taken by the legislation governing the means of telecommunications involved, the categories of data stored, the retention period, the conditions governing access to the stored data and protection against the risks of misuse proved to be irrelevant), the national legislature's room for manoeuvre in the field of law enforcement and national security, which remains the sole responsibility of Member States pursuant to the third sentence of Article 4(2) TEU, would be significantly reduced.

— There must be consistency between the rights enshrined in the Charter and those guaranteed by the European Convention on Human Rights and Fundamental Freedoms ('the ECHR') as interpreted by the European Court of Human Rights ('the ECtHR'), without prejudice to the autonomy of EU law and the authority of the Court.

III. Proceedings before the Court of Justice

24. The requests for a preliminary ruling were lodged with the Court on 29 October 2019.

25. Written observations were submitted by SpaceNet, Telekom Deutschland, the Danish, German, and Estonian Governments, Ireland, the Spanish, French, Netherlands, Polish, Finnish and Swedish Governments, and the Commission.

26. Following the judgment in *La Quadrature du Net*, the referring court was asked whether it wished to withdraw the question referred and, on 13 January 2021, it stated that it wished to continue with the reference, since the question could not be considered to have been answered by that judgment.

27. The public hearing was held jointly with that for the related Case C-140/20 on 13 September 2021, at which, in addition to the parties who had submitted written observations in the proceedings, the Federal Network Agency and the European Data Protection Supervisor also appeared.

IV. Analysis

A. Preliminary consideration

28. These two requests for a preliminary ruling can be addressed either by analysing them in the form they were originally made, or by focusing on the considerations cited by the referring court in its response to the Court of 13 January 2021 as grounds for maintaining the request after learning of the judgment in *La Quadrature du Net*.

[17] According to the referring court, the case-law of the Court does not categorically rule out the possibility of national legislatures making provision, following an appropriate evaluation, for storage of data without a reason (supplemented, where necessary, by strict access rules) to reflect the specific potential risk associated with new means of telecommunication.

[18] This is the precise phrase used by the referring court.

29. While I shall briefly address the most relevant points from the original requests for a preliminary ruling, I shall focus on analysing the reasons why the referring court considers that the involvement of the Court is still relevant. In summary, the premiss underpinning all those reasons is that the underlying legislative position differs from that under consideration in the judgment in *La Quadrature du Net*.

30. In its communication of 13 January 2021, the referring court put forward the following arguments:

— There are appreciable differences between the German legislation and the French and Belgian legislation addressed by the judgment in *La Quadrature du Net*. Under the former, no data are retained in respect of internet sites visited, emails, or communications to or from social or religious telephone helplines.

— Another even more significant difference is that, under Paragraph 113b(1) of the TKG, the retention period is 4 or 10 weeks, rather than one year. This reduces the risk of being able to establish a comprehensive profile of the persons involved.

— The German legislation provides effective protection for retained data against the risks of misuse and unlawful access.

— Following a recent judgment by the Bundesverfassungsgericht (Federal Constitutional Court) concerning Paragraph 113 of the TKG,[19] the application of that provision has been made subject to conditions whose compatibility with EU law is not easy to determine.

— Uncertainty remains over the requirements of EU law concerning IP addresses, because it is not clear from the judgment in *La Quadrature du Net* whether there is a general prohibition on retaining such data, and there is a certain tension between paragraphs 168 and 155 of the judgment.

B. Applicability of Directive 2002/58

31. In essence, Ireland and the French, Netherlands, Polish and Swedish Governments maintain that Directive 2002/58 does not apply to national legislation such as that at issue in these proceedings. Since the purpose of the legislation is to safeguard national security and to prevent and prosecute serious criminal offences, it falls within the exclusive competence of Member States pursuant to Article 4(2) TEU.

32. This objection has been emphatically rejected by the Court in the judgment in *La Quadrature du Net*, when it declared that 'national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58'.[20]

[19] Judgment of 27 May 2020, 1 BvR 1873/13, 1 BvR 2618/13 (DE:BVerfG:2010:rs20100302.1bvr025608). According to the judgment, Paragraph 113 of the TKG is incompatible with Paragraphs 2(1) and 10(1) of the Grundgesetz (Basic Law) and may remain in force only until new regulations are enacted, and until 31 December 2021 at the latest.

