Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 15 January 2020 [1]

Case C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
v
Conseil des ministres,
intervener:
Child Focus

(Request for a preliminary ruling
from the Cour constitutionnelle (Constitutional Court, Belgium)

(Reference for a preliminary ruling – Processing of personal data and protection of privacy in the electronic communications sector – Directive 2002/58/EC – Scope – Article 1(3) – Article 15(1) – Article 4(2) TEU – Charter of Fundamental Rights of the European Union – Articles 4, 6, 7, 8 and 11 and Article 52(1) – Obligation to retain traffic and location data on a general and indiscriminate basis – Effectiveness of the criminal investigations and other objectives in the public interest)

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.

1 Original language: Spanish.

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

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).

– 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 For that reason, some of those States are calling for that case-law to be repealed or refined.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 (United Kingdom,[8] Belgian[9] and French[10]) legislation in this field are compliant with EU law as it has been interpreted by the Court.

5. Upon delivery of the judgment in *Digital Rights*, the Cour constitutionnelle (Constitutional Court, Belgium) annulled the national legislation which had partially transposed into national law Directive 2006/24, declared invalid in that judgment. The Belgian legislature then adopted new rules the compatibility of which with EU Law has in turn been called into question in the light of the judgment in *Tele2 Sverige and Watson*.

6. A particular feature of this reference is that it raises the possibility of temporarily deferring the effects of national legislation which the national courts are bound to annul on account of its incompatibility with EU law.

I. Legislative framework

A. EU law

7. I refer to the relevant section of my Opinion in Joined Cases C-511/18 and C-512/18.

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

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, 'the judgment in *Ministerio Fiscal*', EU:C:2018:788.

7 That is to say, in addition to this case (Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*), Cases C-511/18 and C-512/18, *La Quadrature du Net and Others*, and Case C-623/17, *Privacy International*.

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.

B. National law. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. Article 4 provides that Article 126 de la loi du 13 juin 2005 relative aux communications électroniques [12] is to be worded as follows:

'1. Without prejudice to the Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Law of 8 December 1992 on the protection of privacy with respect to the processing of personal data), providers to the public of telephony services, including via the internet, internet access and internet-based email, operators providing public electronic communications networks and operators providing any of those services shall retain the data referred to in paragraph 3 where those data are generated or processed by them in the course of providing the communications services concerned.

This article shall not concern the content of communications.

…

2. Data retained under this article may be obtained, by simple request, from the providers and operators referred to in the first subparagraph of paragraph 1, for the purposes and under the conditions listed below, only by the following authorities:

1. judicial authorities, with a view to the investigation, detection and prosecution of offences, in order to execute the measures referred to in Articles 46*bis* and 88*bis* of the Code d'instruction criminelle (Code of Criminal Procedure) and under the conditions laid down in those articles;

2. under the conditions laid down in this law, intelligence and security services, in order to carry out intelligence missions employing the data-gathering methods referred to in Articles 16/2, 18/7 and 18/8 of the Loi du 30 novembre 1998 organique des services de renseignement et de sécurité; [13]

3. any judicial police officer attached to the Institut [belge des services postaux et des télécommunications (Belgian Institute for Postal Services and Telecommunications)], with a view to the investigation, detection and prosecution of offences contrary to [the rules on network security] and this article;

4. emergency services providing on-site assistance, in the case where, after having received an emergency call, they cannot obtain from the provider or operator concerned the data identifying the person having made the emergency call … or obtain incomplete or incorrect data. Only the data identifying the caller may be requested and the request must be made no later than 24 hours after the call;

11 Law of 29 May 2016 on the collection and retention of data in the electronic telecommunications sector; 'the Law of 29 May 2016' (Moniteur belge of 18 July 2016, p. 44717).

12 Law of 13 June 2005 on electronic communications; 'the 2005 Law' (*Moniteur belge* of 20 June 2005, p. 28070).

13 Basic Law of 30 November 1998 on the intelligence and security services; 'the 1998 Law' (*Moniteur belge* of 18 December 1998, p. 40312).

5. any judicial police officer attached to the Missing Persons Unit of the Federal Police, in the course of his or her task of providing assistance to persons in danger, searching for persons whose disappearance is a cause for concern and in cases where there are serious presumptions or indications that the physical integrity of the missing person is in imminent danger. Only the data referred to in the first and second subparagraphs of paragraph 3, relating to the missing person, and retained during the 48 hours prior to the data request, may be requested from the operator or provider concerned via a police service designated by the King;

6. the Telecommunications Ombudsman, with a view to identifying a person who has misused an electronic communications network or service … Only the identification data may be requested.

The providers and operators referred to in the first subparagraph of paragraph 1 shall ensure that the data referred to in paragraph 3 are accessible without restriction from Belgium and that those data and any other necessary information concerning those data may be transmitted without delay and only to the authorities referred to in this paragraph.

Without prejudice to other legal provisions, the providers and operators referred to in the first subparagraph of paragraph 1 may not use the data retained under paragraph 3 for any other purposes.

3. Data that can be used to identify the user or subscriber and the means of communication, other than the data specifically provided for in the second and third subparagraphs, shall be retained for 12 months as from the date on which communication was last able to be made using the service employed.

Data relating to the terminal devices' access and connection to the network and the service, and to the location of those devices, including the network termination point, shall be retained for 12 months as from the date of the communication.

