Provisional text

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 15 January 2020 (1)

Joined Cases C−511/18 and C−512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C−511/18)
v
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

(Request for a preliminary ruling from the Conseil d'État (Council of State, acting in its capacity as Supreme Court for administrative-law proceedings, France))

(Reference for a preliminary ruling – Processing of personal data and protection of privacy in the electronic communications sector – Safeguarding national security and combating terrorism – Directive 2002/58/EC – Scope – Article 1(3) – Article 15(3) – Article 4(2) TEU – Charter of Fundamental Rights of the European Union – Articles 6, 7, 8, 11, 47 and 52(1) – General and indiscriminate retention of connection data and data that can be used to identify content creators – Collection of traffic and location data – Access to data)

1. In recent years, the Court has maintained a consistent line of case-law on the retention of, and access to, personal data, the important milestones in which are as follows:

– The judgment of 8 April 2014, *Digital Rights Ireland and Others*, (2) in which it declared Directive 2006/24/EC (3) to be invalid because it permitted a disproportionate interference with the rights recognised in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

– The judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, (4) in which it interpreted Article 15(1) of Directive 2002/58/EC. (5)

– The judgment of 2 October 2018, *Ministerio Fiscal*, (6) in which it confirmed the interpretation of the same provision of Directive 2002/58.

2. Those judgments (in particular the second) are a cause for concern for the authorities of some Member States because, in the view of those authorities, they have the effect of depriving them of an instrument they regard as necessary for the purposes of safeguarding national security and combating crime and terrorism. For that reason, some of those States are calling for that case-law to be repealed or refined.

3. A number of national courts have pointed up that concern in four references for a preliminary ruling (7) on which I am delivering my Opinions today.

4. The principal issue raised by the four cases is the application of Directive 2002/58 to activities related to national security and the combating of terrorism. If that directive is applicable to such matters, it will fall to be determined, next, to what extent Member States may restrict the rights to privacy which it protects. Finally, it will be necessary to analyse to what degree the various bodies of national (UK, (8) Belgian (9) and French (10)) legislation in this field are compliant with EU law as it has been interpreted by the Court.

I. Legislative framework

A. EU law

1. Directive 2002/58

5. According to Article 1 ('Scope and aim'):

'1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

…

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

6. Article 3 ('Services concerned') states:

'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.'

7. Paragraph 1 of Article 5 ('Confidentiality of the communications') provides:

'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.'

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

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

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

…'

9. Paragraph 1 of Article 15 ('Application of certain provisions of Directive 95/46/EC [(11)]') states:

'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. Directive 2000/31/EC (12)

10. Article 14 provides:

'1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

…

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.'

11. According to Article 15:

‘1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.’

3. Regulation (EU) 2016/679 (13)

12. In accordance with Article 2 (‘Material scope’):

‘1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

…’

13. According to paragraph 1 of Article 23 (‘Restrictions’):

‘Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member

State, including monetary, budgetary and taxation … matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.'

14. Article 95 ('Relationship with Directive 2002/58/EC') reads:

'This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.'

B. National law

1. Code de la sécurité intérieure (Internal Security Code)

15. In accordance with Article L. 851-1:

'Subject to the conditions laid down in Chapter I of Title II of this Book, the collection of information or documents processed or retained by their networks or electronic communications services, including technical data relating to the identification of the subscription or connection numbers to electronic communications services, the mapping of all the subscription and connection numbers of a specified person, the location of the terminal equipment used and the communications of a subscriber, namely the list of numbers called and calling and the duration and date of the communications may be authorised from electronic communications operators and the persons referred to in Article L. 34-1 of the Code des postes et des communications électroniques (Post and Electronic Communications Code) as well as from the persons referred to in Article 6(I)(1) and (2) of Loi n.º 2004-575 … pour la confiance dans l'économie numérique (Law No 2004-575 … to promote confidence in the digital economy) …'

16. Articles L. 851-2 and L. 851-4 regulate real-time administrative access to connection data stored in this way, depending on the purposes and methods involved.

17. For the sole purpose of preventing terrorism, Article L. 851-2 authorises the collection of the information or documents referred to in Article L. 851-1 from the aforementioned persons. The collection of such information or documents, in relation to only one or more persons previously identified as being suspected having links to a terrorist threat, is to be carried out in real time. The same is true of Article L. 851-4, which authorises the real-time transmission by operators only of technical data relating to the location of terminal equipment. (14)

18. Article L. 851-3 allows electronic communications operators and providers of technical

services to be required to ‘engage on their networks in automated processing intended, within the parameters specified in the authorisation, to detect connections capable of disclosing a terrorist threat’. (15)

19. Article L. 851-5 states that, under certain conditions, ‘the use of a technical device enabling a person, vehicle or object to be located in real time may be authorised’.

20. Under Article L. 851-6(I), ‘the technical connection data by which terminal equipment or the subscription number of its user can be identified, and data relating to the location of the terminal equipment used, may, under certain conditions, be collected directly by means of a technical apparatus or device as referred to in Article 226-3(1) of the Code pénal (Criminal Code)’.

2. Post and Electronic Communications Code

21. According to Article L. 34-1, in the version applicable to the facts:

‘I. This article shall apply to the processing of personal data in the course of the provision to the public of electronic communications services; it shall apply in particular to networks that support data collection and identification devices.

II. Electronic communications operators, in particular persons whose business is to provide access to online public communication services, shall erase or render anonymous any data relating to traffic, subject to the provisions contained in points III, IV, V and VI.

Persons who provide electronic communications services to the public shall, with due regard for the provisions contained in the preceding paragraph, establish internal procedures for responding to requests from the competent authorities.

Persons who, as a principal or ancillary business activity, provide to the public a connection allowing online communication via access to the network shall, including where this is offered free of charge, be subject to compliance with the provisions applicable to electronic communications operators under this article.

III. For the purposes of investigating, detecting and prosecuting criminal offences or a failure to fulfil an obligation laid down in Article L. 336-3 of the Code de la propriété intellectuelle (Intellectual Property Code) or for the purposes of preventing breaches of automated data processing systems as provided for and punishable under Articles 323-1 to 323-3-1 of the Criminal Code, and for the sole purpose of making information available, as necessary, to the judicial authority or high authority mentioned in Article L. 331-12 of the Intellectual Property Code or to the national authority for the security of information systems mentioned in Article L. 2321-1 of the Code de la défense (Defence Code), operations designed to erase or render anonymous certain categories of technical data may be deferred for a maximum period of one year. A decree adopted in the Conseil d’État (Council of State, France) following consultation of the Commission nationale de l’informatique et des libertés (French Data Protection Authority) shall, within the limits laid down in point VI, determine the categories of data involved and the period for which they are to be retained, depending on the business of the operators, the nature of the communications and the methods of offsetting any identifiable and specific additional costs associated with the services provided for these purposes by operators at the request of the State.

…

VI. Data retained and processed under the conditions set out in points III, IV and V shall relate exclusively to the identification of persons using the services provided by operators, the technical characteristics of the communications provided by the latter and the location of terminal equipment.

Under no circumstance may such data relate to the content of the correspondence exchanged or the information consulted, in any form whatsoever, as part of those communications.

The retention and processing of such data shall be effected with due regard for the provisions of Law No 78-17 of 6 January 1978 on information technology, files and freedoms.

Operators shall take any measures necessary to prevent such data from being used for purposes other than those provided for in this article.'

22. Article R. 10-13(I) provides that, for the purposes of investigating, detecting and prosecuting criminal offences, operators must retain the following data:

'(a) Information identifying the user;

(b) Data relating to the communications terminal equipment used;

(c) The technical characteristics and date, time and duration of each communication;

(d) Data relating to the additional services requested or used and the providers of those services;

(e) Data identifying the addressee or addressees of the communication.'

23. Point II of that same provision states that, in the case of telephony activities, the operator is also to retain data enabling the origin and location of the communication to be identified.