[20] The judgment in *La Quadrature du Net*, paragraph 104.

33. The referring court accepts this premiss when it endorses the view of the first-instance court and adds that the application of Directive 2005/58 to this situation had been 'definitively established' by the judgment in *Tele2 Sverige*.[21]

34. I shall therefore not dwell any further on this point, on which I had occasion to express my views, which reflect the position adopted by the Court, in my Opinion in *La Quadrature du Net*.[22]

C. General and indiscriminate retention versus targeted retention of traffic and location data

35. At the heart of the case-law of the Court concerning Directive 2002/58 is the notion 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.[23]

36. Article 15(1) of Directive 2002/58 allows exceptions to the obligation to ensure confidentiality and to the corresponding obligations in the terms which I shall set out below. The judgment in *La Quadrature du Net* considers at length how to reconcile those exceptions with the fundamental rights whose exercise may be affected.[24]

37. According to the Court, the general and indiscriminate retention of traffic data could be justified only on grounds 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'.[25]

38. In those circumstances (national security), the Court has declared 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'.[26]

39. Those provisions certainly result in a more rigorous and stricter regime than the one which emerges from the case-law of the ECtHR on Article 8 ECHR. The fact that 'the meaning and scope of rights' in the Charter that correspond to rights guaranteed by the ECHR must be the same as those laid down by the latter does not prevent EU law providing more extensive protection, in accordance with the final sentence of Article 52(3) of the Charter.

21 Paragraph 19(a) of the order for reference.

22 My Opinion in *La Quadrature du Net*, points 40 to 90.

23 The judgment in *La Quadrature du Net*, paragraph 109.

24 *Ibidem*, paragraphs 111 to 133.

25 The judgment in *La Quadrature du Net*, paragraph 136.

26 *Ibidem*, paragraph 137 (italics added). The Court goes on to say that this 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', and therefore it must 'be considered that the existence of that threat is, in itself, capable of establishing that connection' (*loc. cit.*).

40. Moreover, the case-law of the ECtHR in its judgments of 25 May 2021, *Big Brother Watch and Others v. the United Kingdom* [27] and *Centrum för Rättvisa v. Sweden*, [28] and in the judgment of 4 December 2015, *Roman Zakharov v. Russia*, [29] concerns situations which, as was argued by most parties during the hearing, are not comparable to the situations at issue in the references for a preliminary ruling under consideration here. The answer to the latter must be arrived at by applying national legislation which is deemed compliant with the *exhaustive* regulation in Directive 2002/58, as interpreted by the Court.

41. Whatever one's opinion on the invocation of national security, in the judgment in *La Quadrature du Net*, as grounds for lifting, under certain conditions, the prohibition on general and indiscriminate retention of traffic and location data (in my view, the boundaries established by the Court are too wide), the principles set out in paragraphs 137 to 139 of that judgment must be respected.

42. Outside that hypothesis, one must analyse whether the national regulations are founded on criteria that are sufficiently *targeted* to satisfy the conditions which, according to the case-law of the Court, may justify a particularly serious interference, such as retention of data, in the fundamental rights that are affected.

43. The *targeted retention* of traffic and location data [30] is the cornerstone of the reasoning in the judgments of the Court on this matter. That targeting may be established in accordance with the categories of persons concerned [31] or based on geographical criteria, [32] among others.

44. Both the referring court and the majority of the parties who submitted observations highlight the difficulties entailed by the criteria established by the Court. I myself noted some of those difficulties [33] in my Opinion in *Ordre des barreaux francophones et germanophone*. [34]

45. However, forms of targeted retention based on those criteria which may be both effective and non-discriminatory should not be ruled out. It is for national legislatures, not the Court, to design such formulas in a way that is respectful of the protection of fundamental rights guaranteed by the Charter. [35]

46. I also wish to emphasise that it would be wrong to conclude that criteria relating to personal and geographic data are the only criteria compatible with Article 15(1) of Directive 2002/58, having regard to the rights safeguarded in the Charter.