Communication data other than content, including the origin and destination thereof, shall be retained for 12 months as from the date of the communication.

The King shall, by decree deliberated in the Council of Ministers and on a proposal from the Minister for Justice and the Minister, and after obtaining the opinion of the Committee for the Protection of Privacy and the Institute, determine the data to be retained by category type as referred to in the first to third subparagraphs and the requirements which those data must satisfy.

4. For the purposes of retention of the data referred to in paragraph 3, the providers and operators referred to in the first subparagraph of paragraph 1 shall:

1. ensure that the retained data are of the same quality and are subject to the same security and protection requirements as data on the network;

2. ensure that the retained data are the subject of appropriate technical and organisational measures to protect them against accidental or unlawful destruction, loss or accidental alteration, or unauthorised or unlawful storage, processing, access or disclosure;

3. ensure that access to data retained in response to requests by the authorities referred to in paragraph 2 is granted only by one or more members of the Coordination Unit referred to in Article 126/1(1);

4. retain data in the territory of the European Union;

5. implement technological protection measures that render the data retained, upon being recorded, illegible and incapable of being used by any person not authorised to have access to them;

6. delete the retained data from any medium on expiry of the retention period applicable to those data which is laid down in paragraph 3, without prejudice to Articles 122 and 123;

7. ensure that the use of data retained in response to each data request made by an authority referred to in paragraph 2 is traceable.

The traceability referred to in point 7 shall be achieved by means of a log. The Institute and the Committee for the Protection of Privacy may consult that log or demand a copy of all or part of that log. The Institute and the Committee for the Protection of Privacy shall conclude a collaboration agreement on consultation and supervision of the content of the log.

5. The Minister and the Minister for Justice shall ensure that statistics on the retention of data generated or processed in the course of the provision of communications services or networks accessible to the public are forwarded annually to the Chamber of Representatives.

Those statistics shall include in particular:

1. cases in which data have been forwarded to the competent authorities in accordance with the applicable statutory provisions;

2. the time lag between the date from which the data were retained and the date on which the competent authorities asked for those data to be forwarded;

3. cases in which requests for data could not be met.

Those statistics cannot include personal data.

…'

9. Article 5 provides for the insertion into the 2005 Law of an Article 126/1, worded as follows:

'1. Within each operator, and within each provider referred to in the first subparagraph of Article 126(1), a Coordination Unit shall be set up which shall be responsible for providing the legally authorised Belgian authorities, at their request, with data retained under Articles 122, 123 and 126, caller identification data under the first subparagraph of Article 107(2) or data that may be required under Articles 46*bis*, 88*bis* and 90*ter* of the Code of Criminal Procedure and Articles 18/7, 18/8, 18/16 and 18/17 of [the 1998 Law].

…

2. Each operator and provider referred to in the first subparagraph of Article 126(1) shall establish an internal procedure for responding to requests from the authorities for access to personal data concerning users. It shall, on request, make available to the Institute information about those procedures, the number of requests received, the legal basis relied on and the response given.

…

3. Each operator and each provider referred to in Article 126(1) shall appoint one or more personal data protection officers, who shall meet the cumulative conditions listed in the third subparagraph of paragraph 1.

…

In carrying out his or her tasks, the personal data protection officer shall act on a fully independent basis and shall have access to all personal data forwarded to the authorities and to all relevant premises of the provider or operator.

…

4. The King shall, by decree deliberated in the Council of Ministers and after obtaining the opinion of the Committee for the Protection of Privacy and the Institute, determine:

…

2. the requirements which the Coordination Unit must satisfy, account being taken of the situation of operators and providers that receive few requests from the judicial authorities, have no establishment in Belgium or operate principally from outside Belgium;

3. the information to be provided to the Institute and the Committee for the Protection of Privacy in accordance with paragraphs 1 and 3 and the authorities that are to have access to that information;

4. the other rules governing collaboration by the operators and providers referred to in the first subparagraph of Article 126(1) with all or some of the Belgian authorities in providing the data referred to in paragraph 1, including, if necessary and for each authority concerned, the form and content of the request.

…’

10. Article 8 provides that Article 46*bis*(1) of the Code of Criminal Procedure is to be worded as follows:

‘1. In the investigation of serious and less serious offences, the Crown Prosecutor may, by reasoned written decision, requesting, if necessary, the assistance of an operator of an electronic communications network, a provider of an electronic communications service or a police service

designated by the King, and on the basis of all of the information available to him or her or obtained by accessing the customer files of operators or service providers, adopt, or arrange for the adoption of, the following measures:

1. identify the subscriber or habitual user of one of the electronic communications services or of the means of electronic communication used;

2. identify the electronic communications services to which a specific person subscribes or habitually uses.

The reasons given [for the decision] shall reflect the fact that the measure is proportionate from the point of view of respect for privacy, and subsidiary to any other investigative obligation.

In cases of extreme urgency, a judicial police officer may, with the prior verbal consent of the Crown Prosecutor and by reasoned written decision, require that that data be provided to him or her. The judicial police officer shall forward that reasoned written decision and the information gathered to the Crown Prosecutor within 24 hours, and shall give reasons for the extreme urgency.