24. Point III of the same article provides that the retention period for the data mentioned in that article is to be one year as from the date of recording.

3. Loi No 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy)

25. The first paragraph of Article 6(II) of Law No 2004-575 provides that persons whose business is to provide access to online public communication services and natural or legal persons who, for the purposes of making them available to the public via online public communication services, store, even free of charge, signals, texts, images, sounds or messages of any nature provided by the recipients of those services 'shall keep and retain the data in such a way as to make it possible to identify anyone who has assisted in the creation of all or part of the content of the services of which they are the providers'.

26. The third paragraph of point II of that provision states that the judicial authority may require those persons to communicate the data referred to in the first paragraph.

27. According to the final paragraph of point II, a decree adopted by the Conseil d'État (Council of State) 'shall define the data referred to in the first paragraph and determine the period for which, and the methods by which, those data are to be retained'. (16)

II. Facts and questions referred for a preliminary ruling

A. Case C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net and the Fédération des fournisseurs d'accès à internet associatifs ('the applicants') made an application to the Conseil d'État (Council of State) for the annulment of various decrees implementing certain provisions of the Internal Security Code. (17)

29. The applicants maintained, in essence, that the contested decrees and the aforementioned provisions of the Internal Security Code were contrary to the rights to respect for private life, the protection of personal data and an effective remedy as guaranteed by Articles 7, 8 and 47 of the Charter respectively.

30. On that basis, the Conseil d'État (Council of State) has raised the following questions:

'(1) Is the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of [Directive 2002/58] to be regarded, against a background of serious and persistent threats to national security, and in particular the terrorist threat, as interference justified by the right to security guaranteed in Article 6 of the Charter … and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 [TEU]?

(2) Is [Directive 2002/58], read in the light of the Charter …, to be interpreted as authorising legislative measures, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?

(3) Is [Directive 2002/58], read in the light of the Charter …, to be interpreted as making the legality of the procedures for the collection of connection data subject in all cases to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural guarantees, since those guarantees ensure that the right to a remedy is effective?'

B. Case C-512/18

31. The applicants in the dispute that has given rise to Case C-511/18, with the exception of Igwan.net, also made an application to the Conseil d'État (Council of State) for the annulment of the rejection (in the form of administrative silence) of their application for the repeal of Article R. 10-13 of the Code des postes et des communications électroniques (Post and Electronic Communications Code) and of Decree No 2011-219 of 25 February 2011.

32. The applicants claim that the contested provisions impose an obligation to retain traffic, location and connection data which, because of its general nature, constitutes a disproportionate interference with the rights to respect for private and family life, the protection of personal data and freedom of expression, protected by Articles 7, 8 and 11 of the Charter, and an infringement of Directive 2002/58.

33. In the course of those proceedings, the Conseil d'État (Council of State) referred the

following questions for a preliminary ruling:

‘(1) Is the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of [Directive 2002/58] to be regarded, inter alia in the light of the guarantees and checks to which the collection and use of such connection data are then subject, as interference justified by the right to security guaranteed in Article 6 of the Charter … and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 [TEU]?

(2) Are the provisions of [Directive 2000/31], read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter …, to be interpreted as allowing a State to introduce national legislation requiring the persons whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that the judicial authority may, where appropriate, require the communication of those data with a view to ensuring compliance with the rules on civil and criminal liability?’

III. Procedure before the Court and positions of the parties

34. The questions referred for a preliminary ruling were registered at the Court on 3 August 2018.

35. Written observations have been lodged by La Quadrature du Net, the Fédération des fournisseurs d’accès à Internet associatifs, French Data Network, the Belgian, Czech, Danish, German and Estonian Governments, Ireland, the Spanish, French, Cypriot, Hungarian, Polish, Swedish and United Kingdom Governments and the Commission.

36. A hearing held on 9 September 2019 in conjunction with the hearings in Cases C−623/17, *Privacy International*, and C−520/18, *Ordre des barreaux francophones et germanophone and Others*, was attended by the parties in the four references for a preliminary ruling, the aforementioned governments and those of the Netherlands and Norway, the Commission and the European Data Protection Supervisor.

IV. Analysis

37. The questions raised by the Conseil d’État (Council of State) can be grouped into three:

– In the first place, whether national legislation which imposes on providers of electronic communications services an obligation to engage in the general and indiscriminate retention of connection data (first question in Case C−511/18 and Case C−512/18) and, in particular, data that can be used to identify the creators of the content offered by those providers (second question in Case C−512/18) is compatible with EU law.

– In the second place, whether the lawfulness of the procedures for the collection of connection data is in any event subject to the obligation to inform the persons concerned in the case where the investigations are not jeopardised (third question in Case C−511/18).

– In the third place, whether the real-time collection of traffic and location data in the absence of any obligation to retain them is compatible – and, if so, under what conditions – with Directive 2002/58 (second question in Case C−511/18).

38. It falls to be determined, in short, whether it is consistent with EU law for national legislation to impose on providers of electronic communications services two types of obligation: (a) on the one hand, to *collect* but not retain certain data; and (b) on the other hand, to *retain* connection data and data that can be used to identify the creators of the content of the services provided by such suppliers.

39. First of all, it will be necessary, on account of the very background (18) against which the national legislation in question has been enacted (that is to say, in circumstances in which national security may be compromised), to determine whether Directive 2002/58 is applicable.

A. The applicability of Directive 2002/58

40. The referring court takes it as read that the legislation at issue falls within the scope of Directive 2002/58. This follows, in its opinion, from the case-law established in the judgment in *Tele2 Sverige and Watson* and borne out in the judgment in *Ministerio Fiscal*.

41. Conversely, some of the governments which have intervened in these proceedings have stated that the legislation at issue does not fall within the scope of the aforementioned directive. In support of their position, they cite, inter alia, the judgment of 30 May 2006, *Parliament* v *Council and Commission*. (19)

42. I agree with the Conseil d'État (Council of State) that the judgment in *Tele2 Sverige and Watson* has settled this part of the debate and confirms that Directive 2002/58 is applicable in principle where providers of electronic services are required by law to retain data belonging to their subscribers and to allow the public authorities to have access to such data. The fact that those obligations are imposed on providers for reasons of national security does nothing to alter that proposition.

43. I should say here and now that, if there were any inconsistency between the judgment in *Tele2 Sverige and Watson* and the previous judgments, the former would have to be assumed to prevail inasmuch as it post-dates the others and has been endorsed by the judgment in *Ministerio Fiscal*. To my mind, however, there is no such inconsistency, as I shall attempt to explain.

1. Judgment in Parliament v Council and Commission

44. The cases settled by the judgment in *Parliament* v *Council and Commission* related to:

– The Agreement between the European Community and the United States of America on the processing and transfer of PNR [Passenger Name Records] data by air carriers to the US authorities. (20)

– The adequacy of the protection afforded to the personal data contained in the Passenger Name Records transferred to those authorities. (21)

45. The Court concluded that the transfer of such data was a processing operation concerning public security and the activities of the State in areas of criminal law. In accordance with Article 3(2), first indent, of Directive 95/46, the two contested decisions did not fall within the scope of Directive 95/46.

46. The data were initially collected by airlines in the course of an activity – the sale of tickets – falling within the scope of EU law. However, the processing of those data in the manner provided for in the contested decision was 'not … necessary for a supply of services, but … regarded as necessary for safeguarding public security and for law-enforcement purposes'. (22)

47. The Court thus took a teleological approach, taking into account the purpose behind the processing of the data: if the data processing were intended to protect public security, it had to be regarded as falling outside the scope of Directive 95/46. The purpose of the processing was not the only decisive criterion, however, (23) and it was for this reason that the Court pointed out that the processing 'falls within a framework established by the public authorities that relates to public security'. (24)

48. The judgment in *Parliament* v *Council and Commission* thus makes apparent the difference between the exclusion clause and the restriction or limitation clauses in Directive 95/46 (similar to those in Directive 2002/58). It is true, however, that both types of clause relate to similar objectives in the public interest and there is therefore some confusion as to the scope commanded by each, as Advocate General Bot noted at the time. (25)

49. It is probably this confusion that underpins the line of argument put forward by those Member States who claim that Directive 2002/58 is inapplicable to this context. In their view, the national security interest is safeguarded only by means of the exclusion provided for in Article 1(3) of Directive 2002/58. The fact is, however, that that same interest is also served by the limitations authorised by Article 15 of the aforementioned directive, including that relating to national security. The latter provision would be superfluous if Directive 2002/58 were inapplicable in the presence of any reliance on national security.