27 CE:ECHR:2021:0525JUD005817013.

28 CE:ECHR:2021:0525JUD003525208.

29 CE:ECHR:2015:1204JUD004714306.

30 The 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.

31 The judgment in *La Quadrature du Net*, paragraphs 148 and 149.

32 The judgment in *La Quadrature du Net*, paragraph 150.

33 In addition to being insufficient, there is also the possibility that they could have the effect of creating a climate of general suspicion in relation to certain segments of the population or of stigmatising certain geographical areas.

34 My Opinion in *Ordre des barreaux francophones et germanophone*, points 88 and 89.

35 *Ibidem*, point 90.

47. Although the French Government maintains that they have been shown to be ineffective, [36] I do not believe that the methods proposed by the Council working groups [37] for defining rules on retention and access that are compatible with the case-law of the Court should be dismissed. [38]

48. In my judgement, the preferred option would be the temporary retention of certain *categories* of traffic and location data which would be limited according to the strict needs of security and which, taken as a whole, could not be used to obtain a clear and detailed picture of the lives of the persons concerned. In practice, this means that within the two main categories (traffic data and location data), retention should only be available, via the appropriate filters, for the *minimum* amount of data deemed absolutely essential for effectively preventing and monitoring crime and safeguarding national security. [39]

49. In any event, I repeat, it is for the Member States or the institutions of the European Union to conduct this selection exercise by way of legislation (with the assistance of their own experts), while abandoning any attempt to prescribe the general and indiscriminate storage of all traffic and location data. [40]

50. That is why, in my Opinion in *Ordre des barreaux francophones et germanophone* I stated that 'the legislative difficulty – which I recognise – of providing a detailed definition of the circumstances and conditions under which targeted retention is feasible is no reason for the Member States, by turning the exception into a rule, to make the general retention of personal data the core principle of their legislation. To do so would be to lend indefinite validity to a significant infringement of the right to the protection of personal data'. [41]

D. Paragraph 168 of the judgment in La Quadrature du Net

51. In this context, the essential elements required for a reply to the referring court can, in my view, be discerned directly from the case-law of the Court concerning Article 15(1) of Directive 2002/58, which is summarised in the judgment in *La Quadrature du Net*.

[36] Paragraph 47 of its written observations. The same position was also taken by some governments at the hearing.

[37] Groupe Échange d'informations et protection des données (DAPIX). The Swedish Government expressed the same view in paragraph 21 of its written observations.

[38] In point 92 of my Opinion in *Ordre des barreaux francophones et germanophone* I noted that the avenues for exploration considered by those working groups include limiting the categories of data retained; pseudonymising data; introducing limited retention periods; excluding certain categories of provider of electronic communications services; renewable storage authorisations; the obligation to retain data stored within the European Union or the systematic and regular supervision by an independent administrative authority of the guarantees given by providers of electronic communications services against the misuse of data.

[39] My Opinion in *Ordre des barreaux francophones et germanophone*, points 93 and 94.

[40] *Ibidem*, point 95.

[41] *Ibidem*, point 104.

52. I must therefore begin with a reminder of the case-law of the Court in that judgment, which is summarised in paragraph 168 of the judgment 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.'

E. Evaluation of the legislation at issue in these references for a preliminary ruling in the light of the judgment in La Quadrature du Net

53. According to the referring court, which is exclusively competent to interpret the German legislation, the legislation requires 'the general retention, without any reason, and without any distinction in terms of personal, temporal or geographical factors, of a large part of the traffic

data of the relevant telecommunications'. [42]

54. The national legislation at issue does not simply authorise the competent authorities to require the retention of traffic and location data for a limited period: the legislature directly imposes an obligation to retain the data indefinitely.

55. Having established this premiss, in its communication of 13 January 2021 the referring court has listed the disparities between the national legislation and the legislation under consideration in the judgment in *La Quadrature du Net* which could lead to a different solution from the one adopted there.

56. I shall analyse those disparities in the order in which they are set out by the referring court, but before doing so I must acknowledge that the German legislature has given serious thought to the task of reconciling national legislation with the requirements posed in this field by the case-law established by the Court.

57. As noted by the referring court, the legislation at issue is the result of a legislative amendment triggered by the case-law of the Bundesverfassungsgericht (Federal Constitutional Court) and by the ramifications of the case-law established in the judgment in *Digital Rights*.