In the case of offences not punishable by a custodial sentence of one year or a more severe penalty, the Crown Prosecutor, or, in extremely urgent cases, the judicial police officer, may request the data referred to in the first paragraph only in respect of the six months prior to his or her decision.

2. All operators of an electronic communications network and all providers of electronic communications services required to furnish the data referred to in the first paragraph shall supply the data requested to the Crown Prosecutor or the judicial police officer within a period to be determined by the King …

…

Anyone who, in the performance of his or her duties, becomes aware of, or assists with, the measure shall maintain its confidentiality. Any breach of that confidentiality shall be punishable in accordance with Article 458 of the Criminal Code.

A refusal to provide data shall be punishable by a fine of between EUR 26 and EUR 10 000.'

11. Article 9 prescribes the following wording for Article 88*bis* of the Code of Criminal Procedure:

'1. Where there are strong indications that the offences are such as to be punishable by a custodial sentence of one year or a more severe penalty, and where the investigating judge considers that there are circumstances that make it necessary to track electronic communications or locate the origin or destination of electronic communications in order to establish the truth, he or she may adopt or arrange for the adoption of the following measures, requesting, if necessary, either directly or via a police service designated by the King, the technical assistance of the operator of an electronic communications network or the provider of an electronic communications service:

1. tracking the data traffic of means of electronic communication from which or to which electronic communications are or were addressed;

2. locating the origin or destination of electronic communications.

In the cases referred to in the first subparagraph, for each means of communication the data of which are tracked or the origin or destination of which is located, the day, hour, duration and, if necessary, place of the electronic communication shall be indicated and recorded in a report.

The investigating judge shall state the factual circumstances of the case that warrant the measure, and that it is proportionate from the point of view of respect for privacy and is subsidiary to any other investigative obligation, in a reasoned order.

He or she shall also specify the period during which the measure may be applied prospectively, which may not exceed two months from the date of the order, without prejudice to renewal, and, where appropriate, the period over which the order extends retrospectively in accordance with paragraph 2.

…

2. As regards the application of the measure referred to in the first subparagraph of paragraph 1, the following provisions shall apply to traffic or location data retained on the basis of Article 126 of the [2005] Law …:

– for offences referred to in Book II, Title I*ter*, of the Criminal Code, the investigating judge may, in his or her order, request data in respect of a period of 12 months prior to the order;

– for other offences referred to in Article 90*ter*(2) to (4) which are not mentioned in the first indent, or for offences committed in the context of a criminal organisation as referred to in Article 324*bis* of the Criminal Code, or for offences punishable by a custodial sentence of five years or a more severe penalty, the investigating judge may, in his or her order, request data in respect of a period of nine months prior to the order;

– for other offences, the investigating judge may request data only in respect of a period of six months prior to the order.

3. The measure may relate to the means of electronic communication of a lawyer or a doctor only if the lawyer or doctor is himself or herself suspected of having committed or participated in an offence referred to in paragraph 1, or if specific facts suggest that third parties suspected of having committed an offence referred to in paragraph 1 have used his or her means of electronic communication.

The measure may not be executed unless the Chair of the Bar Association or the representative of the Provincial Medical Association, as the case may be, is made aware of it. Those persons shall be informed by the investigating judge of the matters which the latter regards as being covered by professional privilege. Those matters shall not be recorded in the report.

4. …

Anyone who, in the performance of his or her duties, becomes aware of, or assists with, the measure shall maintain its confidentiality. Any breach of that confidentiality shall be punishable in accordance with Article 458 of the Criminal Code.

…’

12. In accordance with Article 12, Article 13 of the 1998 Law is to be worded as follows:

‘The intelligence and security services may seek, collect, receive and process information and personal data that may be useful to them in carrying out their tasks, and keep up to date documents relating to particular events, groups and persons of interest to the performance of their tasks.

The information contained in the documents must be linked to the purpose of the case and be confined to the requirements of that case.

The intelligence and security services shall ensure that data relating to their sources and the information and personal data supplied by those sources are kept secure.

Agents of the intelligence and security services shall have access to the information, intelligence and personal data gathered and processed by their service, provided that those data are useful to the performance of their duties or tasks.’

13. Article 14 prescribes a new form of words for Article 18/3 which now provides:

‘1. The specific data-gathering methods referred to in Article 18/2(1) may be implemented in the light of the potential threat referred to in Article 18/1 if the ordinary data-gathering methods are deemed insufficient to enable the information necessary for the completion of an intelligence mission to be gathered. The specific method must be chosen according to the degree of gravity of the potential threat in relation to which it is employed.

The specific method may not be implemented until the director of the service has issued a written reasoned decision and that decision has been notified to the Committee.

2. The decision of the director of the service shall state:

1. the nature of the specific method;

2. as appropriate, the natural or legal persons, associations or groups, items, places, events or information subject to the specific method;

3. the potential threat that warrants use of the specific method;

4. the factual circumstances that warrant use of the specific method, the reasons in relation to subsidiarity and proportionality, including the link between points 2 and 3;

5. the period during which the specific method may be applied as from notification of the decision to the Committee;

…

9. where applicable, the strong indications that the lawyer, doctor or journalist is participating or has participated personally and actively in the instigation or development of the potential threat;

10. where Article 18/8 is applied, the reasons for the length of the period over which the data is to be collected;

…

8. The director of the service shall terminate the specific method when the potential threat warranting it has ceased to exist, when the method is no longer of use for the purpose for which it had been implemented, or when he or she has found it to be unlawful. He or she shall inform the Committee of his or her decision as soon as possible.'