2. Judgment in Tele2 Sverige and Watson

50. The judgment in *Tele2 Sverige and Watson* concerned whether certain national schemes which imposed on providers of publicly accessible electronic communications services a general obligation to retain data relating to those communications. The circumstances were therefore substantially the same as those at issue in the present references for a preliminary ruling.

51. Faced once again with the issue of the applicability of EU law – now in the guise of Directive 2002/58 – the Court started by saying that 'a determination of the scope of Directive 2002/58 must take into consideration, inter alia, the general structure of that directive'. (26)

52. With this in mind, the Court noted that, 'admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active … Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security …, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive'. (27)

53. Thus, the objective pursued by the measures which Member States may adopt under Article 15(1) of Directive 2002/58 in order to limit the right to privacy is the same (in this regard) as that which operates as a justification for exempting certain State activities from the scheme of the directive under Article 1(3) thereof.

54. However, the Court took the view that, 'having regard to the general structure of Directive 2002/58', that fact did not permit 'the conclusion that the legislative measures

referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein … fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met'. (28)

55. The Court went on to say that the limitations authorised by Article 15(1) of Directive 2002/58 'govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services'. It follows that that provision, combined with Article 3 of that directive, 'must be interpreted as meaning that such legislative measures fall within the scope of that directive'. (29)

56. Consequently, the Court held that the scope of Directive 2002/58 extends both to a legislative measure that imposes on providers an obligation 'to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data' (30) and to one that governs access by the national authorities to the data retained by those providers. (31)

57. The interpretation of Directive 2002/58 adopted by the Court in the judgment in *Tele2 Sverige and Watson* is reiterated in the judgment in *Ministerio Fiscal*.

58. Could the judgment in *Tele2 Sverige and Watson* be said to represent a more or less implicit reversal of the case-law established in the judgment in *Parliament* v *Council and Commission*? That is the view taken, for example, by Ireland, which submits that the latter judgment alone is compatible with the legal basis of Directive 2002/58 and respectful of Article 4(2) TEU. (32)

59. The French Government, for its part, takes the view that that contradiction might be overcome by taking into account the fact that the case-law laid down in the judgment in *Tele2 Sverige and Watson* refers to activities of the Member States in matters of criminal law, whereas that established in the judgment in *Parliament* v *Council and Commission* is concerned with State security and defence. On that basis, the case-law in the judgment in *Tele2 Sverige and Watson* would not apply to the situation under examination here, for the purposes of which regard would have to be had to the ruling given in the judgment in *Parliament* v *Council and Commission*. (33)

60. To my mind, as I have already said, those two judgments can be reconciled in a different way from that favoured by the French Government. I do not concur with the latter approach, since, in my opinion, the explicit references which the judgment in *Tele2 Sverige and Watson* makes to the fight against terrorism (34) can be extended to any other threat to national security (including terrorism).

3. Whether an interpretation can be found that reconciles the judgment in Parliament v Council and Commission with the judgment in Tele2 Sverige and Watson

61. I am of the view that, in the judgments in *Tele2 Sverige and Watson* and *Ministerio Fiscal*, the Court took into account the rationale behind the exclusion and restriction clauses and the schematic relationship between those two types of clause.

62. While, in *Parliament* v *Council and Commission*, the Court stated that data processing fell outside the scope of Directive 95/46, this, as I have noted, was due to the fact that, in the context of the cooperation between the European Union and the United States, pursued within a typically international framework, the State dimension of the activity had to take precedence

over the fact that the processing in question would also entail a commercial or private dimension. Indeed, one of the very matters at issue was the appropriate legal basis for the contested decision.

63. In the case of the national measures examined in the judgments in *Tele2 Sverige and Watson* and *Ministerio Fiscal*, on the other hand, the Court placed at the forefront of its considerations the domestic scope of the data processing concerned: the legislative framework within which this took place was exclusively national, and the external dimension that characterised the subject matter of the judgment in *Parliament* v *Council and Commission* was therefore absent.

64. The different weightings of the international and domestic (commercial and private) dimensions of data processing meant that, in the first case, the EU-law exclusion clause was imposed as being the most appropriate for the purposes of protecting the public interest in national security. In the second case, on the other hand, that same interest could be effectively served by the limitation clause contained in Article 15(1) of Directive 2002/58.

65. Another dissimilarity, linked to the different legislative contexts, is in evidence too: those judgments were concerned with the interpretation of two provisions which, other than in appearance, are not the same.

66. Thus, in the judgment in *Parliament* v *Council and Commission*, the Court ruled on the interpretation of Article 3(2) of Directive 95/46, while, in the judgment in *Tele2 Sverige and Watson*, it ruled on Article 1(3) of Directive 2002/58. A careful reading of those articles shows that there is between them a difference sufficient to support the purport of the rulings given by the Court in those two cases.

67. In accordance with Article 3(2) of Directive 95/46, 'this Directive *shall not apply to the processing of personal data* … in the course of an activity which falls outside the scope of Community law … and in any case *to processing operations* concerning public security, defence, State security (including the economic well-being of the State when the *processing operation* relates to State security matters) and the activities of the State in areas of criminal law'. (35)

68. Article 1(3) of Directive 2002/58 provides for its part that it '*shall not apply to activities* which fall outside the scope of the Treaty establishing the European Community … and in any case *to activities* concerning public security, defence, State security (including the economic well-being of the State when the *activities* relate to State security matters) and the activities of the State in areas of criminal law'. (36)

69. While Article 3(2) of Directive 95/46 excludes the *processing of data* concerning – for our purposes here – State security, Article 1(3) of Directive 2002/58 excludes *activities* aimed at preserving – again, for our purposes here – State security.

70. The difference is not insignificant. Directive 95/46 left out of its scope an activity ('the processing of personal data') which anyone can carry out. Specifically excluded under the heading of that activity were processing operations relating, inter alia, to State security. The nature of the *subject* carrying out the data processing, on the other hand, was irrelevant. The approach taken to identifying the actions excluded was therefore teleological or purposive and made no distinction as to who carried them out.

71. It is understandable that, in *Parliament* v *Council and Commission*, the Court should have had regard first and foremost to the objective pursued by the data processing. The fact

that 'the … data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country' was unimportant, the crucial point being that 'the transfer falls within a framework established by the public authorities that relates to public security'. (37)

72. Conversely, the 'activities concerning State security' that fall outside the scope of Directive 2002/58 as analysed in *Tele2 Sverige and Watson* cannot be carried out by anyone, but only by the State itself. What is more, those activities do not include the State's legislative or regulatory functions, but only the material actions of the public authorities.

73. The *activities* listed in Article 1(3) of Directive 2002/58, after all, 'are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active'. (38) Those 'activities' cannot, however, be legislative. If they were, all provisions adopted by the Member States in connection with the processing of personal data would fall outside the scope of Directive 2002/58 if they claimed to be justified on grounds of being necessary in order to ensure State security.

74. First, this would significantly detract from the effectiveness of that directive, since the mere invocation of a legal concept as indeterminate as national security would be enough to render inapplicable to Member States the safeguards designed by the EU legislature in order to protect citizens' personal data. That protection is impracticable without the cooperation of the Member States and citizens benefit from the guarantee of its provision in relation to national public authorities too.