58. The progress that has been achieved in the national legislation at issue is therefore deserving of praise, as indicative of a clear desire to adapt to the requirements of the case-law of the Court.

59. However, legislative efforts have perhaps focused more on aspects relating to the protection of and access to retained data, and less on those concerned with the selective targeting of the data whose retention is necessary.

1. Typology of the retained data

60. The typology of the retained data (there is no storage of data relating to the internet sites visited, email data and data concerning communications to or from social or religious telephone helplines) does not, in my view, obscure the fact that the general and indiscriminate storage requirement applies to a very broad set of traffic and location data and which, overall, is similar to that examined in the judgment in *La Quadrature du Net*.

61. In this context, the fact that data on communications to certain helplines run by social or religious persons, authorities and organisations are excluded is almost irrelevant, given their special characteristics and their very small impact on overall numbers. [43]

62. Nor is the fact that content (whether of internet sites visited or of emails) is not covered by the retention obligation a decisive factor, since the judgment in *La Quadrature du Net* did not refer to content but to traffic and location data relating to electronic communications.

[42] Paragraph 25b(b) of the original German text of the order for reference.

[43] At the hearing, the German Government put the number of undertakings whose electronic communications are excluded from the retention obligation at 1 300, and clarified that the exclusion could not be applied to professionals who were subject to a duty of professional secrecy (such as lawyers or doctors), due to the large number of such persons.

2. Length of the data retention obligation

63. The most significant difference as compared with the national legislation analysed in the judgment in *La Quadrature du Net* concerns the retention period which, under Paragraph 113b(1) of the TKG, is either 4 or 10 weeks (4 weeks for location data and 10 weeks for other data) rather than one year.

64. Both the referring court and some governments who entered an appearance emphasise this point, stressing that the legislation at issue significantly reduces the data retention period. In the view of the referring court, the shorter duration reduces the risk of being able to establish a comprehensive profile of the persons involved.

65. As I maintained in my Opinion in *Ordre des barreaux francophones et germanophone*, along similar lines to the national legislation with which we are now concerned, data retention must be available only for a given period, [44] depending on the category of data concerned. [45]

66. However, while the time limit on the retention period is a relevant factor in assessing the legislation at issue, it cannot correct for the fact that the legislation imposes a general and indiscriminate requirement to retain traffic and location data.

67. I have already explained that, under the case-law of the Court, other than in the case of safeguarding national security, electronic communications data may be retained only on a targeted basis, because of the serious risk entailed by general retention of data.

68. It is that risk which has clearly inspired the case-law of the Court on the matter: 'traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications'. [46]

69. It is true that, as noted by the referring court, a very limited retention period may make it harder to establish profiles.

70. However, the extent of the difficulty in this regard is determined not only by the length of the retention period but also by the quantity and nature of the data that are retained: the greater the amount of data, the greater the likelihood of obtaining sensitive information during time periods the length of which will, in turn, be dependent on developments in techniques for monitoring,

[44] My Opinion in *Ordre des barreaux francophones et germanophone*, point 96. This means that they 'cannot be used to provide a detailed picture of the lives of the persons concerned. That retention period must also be adjusted according to the nature of the data, so that data providing more detailed information on the lifestyles and habits of those persons are stored for a shorter period of time'.

[45] *Ibidem*, point 97. 'In other words, having a different retention period for each category of data depending on how useful the data in question is for the purposes of achieving security objectives is an avenue that must be explored. Curtailing the period of time during which the various categories of data can be stored simultaneously (and, therefore, can be used to find correlations that reveal the lifestyles of the persons concerned) extends the protection afforded to the right enshrined in Article 8 of the Charter.'

[46] The judgment in *La Quadrature du Net*, paragraph 117.

correlating and evaluating the set of electronic communications data. What may at present be an insufficient period in which to accumulate enough information to produce profiles may be more than enough to do so at some point in the future. [47]

71. In any event, according to the Court, 'the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that is entailed by a public authority's access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious *regardless of the length of the period in respect of which access to those data is sought* and the quantity or nature of the data available in respect of such a period, when … that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned'. [48]

72. To sum up, I consider that, in spite of the differences identified by the referring court, the similarities in this regard between the legislation at issue in the proceedings that give rise to this reference and the legislation at issue in the proceedings leading to the judgment in *La Quadrature du Net* mean that it is not possible to disregard the case-law established by that judgment.