14. Article 18/8 of the 1998 Law reads as follows:

'1. The intelligence and security services may, in the interests of performing their missions, requesting to that end, if necessary, the technical assistance of the operator of an electronic communications network or the provider of an electronic communications service, adopt or arrange for the adoption of, the following measures:

1. tracking the traffic data of means of electronic communication from which or to which electronic communications are or were addressed;

2. locating the origin or destination of electronic communications.

…

2. As regards the application of the method referred to in paragraph 1 to data retained on the basis of Article 126 of the [2005] Law …, the following provisions shall apply:

1. for a potential threat relating to an activity that may be linked to criminal organisations or harmful sectarian organisations, the director of the service may, in his or her decision, only request the data in respect of a period of six months prior to the decision;

2. for a potential threat other than those referred to in points 1 and 3, the director of the service may, in his or her decision, request the data in respect of a period of nine months prior to the decision;

3. for a potential threat relating to an activity that may be linked to terrorism or extremism, the director of the service may, in his or her decision, request the data in respect of a period of 12 months prior to the decision.

…'

II. Facts and questions referred for a preliminary ruling

15. In its judgment of 11 June 2015,[14] the Cour constitutionnelle (Constitutional Court, Belgium) annulled the new version of Article 126 of the 2005 Law, on the same grounds as those on which the Court of Justice had declared Directive 2006/24 invalid in the judgment in *Digital Rights*.

[14] Judgment No 84/2015, *Moniteur belge* of 11 August 2015.

16. In the light of that annulment, the national legislature adopted (prior to the delivery of the judgment in *Tele2 Sverige and Watson*) the Law of 29 May 2016.

17. VZ and Others, the Ordre des barreaux francophones et germanophone ('Ordre des barreaux'), the Liga voor Mensenrechten ASBL ('LMR'), the Ligue des Droits de l'Homme ASBL ('LDH') and the Académie Fiscale ASBL ('Académie Fiscale') brought before the referring court a number of actions seeking a declaration that the aforementioned law was unconstitutional on the ground, in essence, that it went beyond what was strictly necessary and did not establish adequate guarantees of protection.

18. It is in those circumstances that the Cour constitutionnelle (Constitutional Court) has referred the following questions to the Court of Justice:

'(1) Must Article 15(1) of [Directive 2002/58], read in conjunction with the right to security, guaranteed by Article 6 of the Charter of Fundamental Rights of the European Union ['the Charter'], and the right to respect for personal data, as guaranteed by Articles 7, 8 and 52(1) of the Charter …, be interpreted as precluding national legislation such as that at issue, which lays down a general obligation for operators and providers of electronic communications services to retain the traffic and location data within the meaning of [Directive 2002/58], generated or processed by them in the context of the supply of those services, national legislation whose objective is not only the investigation, detection and prosecution of serious criminal offences but also the safeguarding of national security, the defence of the territory and of public security, the investigation, detection and prosecution of offences other than serious crime or the prevention of the prohibited use of electronic communication systems, or the attainment of another objective identified by Article 23(1) of Regulation (EU) 2016/679 [of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1)] and which, furthermore, is subject to specific guarantees in that legislation in terms of data retention and access to those data?

(2) Must Article 15(1) of [Directive 2002/58], in conjunction with Articles 4, 7, 8, 11 and 52(1) of the Charter …, be interpreted as precluding national legislation such as that at issue, which lays down a general obligation for operators and providers of electronic communications services to retain the traffic and location data within the meaning of [Directive 2002/58], generated or processed by them in the context of the supply of those services, if the object of that legislation is, in particular, to comply with the positive obligations borne by the authority under Articles 4 and 8 of the Charter, consisting in providing for a legal framework which allows the effective criminal investigation and the effective punishment of sexual abuse of minors and which permits the effective identification of the perpetrator of the offence, even where electronic communications systems are used?

(3) If, on the basis of the answer to the first or the second question, the Cour constitutionnelle (Constitutional Court) should conclude that the contested law fails to fulfil one or more obligations arising under the provisions referred to in these questions, might it maintain on a temporary basis the effects of the [contested Law] in order to avoid legal uncertainty and to enable the data previously collected and retained to continue to be used for the objectives pursued by the law?'

III. Procedure before the Court of Justice

19. The reference for a preliminary ruling was registered at the Court on 2 August 2018.

20. Written observations have been submitted by VZ and Others, Académie Fiscale, LMR, LDH, Ordre des barreaux, the Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), the Belgian, Czech, Danish, German and Estonian Governments, Ireland, the Spanish, French, Cypriot, Hungarian, Netherlands, Polish, Swedish and United Kingdom Governments, and the European Commission.

21. A hearing held on 9 September 2019, in conjunction with the hearings in Cases C-511/18, C-512/18 and C-623/17, was attended by the parties in the four references for a preliminary ruling, the aforementioned governments and the Government of Norway, the Commission and the European Data Protection Supervisor.