75. Secondly, an interpretation of the concept of 'activities of the State' as including those resulting in the enactment of rules and provisions of law would render meaningless Article 15 of Directive 2002/58, which specifically empowers the Member States – on grounds of the protection, inter alia, of national security – to adopt 'legislative measures' aimed at reducing the scope of certain rights and obligations provided for in the same directive. (39)

76. As the Court pointed out in *Tele2 Sverige and Watson*, 'a determination of the scope of Directive 2002/58 must take into consideration, inter alia, the general structure of that directive'. (40) From that point of view, a meaningful interpretation of Article 1(3) and Article 15 of Directive 2002/58 that does not detract from their effectiveness is one which regards the first of those two provisions as providing for a material exclusion of the *activities* performed by the Member States in the field of national security (and the like), and the second as empowering the Member States to adopt *legislative measures* (that is to say, provisions of general application) which, in the interests of national security, affect the activities of individuals subject to the authority of the Member States by restricting the rights guaranteed by Directive 2002/58.

4. Exclusion of national security in Directive 2002/58

77. National security (or its synonym 'State security', to which Article 15(1) refers) is addressed in two ways in Directive 2002/58. First, it is grounds for *excluding* (from the application of the directive) all activities of the Member States specifically 'concerning' it. Secondly, it is grounds for *imposing restrictions*, which must be adopted by legislative measures, on the rights and obligations provided for in Directive 2002/58, that is, in connection with private or commercial activities falling outside the sphere of activities reserved to the State. (41)

78. To what activities does Article 1(3) of Directive 2002/58 apply? In my opinion, the Conseil d'État (Council of State) itself provides a good example when it cites

Articles L. 851-5 and L. 851-6 of the Internal Security Code, referring to 'information collection techniques that are applied directly by the State but do not govern the activities of providers of electronic communications services by imposing specific obligations on them'. (42)

79. I believe that this is the key to determining the scope of the exclusion provided for in Article 1(3) of Directive 2002/58. The provisions of the directive will not apply to *activities* which are intended to safeguard national security and are undertaken by the public authorities themselves, without requiring the cooperation of private individuals and, therefore, without imposing on them obligations in the management of businesses.

80. The range of public authority activities that are exempt from the general regime governing the processing of personal data must, however, be interpreted narrowly. Specifically, the notion of *national security*, which is the sole responsibility of each Member State under Article 4(2) TEU, cannot be extended to other sectors of public life that are, to varying degrees, related to it.

81. As the present references for a preliminary ruling are concerned with the actions of individuals (that is to say, persons who provide electronic communications services to users) and not simply with the intervention of the State authorities, there will be no need to dwell on defining the parameters of national security *stricto sensu*.

82. I believe, however, that guidance can be found in the criterion established in Framework Decision 2006/960/JHA, (43) Article 2(a) of which distinguishes between security services in a broad sense – which include 'a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities' – on the one hand, and 'agencies or units dealing especially with national security issues', on the other. (44)

83. Recital 11 of Directive 2002/58 states that that directive, 'like Directive 95/46 … does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security …'.

84. Indeed, there is continuity between Directive 95/46 and Directive 2002/58 with regard to the competence of Member States over national security. Neither directive is intended to protect fundamental rights in this specific area, in which Member States' activities are not 'governed by [EU] law'.

85. The 'balance' referred to in recital 11 of Directive 2002/58 arises from the need to respect the competence of the Member States over national security matters, where they exercise that competence *directly, using their own resources*. By contrast, where, even for those same reasons of national security, the involvement of individuals, on whom certain obligations are imposed, is required, that circumstance dictates inclusion within an area (namely the protection of privacy required of those private operators) governed by EU law.

86. Both Directive 95/46 and Directive 2002/58 seek to achieve that balance by allowing the rights of private individuals to be restricted by legislative measures adopted by Member States pursuant to Article 13(1) and Article 15(1) respectively of those directives. On this point there is no difference between them.

87. As regards Regulation 2016/679, which establishes a (new) general framework for the

protection of personal data, Article 2(2) thereof rules out the application of that regulation to the 'processing of personal data' where the Member States '[carry] out activities which fall within the scope of Chapter 2 of Title V of the TEU'.

88. Just as, in Directive 95/46, the processing of personal data was classified exclusively by reference to its purpose, irrespective of the person carrying it out, in Regulation 2016/679, the types of processing that are excluded are identified by reference both to their purpose and to their agents: processing carried out by the Member States in the course of an *activity* which falls outside the scope of EU law (Article 2(2)(a) and (b)), and processing carried out by the authorities *for the purposes of combating criminal offences and providing protection* against threats to public security, are excluded. (45)

89. Those public authority activities must necessarily be defined narrowly, so as not to deprive EU privacy law of its effect. Article 23 of Regulation 2016/679 makes provision – in line with Article 15(1) of Directive 2002/58 – for restricting, *by way of a legislative measure*, the rights and obligations established by the regulation, where necessary in order to safeguard, among other objectives, national security, defence or public security. Once again, if the protection of those objectives were sufficient grounds for exemption from the scope of application of Regulation 2016/679, there would be no need to invoke national security as grounds for introducing legislative measures to restrict the rights guaranteed by that regulation.

90. As is the case with Directive 2002/58, it would not be consistent for the legislative measures provided for in Article 23 of Regulation 2016/679 (which, as I have said, authorises the Member States to restrict citizens' rights to privacy on grounds of national security) to fall within the scope of that regulation if, at the same time, the invocation of national security automatically rendered the regulation itself inapplicable and thereby removed the recognition of any subjective rights at all.

B. Endorsement of, and scope for building on, the case-law in Tele2 Sverige and Watson

91. In my Opinion in Case C−520/18, I carry out a detailed analysis (46) of the Court's case-law on this subject and, in conclusion thereto, propose that that case-law should be endorsed, while at the same time suggesting an interpretative approach that would refine its content.

92. I refer to that analysis, which, in the interests of brevity, I do not consider it necessary to reproduce here. The thoughts I shall set out below on the questions referred for a preliminary ruling by the Conseil d'Etat (Council of State) must therefore be read as being premissed on the corresponding sections of the Opinion in Case C−520/18.

C. Answer to the questions referred

1. The obligation to retain data (first question in Cases C−511/18 and C−512/18 and second question in Case C−512/18)

93. As regards the obligation to retain data that is imposed on providers of electronic communications services, the referring court wishes to ascertain, in particular:

– Whether that obligation, enforceable under Article 15(1) of Directive 2002/58, constitutes an interference justified by the 'right to security' guaranteed in Article 6 of the Charter and by requirements of national security (first question in Cases C−511/18 and C−512/18, and third question in C−511/18).

– Whether Directive 2000/31 permits the retention of data that can be used to identify persons who have assisted in the creation of content accessible by the public online (second question in Case C−512/18).

(a) Preliminary consideration

94. The Conseil d'État (Council of State) refers to the fundamental rights recognised in Articles 7 (respect for private and family life), 8 (protection of personal data) and 11 (freedom of expression and information) of the Charter. These are, after all, the rights which, according to the Court, may be affected by the obligation to retain traffic data which national authorities impose on providers of electronic communications services. (47)

95. The referring court also refers to the right to security protected by Article 6 of the Charter. Rather than as a right that may be adversely affected, that court cites it as a factor capable of justifying the imposition of that obligation.

96. I agree with the Commission that this reliance on Article 6 may be misplaced. Like the Commission, I am of the view that that provision is to be interpreted as meaning that it is capable of 'imposing on the Union a positive obligation to adopt measures aimed at protecting persons against criminal acts'. (48)

97. The security guaranteed by that article of the Charter is not synonymous with public security. Or, if you will, it has as much to do with it as any other fundamental right, inasmuch as public security is an essential condition for the enjoyment of fundamental rights and freedoms.