3. Protection of data from unlawful access

73. According to the referring court, the German legislation provides effective protection for retained data against the risks of misuse and unlawful access.

74. Without wishing to underestimate the legislative effort expended on data protection and data access, it cannot be forgotten that, for the Court, 'the retention of traffic and location data constitutes, *in itself* … an interference with the fundamental rights to respect for private life and the protection of personal data'. [49] In this regard, 'access to such data is a *separate interference*' with those fundamental rights, irrespective of the subsequent use made of it. [50]

75. For present purposes it is therefore irrelevant that the data protection arrangements for retained data provided for in the German legislation: (a) provide effective safeguards to protect those data; (b) place rigorous and effective limits on access conditions, restricting the circle of people who can access the data; and (c) allow the retained data to be used solely for the purposes of investigating serious offences and preventing specific risks to life or a person's freedom or to the security of the State.

76. The truly decisive element is that, as also noted by the referring court, the retention obligation at issue is not in itself subject to any specific conditions.

[47] As noted during the hearing, even 10 weeks of accumulated metadata (traffic and location data) could be enough to identify patterns in the subscriber's behaviour which, because they are repeated, would reveal sensitive personality and life traits.

[48] Judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 39). Italics added.

[49] The judgment in *La Quadrature du Net*, paragraph 115.

[50] *Ibidem*, paragraph 116. No italics in the original.

4. Relevance of the judgment of the Bundesverfassungsgericht (Federal Constitutional Court) of 27 May 2020

77. The referring court refers to a ruling on Paragraph 113 of the TKG by the Bundesverfassungsgericht (Federal Constitutional Court),[51] which declared the provision to be unconstitutional and which has meant that its continuation in force was subject to conditions whose compatibility with EU law would not be easy to determine.

78. The Court has nothing to say at present on the effects of that judgment, still less on the shape of the new legislation to be enacted (or which may have been enacted) by the German legislature.

79. If, as the referring court says, its judgment in the appeal must be based on the law as it stands at the date of the judgment, it will have to determine for itself whether that law is compatible with EU law in the light of the case-law of the Court on the protection of electronic communications data.

5. IP addresses

80. According to the referring court, the conclusion to be drawn from paragraph 168 of the judgment in *La Quadrature du Net* is that the Court requires the retention of IP addresses to be justified by reference to the objective of safeguarding national security, combating serious crime and preventing serious threats to public security. However, paragraph 155 would appear to indicate that no specific grounds are required for the retention of IP addresses, and that it is only use of the retained data that would necessitate grounds connected with that objective.

81. However, I cannot detect any such tension (still less a contradiction). While paragraph 155 states that the general and indiscriminate retention of IP addresses assigned to the source of a connection 'does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58', the judgment immediately goes on to say, in paragraph 156, that 'in the light of the seriousness of the interference entailed by that retention with the fundamental rights … only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. …'.

82. When taken together, paragraphs 155 and 156 of the judgment in *La Quadrature du Net* therefore lead to the consistent response given by the Court in paragraph 168 of the judgment to the questions on the retention of IP addresses referred in those proceedings.

83. At the hearing, attention was drawn to certain problems concerning the retention of IP addresses which, in the opinion of some parties, required clarification by the Court. In my view, the answer to those problems (which, among others, include problems arising from the difference between dynamic and static IP addresses and the impact of the Ipv6 protocol) goes beyond the question put by the referring court, whose original requests for a preliminary ruling[52] and communication of 13 January 2021 are far more limited in scope on this point.

[51] See footnote 19 to this Opinion.

[52] Paragraph 30 of the order for reference.

V. Conclusion

84. In the light of the above, I suggest to the Court that it should reply to the Bundesverwaltungsgericht (Federal Administrative Court, Germany) in the following terms:

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, in conjunction with Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union and Article 4(2) TEU, must be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services on a precautionary, general and indiscriminate basis for purposes other than that of safeguarding national security in the face of a serious threat that is shown to be genuine and present or foreseeable.