IV. Analysis

22. The first question in this reference for a preliminary ruling is, in essence, the same as those to be disposed of in Cases C-511/18 and C-512/28. It differs from the latter, however, with respect to the objectives pursued by the national legislation, which, in this instance, are not only the fight against terrorism and the most serious forms of crime and the safeguarding of national security, but also 'defence of the territory, public security [and] the investigation, detection and prosecution of offences other than serious crime', as well as, generally, any of the objectives provided for in Article 23(1) of Regulation 2016/679.

23. The second question is linked to the first but supplements it by asking whether the positive obligations which fall to the public authority in relation to the investigation and punishment of the sexual abuse of minors would justify the contested measures.

24. The third question is raised in the event that the national legislation is incompatible with EU law. The referring court wishes to ascertain whether, in that event, the effects of the Law of 29 May 2016 could be temporarily maintained.

25. I shall address these questions by analysing, in the first place, the applicability of Directive 2002/58, to which end I shall refer to my Opinion in some of the other references for a preliminary ruling related to this one. In the second place, I shall set out the main lines of the case-law of the Court in this area and the scope for its further development. Finally, I shall look at how each of the questions referred for a preliminary ruling should be answered.

A. Applicability of Directive 2002/58

26. Like the other three references for a preliminary ruling, this one too has called into question the applicability of Directive 2002/58. Given that the stances taken by the Member States in this regard are the same, I refer on this point to the Opinion in Joined Cases C-511/18 and C-512/18. [15]

[15] Point 40 et seq.

B. Case-law of the Court on the retention of, and access to, personal data by the public authorities under Directive 2002/58

1. The principle of the confidentiality of communications and related data

27. The provisions of Directive 2002/58 'particularise and complement' Directive 95/46/CE [16] with a view to achieving a high level of protection for personal data in the context of the provision of electronic communications services. [17]

28. Article 5(1) of Directive 2002/58 provides that, in their national legislation, Member States must ensure the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as the confidentiality of related traffic data.

29. The confidentiality of communications implies, inter alia (second sentence of Article 5(1) of Directive 2002/58), that any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. Exceptions are created for 'persons lawfully authorised … and the technical storage necessary for conveyance of a communication'. [18]

30. Articles 5 and 6 and Article 9(1) of Directive 2002/58 have as their purpose to preserve the confidentiality of communications and related data and to minimise the risk of abuse. Their scope must be assessed in the light of recital 30 of that directive, according to which 'systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict *minimum*'. [19]

31. As regards that data, a distinction may be drawn between:

– *Traffic* data, the processing and storage of which are permitted only to the extent and for the time necessary for the billing and marketing of services and the provision of value added services (Article 6 of Directive 2002/58). Once that period has elapsed, the data processed and stored must be erased or made anonymous. [20]

– *Location* data other than traffic data, which may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained (Article 9(1) of Directive 2002/58). [21]

16 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). See Article 1(2) of Directive 2002/58. Directive 95/46 was repealed with effect from 25 May 2018 by Regulation 2016/679. Consequently, in so far as Directive 2002/58 refers to Directive 95/46 or does not lay down rules of its own, account must be taken of the provisions of that regulation (see Article 94(1) and (2) of Regulation 2016/679).

17 Judgment in *Tele2 Sverige and Watson*, paragraphs 82 and 83.

18 *Ibidem*, paragraph 85 and the case-law cited.

19 *Ibidem*, paragraph 87. No emphasis in the original.

20 *Ibidem*, paragraph 86 and the case-law cited.

21 *Ibidem*, paragraph 86, *in fine*.

2. The restriction clause laid down in Article 15(1) of Directive 2002/58

32. Article 15(1) of Directive 2002/58 allows Member States to '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 that directive.

33. Any restriction must constitute '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]'.

34. That list of objectives is exhaustive: [22] for example ('inter alia'), 'legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph' are permitted.

35. In any event, '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'. Consequently, Article 15(1) of Directive 2002/58 must be interpreted in the light of the fundamental rights guaranteed by the Charter. [23]

36. Of those rights recognised in the Charter, the Court has referred, for the purposes of the present case, to the right to privacy (Article 7), the right to the protection of personal data (Article 8) and the right to freedom of expression (Article 11). [24]

37. The Court has also emphasised, as a guide to its interpretation of Article 15(1) of Directive 2002/58, that the restrictions on the obligation to ensure the confidentiality of communications and related traffic data must be interpreted strictly.

38. In particular, it has held that 'the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58 [must not] become the rule, if the latter provision is not to be rendered largely meaningless'. [25]

39. That twofold observation strikes me as being crucial to understanding why the Court has deemed the general and indiscriminate retention of traffic and location data relating to electronic communications to be incompatible with Directive 2002/58.

40. By that finding, the Court did no more than 'strictly' [26] apply the proportionality criterion which it had already employed previously: [27] 'the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary'. [28]

22 *Ibidem*, paragraph 90.

23 *Ibidem*, paragraph 91 and the case-law cited.

24 *Ibidem*, paragraph 93 and the case-law cited.

25 *Ibidem*, paragraph 89.

26 The use of this adverb in the judgment in *Tele2 Sverige and Watson*, paragraph 95, comes from recital 11 of Directive 2002/58.