98. As the Commission recalls, Article 6 of the Charter corresponds to Article 5 of the European Convention on Human Rights ('the ECHR'), as is made clear in the explanations that accompany the former. It is apparent from reading Article 5 of the ECHR that the 'security' it protects is strictly personal security, in the sense of a guarantee of the right to physical freedom from arbitrary arrest or detention. In short, it is an assurance that nobody can be deprived of his or her liberty save in the cases and in accordance with the requirements and procedures prescribed by law.

99. It is, therefore, *personal security*, concerned with the conditions under which individuals may have their physical freedom restricted, (49) not the *public security* inherent in the existence of the State, which is an essential prerequisite in a developed society for reconciling the exercise of public powers with the enjoyment of individual rights.

100. Some governments, however, ask that more account be taken of the right to security in the latter sense. In actual fact, the Court has not disregarded that right. Indeed, it has made express reference to it in its judgments (50) and opinions. (51) It has never denied the importance of the public-interest objectives of the protection of national security and public order, (52) the fight against international terrorism in order to maintain international peace and security and the fight against serious crime in order to ensure public security, (53) which it has rightly described as being of 'utmost' importance. (54) As it once stated, 'the protection of public security also contributes to the protection of the rights and freedoms of others'. (55)

101. The present references for a preliminary ruling provide an opportunity that could be used to propose in a clearer way that a balance be sought between the right to security, on the one hand, and the right to privacy and the right to the protection of personal data, on the other. This would avoid criticisms that the latter are favoured to the detriment of the former.

102. It is to that balance that recital 11 and Article 15(1) of Directive 2002/58 allude, in my opinion, when they speak of the need for restrictive measures to be necessary and proportionate *within a democratic society*. The right to security, as I have said, is consubstantial with the very existence and survival of a democracy and must for that reason be taken fully into account in the context of an assessment of the proportionality of such measures. In other words, while preserving the principle of the confidentiality of data is of utmost importance in a democratic society, it is also necessary not to underestimate the importance of the security of that society.

103. A background of serious and persistent threats to national security, in particular the terrorist threat, must therefore be taken into account, as the last sentence of paragraph 119 of the judgment in *Tele2 Sverige and Watson* states. A national system may respond proportionately to the nature and intensity of the threats with which the State is faced without necessarily having to respond in exactly the same way as other Member States.

104. I should add, in short, that the foregoing reflections do not rule out the possibility that, in genuinely *exceptional* situations, characterised by an imminent threat or extraordinary risk such as to warrant the official declaration of a state of emergency in a Member State, national legislation may provide for the option, for a limited period of time, of imposing a data retention obligation as extensive and general as is considered necessary. (56)

105. Consequently, the first question in both references for a preliminary ruling should be reformulated in such a way as to ask, rather, whether the interference is justifiable on grounds of national security. The issue, then, would be whether the obligation imposed on operators of electronic communications services is compatible with Article 15(1) of Directive 2002/58.

(b) Assessment

(1) Characterisation of the domestic rules, as they are set out in the two references for a preliminary ruling, in the light of the case-law of the Court

106. According to the orders for reference, the legislation at issue in the originating proceedings imposes an obligation to retain data on:

– operators of electronic communications services, in particular those that provide access to online public communication services; and

– natural or legal persons who, for the purposes of making them available to the public online, store, even free of charge, signals, texts, sounds or images and messages of any kind provided by recipients of those services. (57)

107. Operators must retain for a period of one year starting from the date of recording information that can be used to identify the user, data relating to the communications terminal equipment used, the technical characteristics, date, time and duration of each call, data relating to the supplementary services requested or employed and the providers of those services, as well as data that can be used to identify the recipient of the communication and, in the case of telephony activities, the origin and location of the communication. (58)

108. As regards, in particular, internet access services and storage services, the national legislation appears to require the retention of IP addresses, (59) passwords and, in the case where the user signs up to a contract or payment account, the type of payment made and its reference and the amount, date and time of the transaction. (60)

109. That retention obligation serves to facilitate the investigation, detection and prosecution of criminal offences. (61) Which is to say that, unlike the situation that obtains – as I shall show – in the case of the obligation to *collect* traffic and location data, the duty to *retain* data does not have as its sole objective the prevention of terrorism. (62)

110. As regards the conditions governing *access* to the data retained, it follows from the information contained in the documents before the Court that either these are the same as under the ordinary arrangements (application to the courts) or such access is restricted to officers individually appointed and empowered for that purpose following an authorisation issued by the Prime Minister on the basis of a non-binding report of an independent administrative authority. (63)

111. It is readily apparent, as the Commission has noted, (64) that the data required to be retained by the national rules is largely the same as that examined by the Court in the judgments in *Digital Rights* and *Tele2 Sverige and Watson*. (65) As on those occasions, the data at issue is the subject of a 'general and indiscriminate retention obligation', as the Conseil d'État (Council of State) very frankly points out at the start of the questions it has referred.

112. If that is the case, a question which, ultimately, falls to be assessed by the referring court, it cannot but be concluded that the legislation at issue entails an 'interference … in the fundamental rights enshrined in Articles 7 and 8 of the Charter [that] is very far-reaching and must be considered to be particularly serious'. (66)

113. None of the parties represented has called into question the proposition that legislation of that kind entails an interference with those rights. There is no need to dwell on this point now, not even in order to recall that an infringement of those rights inevitably operates to the detriment of the very foundations of a society aspiring to respect, among other values, the personal privacy enshrined in the Charter.

114. Applying the case-law established in the judgment in *Tele2 Sverige and Watson* and ratified in the judgment in *Ministerio Fiscal* would naturally lead to the conclusion that legislation such as that at issue here 'exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and 52(1) of the Charter'. (67)

115. For, like that analysed in the judgment in *Tele2 Sverige and Watson*, the legislation with which we are concerned here also 'covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data [and] provides for no differentiation, limitation or exception according to the objective pursued'. (68) Consequently, it 'applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences', does not provide for any exception and, 'consequently … applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy'. (69)

116. Thus, also, the contested legislation 'does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime'. (70)

117. The foregoing supports the inference that that legislation 'exceeds the limits of what is

strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and 52(1) of the Charter'. (71)

118. The foregoing was sufficient for the Court to conclude that the national rules in question were not compatible with Article 15(1) of Directive 2002/58, inasmuch as, 'for the purpose of fighting crime, [they provide] for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication'. (72)

119. The question that arises now is whether the Court's case-law on the retention of personal data can be, if not reconsidered, at least refined where the purpose served by the 'general and indiscriminate' retention of data is the fight against terrorism. The first question in Case C−511/18 is specifically formulated 'against a background of serious and persistent threats to national security, and in particular the terrorist threat'.

120. Now, while that is the *factual background* against which the data retention obligation is imposed, the fact is that the *legislative background* to that obligation is not informed by terrorism alone. The scheme for the retention of, and access to, data that is at issue in the proceedings before the Conseil d'État (Council of State) makes that obligation conditional upon pursuit of the aims of investigating, detecting and prosecuting criminal offences in general.

121. In any event, I would recall that, despite the fact that the fight against terrorism was not left out of the arguments advanced in the judgment in *Tele2 Sverige and Watson*, the Court did not feel that that form of crime called for any adaptation of its case-law. (73)

122. I therefore take the view in principle that the question raised by the referring court, although focused on the specific feature of the terrorist threat, should be answered along the same lines as the ruling given by the Court in the judgment in *Tele2 Sverige and Watson*.

123. As I maintained in the Opinion in *Stichting Brein*, 'certainty in the application of the law obliges the court, if not to apply the *stare decisis* in absolute terms, then to take care to follow the decisions it has itself, after mature reflection, previously adopted in relation to a given legal problem'. (74)

(2) Retention of restricted data in the face of threats to State security including terrorism

124. Is it possible, nonetheless, to refine or supplement that case-law in the light of its consequences on the fight against terrorism or the protection of the State against other, similar threats to national security?