27 Judgment in *Digital Rights*, paragraph 48: 'In view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict'.

28 Judgment in *Tele2 Sverige and Watson*, paragraph 96 and the case-law cited.

3. Proportionality in the retention of data

(a) The disproportionate nature of general and indiscriminate retention

41. The Court recognised that the fight against serious crime, in particular against organised crime and terrorism, is of the utmost importance in order to ensure public security, and that its effectiveness may depend to a great extent on the use of modern investigation techniques. It went on to say that, 'however, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight'. [29]

42. In order to determine whether a measure of this kind was confined to what was strictly necessary, the Court had regard, first and foremost, to the particular seriousness of its interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. [30] The particular seriousness derived from the very fact that the national legislation provided for 'a general and indiscriminate retention of *all traffic and location data of all subscribers and registered users relating to all means of electronic communication*, and … imposes on providers of electronic communications services an obligation to retain that data *systematically and continuously, with no exceptions*'. [31]

43. The interference which that measure entailed in the lives of citizens is reflected in the Court's foregoing findings with respect to the effects of the retention of data.

That data [32]

– 'makes it possible to trace and identify the source of a communication and its destination, to identify the date, time duration and type of communication, to identify users' communication equipment, and to establish the location of mobile communication equipment'. [33]

– 'makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period'. [34]

– 'is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'. [35]

29 Judgment in *Digital Rights*, paragraph 51. See to the same effect the judgment in *Tele2 Sverige and Watson*, paragraph 103.

30 Judgments in *Digital Rights*, paragraph 65, and *Tele2 Sverige and Watson*, paragraph 100.

31 Judgment in *Tele2 Sverige and Watson*, paragraph 97. My emphasis.

32 Which include the name and address of the subscriber or registered user, the source and destination telephone numbers and an IP address for internet services.

33 Judgment in *Tele2 Sverige and Watson*, paragraph 98.

34 *Ibidem*, paragraph 98.

35 *Ibidem*, paragraph 99.

– 'Provides the means … of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications'. [36]

44. The interference may also cause 'the persons concerned to feel that their private lives are the subject of constant surveillance', since 'the data is retained without the subscriber or registered user being informed'. [37]

45. Given the extent of the interference, only the fight against serious crime is capable of justifying such a data retention measure. [38] Such a measure must not, however, become the general rule, since 'the system put in place by Directive 2002/58 requires the retention of data to be the exception'. [39]

46. Two other considerations present were the fact that the measure at issue provided for 'no differentiation, limitation or exception according to the objective pursued' [40] and 'does not require there to be any relationship between the data which must be retained and a threat to public security': [41]

– First, the measure was comprehensive in that it '[affected] all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings … Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy'. [42]

– Secondly, 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'. [43]

47. In those circumstances, the national legislation at issue exceeded the limits of what was strictly necessary. For that reason, it could not 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 and 11 and Article 52(1) of the Charter. [44]

(b) The viability of targeted data retention

48. The Court has recognised as being consistent with EU law national legislation 'permitting, as a preventive measure, the *targeted retention* of traffic and location data, for the purpose of fighting serious crime'. [45]

36 *Ibidem*, paragraph 99 *in fine*.
37 *Ibidem*, paragraph 100.
38 *Ibidem*, paragraph 102.
39 *Ibidem*, paragraph 104.
40 *Ibidem*, paragraph 105.
41 *Ibidem*, paragraph 106.
42 *Ibidem*, paragraph 105.
43 *Ibidem*, paragraph 106.
44 *Ibidem*, paragraph 107.
45 *Ibidem*, paragraph 108. My emphasis.

49. The validity of the targeted retention of data is conditional upon the latter being 'limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.

50. The guidelines which the judgment in *Tele 2 Sverige and Watson* provide for the purposes of determining when the foregoing conditions are met are not (and perhaps could not be) exhaustive and are framed in more general terms. If they are to adhere to those guidelines, Member States must:

– lay down clear and precise rules governing the scope and application of such a data retention measure; [46]

– lay down 'objective criteria that establish a connection between the data to be retained and the objective pursued'; [47] and

– '[base the national legislation] on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting crime or to preventing a serious risk to public security'. [48]

51. So far as the aforementioned objective is concerned, the Court has pointed by way of example to the possibility of using a geographical criterion in order to define the public and situations potentially affected. The mention of that criterion, about which certain Member States have been critical, is not, in my opinion, intended to confine to it alone the range of permissible filters.

4. Proportionality in access to data

(a) The judgment in Tele2 Sverige and Watson

52. The Court addresses *access* to data by the national authorities separately from the scope of the obligation to *retain* that is imposed on providers of electronic communications services and, in particular, from the general or specific nature of the retention of those data. [49]

53. After all, although the purpose of retention is to facilitate later access to data, both access and retention are capable of giving rise to different infringements of the fundamental rights protected by the Charter. That distinction does not mean, however, that some of the considerations relating to retention are not also applicable to access to the data retained.

54. Accordingly, access:

– 'Must correspond, genuinely and strictly, to one of [the] objectives' set out in the first sentence of Article 15(1) of Directive 2002/58. There must also be consistency between the interference

[46] *Ibidem*, paragraph 109. In particular, they must indicate 'in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary'.

[47] *Ibidem*, paragraph 110.

[48] *Ibidem*, paragraph 111.

[49] *Ibidem*, paragraph 113.

and the objective pursued. If the interference is considered to be serious, it may be justified only by the fight against serious crime. [50]

– It may be authorised only within the limits of what is strictly necessary. [51] Furthermore, legislative measures must lay down 'clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law'. [52]

– More specifically, national legislation must lay down 'the substantive and procedural conditions governing the access of the competent national authorities to the retained data'. [53]

55. The foregoing supports the inference that 'general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary'. [54]

56. According to the Court, 'the national legislation must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of the subscribers or registered users'. [55] 'In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only *to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime*'. [56]

57. In other words, national rules which grant competent national authorities access to retained data must have a sufficiently limited scope. There must be a link between the persons concerned and the objective pursued so as to ensure that access does not extend to a significant number of persons, or even to all persons, all means of electronic communication and all stored data.

58. Those rules can, however, be relaxed in certain circumstances. The Court has in mind 'particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities'. In such situations, 'access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities'. [57]

59. That clarification from the Court makes it possible for Member States to establish a specific regime for more extensive access to data, in the exceptional case where this is necessary in order to combat threats to overriding State interests (national security, defence and public security), [58] that even includes persons only indirectly linked to such risks.

50 *Ibidem*, paragraph 115.

51 *Ibidem*, paragraph 116.

52 *Ibidem*, paragraph 117.

53 *Ibidem*, paragraph 118.

54 *Ibidem*, paragraph 119.

55 Idem.

56 Idem. My emphasis.

57 Idem.

58 Such an exception might be justified not only by terrorist activities but also, for example, a large-scale computer attack on critical State infrastructures or a threat relating to nuclear proliferation.

60. Access by the national authorities to stored data must, whatever the description of the data, be subject to three conditions:

– It must, 'as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body'. The decision of that court or body must be made 'following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime'. [59]

– 'The competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities'. [60]

– Member States must adopt rules on the security and protection of data in the possession of providers of electronic communications services in order to avoid misuse of, and unlawful access to, that data. [61]

(b) The judgment in Ministerio Fiscal

61. That case concerned whether national legislation allowing the competent authorities to access data relating to the civil identity of holders of certain SIM cards was compatible with Article 15(1) of Directive 2002/58, interpreted in the light of Articles 7 and 8 of the Charter.

62. The Court held that the first sentence of Article 15(1) of Directive 2002/58 does not limit the objective of preventing, investigating, detecting and prosecuting criminal offences to the fight against serious crime alone, but refers to 'criminal offences' generally. [62]

63. It went on to say that, in order to justify access to data by the competent national authorities, there must be a correspondence between the seriousness of the interference and the seriousness of the offences in question. Consequently:

– 'Serious interference can be justified … only by the objective of fighting crime which must also be defined as "serious"'. [63]

– By contrast, 'when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting "criminal offences" generally'. [64]

59 Judgment in *Tele2 Sverige and Watson*, paragraph 120.

60 *Ibidem*, paragraph 121.

61 *Ibidem*, paragraph 122.

62 Judgment in *Ministerio Fiscal*, paragraph 53.

63 *Ibidem*, paragraph 56.

64 *Ibidem*, paragraph 57.

64. Starting from that premiss, and unlike in the judgment in *Tele2 Sverige and Watson*, the Court did not classify the interference with the rights protected in Articles 7 and 8 of the Charter as 'serious', since 'the sole purpose of the request … [was] to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone'. [65]

65. In order to highlight the less serious nature of the interference, the Court explained that 'the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile phone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period'. [66]

66. The case disposed of by the judgment in *Ministerio Fiscal* was not concerned with whether the personal data being accessed had been retained by providers of electronic communications services in accordance with the conditions set out in Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter. [67] Neither did that judgment address whether or not the conditions of access laid down in that article had been fulfilled.

67. It follows that a reading of the judgment in *Ministerio Fiscal* does not support the inference of any change in the Court's case-law on the incompatibility with EU law of a national scheme which authorises the general and indiscriminate storage of data within the meaning of the judgment in *Tele2 Sverige and Watson*.

68. It is my view, however, that, inasmuch as the Court recognises the validity of a scheme granting access only to certain personal data (those relating to the civil identity of the holders of SIM cards), it implicitly accepts the feasibility of the same data being retained by service providers.

C. The main criticisms of the Court's case-law

69. Both the referring court and the majority of the Member States which have submitted observations ask the Court to clarify, refine or even reconsider various aspects of its case-law in this field, of which they are critical.

70. Most of their criticisms, whether veiled or direct, were originally expressed in relation to the judgment in *Digital Rights* and were rejected in the judgment in *Tele 2 Sverige and Watson*. In the form in which they have re-emerged now, they claim, in essence, that strict rules on access to data held by providers of electronic communications services would be sufficient to offset to some extent the seriousness of the interference represented by the general and indiscriminate retention of such data.

65 *Ibidem*, paragraph 59. Access had been requested 'to the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern, as confirmed by both the Spanish Government and the Public Prosecutor's Office during the hearing, the communications carried out with the stolen mobile phone or its location'.

66 *Ibidem*, paragraph 60.

67 Judgment in *Ministerio Fiscal*, paragraph 49.

71. Some of those criticisms also underscore the need to adopt genuinely effective measures to combat serious threats to security and crime in general, and ask the Court to take into account the right to security (Article 6 of the Charter) and the discretion enjoyed by the Member States when it comes to safeguarding national security. In one case, it is added that the Court has failed to consider the preventive nature of intervention by the security and intelligence services.