125. I have already made the point that retention of personal data entails in itself an interference with the rights guaranteed by Articles 7, 8 and 11 of the Charter. (75) Aside from the fact that the ultimate purpose of such retention is to make it possible to *access* data at a given point in time, be this retrospectively or simultaneously, (76) the retention of data to an extent greater than that which is strictly necessary for the purposes of transmitting a communication or billing for services provided by the supplier is in itself a failure to observe the limits laid down in Articles 5 and 6 of Directive 2002/58.

126. The users of those services (in reality, almost all citizens in the most developed societies) have, or should have, a legitimate expectation that, without their consent, their data will not be retained in an amount greater than that of the data stored in accordance with those provisions.

The exceptions provided for in Article 15(1) of Directive 2002/58 must be read on the basis of that premiss.

127. As I have already explained, in the judgment in *Tele2 Sverige and Watson*, the Court rejected the general and indiscriminate retention of personal data even in the context of the fight against terrorism. (77)

128. In response to the criticisms received, I do not believe that the case-law established in that judgment underestimates the terrorist threat as a particularly serious form of crime the explicit purpose of which is to challenge the authority of the State and destabilise or destroy its institutions. The anti-terrorist fight is, literally, vital to the State and its success and is a public-interest objective which no State based on the rule of law can afford to forego.

129. Virtually all the governments represented in these proceedings, and the Commission, are in agreement that, not to mention the associated technical difficulties, a partial and differentiated retention of personal data would deprive the national intelligence services of the possibility of accessing information essential to the identification of threats to public security and the defence of the State, as well as to the prosecution of the perpetrators of terrorist attacks. (78)

130. In opposition to that assessment, I think it relevant to make the point that the fight against terrorism must not be considered solely from the point of view of how effective it is. Therein lies its difficulty, but also its nobility, when its means and methods are compatible with the requirements of the rule of law, characterised first and foremost by the requirement that power and strength are subject to the limits of the law and, in particular, to a legal order that finds in the defence of fundamental rights the reason and purpose of its existence.

131. While, for terrorists, the justification of their means is assessed by reference only to the pure (and maximum) effectiveness of their attacks on the established order, for a State based on the rule of law, effectiveness is measured in terms that do not tolerate the prospect of dispensing, in the defence of that State, with the procedures and safeguards that define it as a legitimate order. If it simply gave primacy to mere effectiveness, a State based on the rule of law would lose that distinguishing quality and might, in extreme cases, itself become a threat to the citizen. If the public authorities were armed with a panoply of instruments of criminal prosecution such as to enable them to disregard or violate fundamental rights, there would be no way of ensuring that their uncontrolled and entirely unfettered actions would not operate ultimately to the detriment of everyone's freedom.

132. The effectiveness of public authority, as I have said, is met with an insurmountable barrier in the form of the fundamental rights of citizens, any limitations on which, as Article 52(1) of the Charter stipulates, may be provided for only by law and with due respect for the essence of those rights, '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'. (79)

133. On the conditions under which a *selective* retention of data would be permissible, in accordance with the judgment in *Tele2 Sverige and Watson*, I refer to my Opinion in Case C−520/18. (80)

134. Circumstances in which information available to the security services supports the well-founded suspicion of the preparation of a terrorist attack may constitute a legitimate scenario for the imposition of the obligation to retain certain data. The actual commission of an attack may make for an even more compelling scenario. While, in the latter case, the perpetration of

the offence may in itself be a circumstance justifying the adoption of that measure, in the case of a mere suspicion of a possible attack, the circumstances warranting that suspicion would have to exhibit a minimum degree of plausibility, as, without this, the evidence that might justify the adoption of that measure could not be objectively assessed.

135. While it is difficult, it is not impossible to determine precisely and on the basis of objective criteria the categories of data that it is deemed essential to retain, and the circle of persons who are affected. It is true that the most *practical and effective* option would involve the general and indiscriminate retention of any data that might be collected by the providers of electronic communications services, but, as I have already said, the issue cannot be settled by reference to what is *practically effective*; resolving the issue is not a matter of *practical effectiveness* but of *legal effectiveness* within the framework of the rule of law.

136. The task of determining these questions is inherently a matter for legislation, within the limits set by the case-law of the Court. I refer once again to my submissions in this regard in my Opinion in Case C−520/18. (81)

(3) Access to retained data

137. Starting from the premiss that the operators have collected the data in a manner that complies with the provisions of Directive 2002/58 and that it has been retained in accordance with Article 15(1) of the directive, (82) access to that information by the competent authorities must take place in accordance with the requirements that have been laid down by the Court, which I examine in the Opinion in Case C−520/18, to which I refer. (83)

138. Therefore, in this situation too, the national legislation must establish the substantive and procedural requirements governing access by the competent authorities to the retained data. (84) In the context of these references for a preliminary ruling, those requirements would allow access to the data of persons suspected of planning, of being about to commit, of having committed, or of being involved in, an act of terrorism. (85)

139. In any event, the fundamental point is that, other than in duly substantiated cases of urgency, access to the data in question must be subject to prior review by a court or an independent administrative authority whose decision should be made in response to a reasoned request by the competent authorities.(86) In this way, where a question cannot be judged in abstract by the law, there is a guarantee that it will be judged on its specific terms by that independent authority, which is committed both to safeguarding national security and to defending citizens' fundamental rights.

(4) Obligation to retain data that can be used to identify the authors of content, viewed in the light of Directive 2000/31 (second question referred in Case C−512/18)

140. The referring court mentions Directive 2000/31 as a point of reference for determining whether certain persons (87) and operators offering public communication services can be compelled to retain data 'that is capable of being used to identify someone who has assisted in the creation of all or some of the content of the services which those persons or operators provide, so as to enable the judicial authority, where appropriate, to require that the data in question be communicated for the purposes of compliance with the rules on civil or criminal liability'.

141. I agree with the Commission that it would be inappropriate to examine the compatibility of that obligation with Directive 2000/31, (88) given that Article 1(5)(b) of that directive

excludes from its scope ‘questions relating to information society services covered by [Directive 95/46 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24, p. 1)]’, which provisions now correspond to Regulation 2006/679 and Directive 2002/58, (89) Articles 23(1) and 15(1), respectively, of which must, in my opinion, be interpreted in the manner indicated previously.

2. The obligation to collect traffic and location data in real time (second question in Case C-511/18)

142. In the view of the referring court, Article L. 851-2 of the Internal Security Code authorises, solely for the purposes of preventing terrorism, the real-time collection of information concerning persons previously identified as being suspected of having links to a terrorist threat. In the same way, Article L. 851-4 of that code allows operators to transmit technical data relating to the location of terminal equipment in real time.

143. According to the referring court, those techniques do not impose on suppliers a retention obligation additional to that required for the purposes of billing for or marketing their services.

144. Furthermore, Article L. 851-3 of the Internal Security Code provides that electronic communications operators and providers of technical services may be compelled to ‘apply on their networks automated data-processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat’. That technique does not involve the general and indiscriminate retention of data but has as its purpose to collect, for a limited period, any connection data that might be related to an offence of a terrorist nature.

145. In my opinion, the conditions governing access to retained personal data must also be applied to real-time access to data generated in the course of electronic communications. I refer, therefore, to my submissions in relation to the former. It makes no difference whether the data in question are retained or obtained instantly, since both scenarios involve the disclosure of personal data, be those data historical or current.

146. In particular, if real-time access is the consequence of links detected by way of an automated processing measure such as that provided for in Article L. 851-3 of the Internal Security Code, the scenarios and criteria pre-established for such processing must be specific, reliable and non-discriminatory, so as to facilitate the identification of individuals who may reasonably be suspected of involvement in terrorist activities. (90)

3. The obligation to inform the persons concerned (third question in Case C-511/18)

147. The Court has held that the authorities to which access to the data has been granted must inform the persons concerned to that effect, provided that this does not jeopardise the investigations under way. The reason for that duty lies in the fact that that information is necessary to enable those persons to exercise their right to an effective legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, where their rights have been infringed. (91)

148. By its third question in Case C-511/18, the Conseil d’État (Council of State) wishes to ascertain whether that requirement to inform is mandatory in all cases or whether it can be dispensed with where other guarantees such as those which it describes in its order for reference have been provided for.

149. According to the explanation provided by the referring court, (92) those guarantees take

the form of the option available to persons wishing to establish whether an information-gathering technique has been applied illegally to apply to the Conseil d'État (Council of State) itself. That body can, if appropriate, go so far as to cancel the authorisation given for the measure and order the destruction of the material collected, as part of a procedure that is not subject to the *audi alteram partem* principle usually applicable in judicial proceedings.

150. The referring court considers that that legislation does not infringe the right to an effective legal remedy. It is my view, however, that, while this might well be true, in theory, in the case of persons who decide to find out whether they are the subject of an intelligence operation, that right is *not* respected if persons who are or have been the subject of such an operation are not alerted to that fact and, for that reason, are not even in a position to raise the question of whether or not their rights have been breached.

151. The judicial guarantees mentioned by the referring court seem to be conditional on the initiative of the person who suspects that information is being collected about him or her. However, access to the courts for the purposes of defending one's rights must be effectively available to everyone, which means that anyone whose personal data have been processed must have the possibility of challenging the legality of such processing before the courts, and must therefore be notified of the existence of that processing.

152. It is true that, according to the information provided, legal proceedings may be instituted either *ex officio* or on the basis of an administrative complaint. In any event, however, the person concerned must be given the opportunity to bring such proceedings him or herself and must, to that end, be made aware that his or her personal data have been the subject of some processing. The defence of his or her rights cannot be entrusted to the contingency that he or she will find out about the processing of his or her data from third parties or by his or her own means.

153. Consequently, in so far as the course of the investigations for the purposes of which access to the retained data has been granted is not jeopardised, such access must be notified to the person concerned.

154. Whether, once the person concerned has taken legal action after having been made aware that his or her data have been accessed, the court proceedings that follow meet the requirements of confidentiality and discretion inherent in any review of action taken by the public authorities in areas as sensitive as State security and defence, is a different matter. This, however, is a question that falls outside the scope of these references and it is not therefore appropriate, in my opinion, for the Court to give a ruling in that regard.

V. Conclusion

155. In the light of the foregoing, I propose that the Court's answer to the Conseil d'État (Council of State, France) should be as follows:

'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), read in conjunction with Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as:

(1) Precluding national legislation which, against a background of serious and persistent threats to national security, in particular the terrorist threat, imposes on operators and

providers of electronic communications services the obligation to retain, in a general and indiscriminate fashion, the traffic and location data of all subscribers, as well as data that can be used to identify the creators of the content offered by the providers of those services.

(2) Precluding national legislation that does not lay down an obligation to inform the persons concerned about the processing of their personal data by the competent authorities, unless such notification jeopardises the actions of those authorities.

(3) Not precluding national legislation which permits the real-time collection of traffic and location data on individuals, in so far as those activities are carried out in accordance with established procedures for accessing legitimately retained personal data and carry the same guarantees.'

---

1 Original language: Spanish.

---

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

---

3 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).

---

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

---

5 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).

---

6 Case C−207/16, EU:C:2018:788; 'the judgment in *Ministerio Fiscal*'.

---

7 In addition to these two (Cases C−511/18 and C−512/18), Cases C−623/17, *Privacy International*, and C−520/18, *Ordre des barreaux francophones et germanophone and Others*.

---

8 *Privacy International*, C−623/17.

---

9 *Ordre des barreaux francophones et germanophone and Others*, C−520/18.

---

10 *La Quadrature du Net and Others*, C−511/18 and C−512/18.

---

11 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).

---

12 Directive of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).

---

13 Regulation 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 2016 L 119, p. 1).

---

14 According to the referring court, these techniques do not impose on service providers an obligation to store information and documentation additional to that required for the purposes of billing or marketing their services or for the purposes of providing added-value services.

---

15 According to the referring court, this technique, which does not involve general and indiscriminate retention, is intended only to facilitate the collection, for a limited period and from all of the collection data processed by those persons, such data as might be related to a serious offence of this kind.

---

16 Those data were defined by Décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decree No 2011-219 of 25 February 2011 on the retention and communication of data that can be used to identify any person having assisted in the creation of content posted online). Prominent among the provisions of that decree are: (a) Article 1(1), according to which persons providing access to online communication services must retain the following data: the connection identifier, the identifier assigned to the subscriber, the identifier of the terminal used for the connection, the date and time of the start and end of the connection and the characteristics of the subscriber's line; (b) Article 1(2), which provides that persons who, for the purposes of making them available to the public via online public communication services, store, even free of charge, signals, texts, images, sounds or messages of any nature provided by recipients of those services must retain, in connection with each operation, the following data: the identifier of the connection giving rise to the communication, the identifier assigned to the content forming the subject of the operation, the types of protocols used to connect to the service and transfer the content, the nature of the operation, the date and time of the operation and the identifier used by the author of the operation; and, finally, (c) Article 1(3), which provides that the persons referred to in the preceding two paragraphs must retain the following information provided by a user when signing up to a contract or creating an account: the identifier of the connection at the time when the account was created; the first name and surname or business name; the associated postal addresses, the pseudonyms used, the associated email or account addresses, the telephone numbers, the updated password and the data for verifying or changing it.

---

17 The contested decrees were as follows: (a) Décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Decree No 2015-1185 of 28 September 2015 designating specialist intelligence services); (b) Décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement

soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decree No 2015−1211 of 1 October 2015 on litigation relating to the implementation of intelligence techniques subject to authorisation and files on matters of State security); (c) Décret n.º 2015−1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (Decree No 2015−1639 of 11 December 2015 on the designation of services other than the specialist intelligence services which are authorised to use the techniques referred to in Title VIII of the Internal Security Code); and (d) Décret n.º 2016−67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Decree No 2016−67 of 29 January 2016 on intelligence gathering techniques).

---

18 'A background of serious and persistent threats to national security, and in particular the terrorist threat', as the first question in Case C−511/18 describes it.

---

19 Cases C−317/04 and C−318/04, EU:C:2006:346; 'the judgment in *Parliament* v *Council and Commission*'.

---

20 Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, p. 83, and corrigendum in OJ 2005 L 255, p. 168) (Case C−317/04).

---

21 Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (OJ 2004 L 235, p. 11) (Case C−318/04).

---

22 The judgment in *Parliament* v *Council and Commission*, paragraph 57. In paragraph 58, it is pointed up that the fact that 'the … data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country' does not mean that that transfer does not constitute one of the cases of non-application of Directive 95/46 that are listed in Article 3(2), first indent, of that directive, since 'the transfer falls within a framework established by the public authorities that relates to public security'.

---

23 A point that would later be made by the much-missed Advocate General Bot in his Opinion in *Ireland* v *Parliament and Council* (C−301/06, EU:C:2008:558). He stated that the judgment in *Parliament* v *Council and Commission* 'does not mean that only the examination of the objective pursued by the processing of personal data is relevant for the purpose of including or excluding such processing from the scope of the system of data protection instituted by Directive 95/46. It is also necessary to ascertain in the course of which type of activity data processing is carried out. It is only where it is undertaken in course of activities specific to States or to State authorities and unrelated to the fields of activity of individuals that it is excluded from the Community system of personal data protection arising from Directive 95/46 pursuant to the first indent of Article 3(2) thereof' (point 122).

---

24 The judgment in *Parliament* v *Council and Commission*, paragraph 58. The principal purpose of the agreement was to require airlines operating passenger transport services between the EU and the United States to make it easier for the US authorities to gain electronic access to the PNR data related to numbers of passenger contained in their computerised reservation and departure control systems. It thus established a form of international cooperation between the EU and the United States in the fight against terrorism and other serious crimes and sought to reconcile that objective with the objective of protecting passengers' personal data. In that context, the obligation imposed on airlines was not very different from a direct exchange of data between public authorities.

---

25 Opinion of Advocate General Bot in *Ireland* v *Parliament and Council* (C−301/06, EU:C:2008:558, point 127).

---

26 The judgment in *Tele2 Sverige and Watson*, paragraph 67.

---

27 *Ibidem*, paragraph 72.

---

28 *Ibidem*, paragraph 73.

---

29 *Ibidem*, paragraph 74.

---

30 *Ibidem*, paragraph 75.

---

31 *Ibidem*, paragraph 76.

---

32 Paragraphs 15 and 16 of Ireland's written observations.

---

33 Paragraphs 34 to 50 of the French Government's written observations.

---

34 Judgment in *Tele2 Sverige and Watson*, paragraphs 103 and 119.

---

35 My emphasis.

---

36 My emphasis.

---

37 The judgment in *Parliament* v *Council and Commission*, paragraph 58.

---

38 The judgment in *Ministerio Fiscal*, paragraph 32. To the same effect, the judgment in *Tele2 Sverige and Watson*, paragraph 72.

---

39 It would, after all, be difficult to argue that Article 15(1) of Directive 2002/58 allows the Member States to limit the rights and obligations for which it provides in a context, such as national security, which would in principle fall outside its scope, pursuant to Article 1(3) of that directive. As the Court held in the judgment in *Tele2 Sverige and Watson*, paragraph 73, Article 15(1) of Directive 2002/58 'necessarily presupposes that the national measures referred to therein … fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met'.

---

40 The judgment in *Tele2 Sverige and Watson*, paragraph 67.

---

41 As Advocate General Saugmandsgaard Øe noted in his Opinion in *Ministerio Fiscal* (C−207/16, EU:C:2018:300, point 47), 'the personal data processed *directly* in the context of the activities – of a sovereign nature – of the State in a field governed by criminal law must not be confused with the data processed in the context of the activities – of a commercial nature – of an electronic communications service provider which are *then* used by the competent State authorities'.

---

42 Paragraphs 18 and 21 of the order for reference in Case C−511/18.

---

43 Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ 2006 L 386, p. 89).

---

44 By the same token, Article 1(4) of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350, p. 60) provided that that decision 'is without prejudice to essential national security interests and specific intelligence activities in the field of national security'.

---

45 Regulation 2016/679 thus excludes the processing of personal data by the Member States in the course of an *activity* which falls outside the scope of Union law, as well as processing carried out by the authorities *for the purposes of protecting* public security.

---

46 Points 27 to 68.

---

47 See, to this effect, the judgment in *Tele2 Sverige and Watson*, paragraph 92, which cites, by analogy, the judgment in *Digital Rights*, paragraphs 25 and 70.

---

48 Paragraph 37 of the Commission's written observations.

---

49 This is the interpretation adopted by the European Court of Human Rights. See, inter alia, judgment of 5 July 2016, *Buzadji v. The Republic of Moldova*, ECHR:2016:0705JUD002375507, § 84 of which states that the key purpose of Article 5 of the ECHR is to prevent the arbitrary or unjustified deprivation of an individual's liberty.

50 The judgment in *Digital Rights*, paragraph 42.

51 Agreement 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592; 'Opinion 1/15'; paragraph 149 and the case-law cited).

52 Judgment of 15 February 2016, *N.* (C−601/15 PPU, EU:C:2016:84, paragraph 53).

53 The judgment in *Digital Rights*, paragraph 42 and the case-law cited.

54 *Ibidem*, paragraph 51.

55 Opinion 1/15, paragraph 149.

56 See points 105 to 107 of my Opinion in Case C−520/18.

57 This follows from Article L. 851−1 of the Internal Security Code, which refers to Article L. 34−1 of the Post and Electronic Communications Code and Article 6 of Law No 2004−575 to promote trust in the digital economy.

58 This comes from Article R. 10−13 of the Post and Electronic Communications Code.

59 It is for the referring court to clarify this point, over which there was disagreement at the hearing.

60 Article 1 of Decree No 2011−219.

61 Article R. 10−13 of the Post and Electronic Telecommunications Code.

62 Both La Quadrature du Net and the Fédération des fournisseurs d'accès à Internet associatifs emphasise the breadth of the purposes served by retention, the discretion conferred on the authorities, the fact that that discretion is not defined by any objective criteria and the significance attached to forms of crime that cannot be classified as serious.

63 The Commission nationale de contrôle des techniques de renseignement (National Commission for the Oversight of Intelligence Techniques). See, in this regard, paragraphs 145 to 148 of the French Government's observations.

64 Paragraph 60 of the Commission's observations.

65 In actual fact, this case concerns a slightly more extensive range of data, since there appears to be provision, so far as internet-access services are concerned, for IP addresses and passwords to be retained.

66 The judgment in *Tele2 Sverige and Watson*, paragraph 100.

67 *Ibidem*, paragraph 107.

68 *Ibidem*, paragraph 105.

69 *Loc. ult. cit.*

70 The judgment in *Tele2 Sverige and Watson*, paragraph 106.

71 *Ibidem*, paragraph 107.

72 *Ibidem*, paragraph 112.

73 *Ibidem*, paragraph 103.

74 Case C−527/15, EU:C:2016:938, point 41.

75 As the Court recalled in Opinion 1/15, paragraph 124, 'the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference'.

76 As Advocate General Cruz Villalón noted in the Opinion in Joined Cases *Digital Rights Ireland and Others* (C−293/12 and C−594/12, EU:C:2013:845, point 72), 'the collection and, above all, the retention, in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period'.

77 The judgment in *Tele2 Sverige and Watson*, paragraph 103: 'cannot … justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight'.

---

78 This was the view, for example, of the French Government, which illustrates the above assertion with specific examples of the usefulness of the general retention of data, which has enabled France to respond to the serious terrorist attacks suffered by that country in recent years (paragraphs 107 and 122 to 126 of the French Government's observations).

---

79 Judgment of 15 February 2016, *N.* (C−601/15 PPU, EU:C:2016:84, paragraph 50). This, then, is the difficult balance between public order and freedom to which I have already referred and to which any EU legislation in principle aspires. An example is Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ 2017 L 88, p. 6). At the same time as it provides in Article 20(1) that Member States must ensure that those responsible for investigating or prosecuting terrorist offences have 'effective investigative tools', recital 21 thereof states that the use of those effective tools 'should be targeted and take into account the principle of proportionality and the nature and seriousness of the offences under investigation and should respect the right to the protection of personal data'.

---

80 Paragraphs 87 to 95.

---

81 Points 100 to 107.

---

82 Provided that the conditions mentioned in paragraph 122 of the judgment in *Tele2 Sverige and Watson* are observed: the Court held that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and (1a) of that directive, which requires providers to take measures to ensure the effective protection of retained data against risks of misuse and against unlawful access. By the same token, it held that, 'given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period'.

---

83 Points 52 to 60.

---

84 The judgment in *Tele2 Sverige and Watson*, paragraph 118.

---

85 *Ibidem*, paragraph 119.

---

86 *Ibidem*, paragraph 120.

---

87 Those that, ‘for the purposes of making them available to the public via online public communication services, store signals, texts, images, sounds or messages of any kind that are provided by recipients of those services …’.

---

88 That directive is mentioned by the referring court, in general terms and without mention of any particular provision, in the second question in Case C−512/18.

---

89 Paragraphs 112 and 113 of the Commission’s written observations.

---

90 The judgment in *Digital Rights*, paragraph 59.

---

91 The judgment in *Tele2 Sverige and Watson*, paragraph 121.

---

92 Paragraphs 8 to 11 of the order for reference.