D. My assessment of those criticisms and of the refinements that could be made to the Court's case-law

72. In my opinion, the Court should maintain the position in principle at which it arrived in its previous judgments: a general and indiscriminate obligation to retain all traffic and location data of subscribers and registered users disproportionately infringes the fundamental rights protected by Articles 7 and 8 of the Charter.

73. Conversely, national legislation which attaches appropriate restrictions to the retention of some of those data, generated in the course of the provision of electronic communications services, might be compatible with EU law. The key, therefore, lies in *limited retention*, of such data.

74. As I shall go on to explain, the limitations on retention should not be confined to ones defined by a geographical area or a category of particular persons: the discussion of those criteria has shown that they might well be unachievable or unfit for the purposes for which they were intended, or might even become a source of discrimination.

75. I should say at the outset that I do not endorse the criticism that advocates the duality of 'more extensive retention in return for more restricted access'. The Court's reasoning, with which I agree, is that retention of, and access to, data are two different types of interference. Even in the case where data retention is useful from the point of view of potential subsequent access by the competent authorities, each one of those interferences must be justified separately by being examined specifically in the light of the objective pursued.

76. It follows that a national system which provides for the general and indiscriminate storage of data cannot be justified on the basis that the rules under that system simultaneously lay down strict substantive and procedural conditions of access to those data.

77. There must, therefore, be specific data retention rules that subject retention to certain conditions in order to ensure that it does not become general and indiscrimininate. This is the only way of guaranteeing the compatibility of retaining data with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

78. This, moreover, is the approach that has been taken by the working groups meeting within the Council to define rules on retention and access that are compatible with the Court's case-law, inasmuch as they are examining the two types of interference in tandem. [68]

[68] The Member States have since 2017 been participating in a working group the purpose of which is to bring their laws into line with the criteria laid down in the Court's case-law in this field [Groupe Échange d'informations et protection des données (DAPIX)].

79. Applying limitations to each of those two types of interference will make it possible to assess whether any cumulative effect those limitations may have, combined with strong safeguards, is such as to mitigate the impact of data retention on the fundamental rights protected by Articles 7, 8 and 11 of the Charter, while at the same time ensuring the effectiveness of investigations.

80. In order to protect those rights, the system must:

– Provide for a data retention regime that contains certain limitations and differences depending on the objective pursued.

– Regulate access to those data only to the extent strictly necessary for the purpose for which they are intended and under the supervision of a court or independent administrative authority.

81. The justification for providers of electronic communications services retaining certain data, and not only for the purposes of managing their contractual obligations to users, increases in tandem with advances in technology. If we accept the proposition that such retention is useful from the point of view of preventing and combating terrorism (which is difficult to refute [69]), there would seem to be no logic in confining the scope of such retention exclusively to the exploitation of data which operators retain in order to carry on their commercial activities, and to the period of time necessary for the completion of those activities.

82. Having recognised the usefulness of an obligation to retain data for the purposes of safeguarding national security that goes beyond the retention in which operators may engage in order to meet their technical and commercial needs, we must now define the parameters of that obligation.

83. Each retention scheme must be strictly adapted to its intended purpose so as to ensure that the retention does not become indiscriminate. [70] It must also ensure that the sum of those data does not provide a *profile* of the person concerned (that is to say, of his or her usual activities and social relations) that comes close or is similar to that which would be obtained from knowing the content of his or her communications.

84. In the interests of clearing up a number of misconceptions and misunderstandings, it is important to take into account what the Court *did not state* in its judgments in *Digital Rights* and *Tele2 Sverige and Watson*. In those judgments, the Court did not censure the existence *per se* of a data retention scheme as a useful instrument for fighting crime. On the contrary, it recognised the legitimacy of the objective of preventing and punishing criminal acts, and the usefulness of a data retention scheme in achieving that objective.

85. What the Court ruled out, and ruled out firmly, on those occasions, as I have said before, was the proposition that Member States can rely on that objective in order to prescribe the indiscriminate retention of, and general access to, *all* data generated in the course of the provision of electronic communications services.

69 In any event, the determination of those investigation techniques and the assessment of their effectiveness are matters falling within the discretion of the Member States.

70 Judgment in *Digital Rights*, paragraph 57, and judgment in *Tele2 Sverige and Watson*, paragraph 105.

86. It is therefore necessary to find forms of data retention that mean that the retention cannot be so characterised ('general and indiscriminate') as to be incompatible with the protection required by Articles 7, 8 and 11 of the Charter.

87. One such form would be the *targeted* retention of data, whether relating to a specific public (in theory, individuals with certain links, direct or otherwise, to the most serious threats) or a particular geographical area.

88. This approach, however, presents a number of difficulties:

– It would probably not be enough to identify a group of potential aggressors if the latter use anonymisation techniques or falsify their identities. Choosing such groups could also have the effect of creating a climate of general suspicion in relation to certain segments of the population and might be considered discriminatory, depending on the algorithm used.

– Selection by geographical criteria (which, to be effective, would involve targeting areas of a not insignificant size) raises the same problems and creates yet more, as the European Data Protection Supervisor indicated at the hearing, in that it could stigmatise certain areas.

89. There may also be a degree of contradiction between the preventive targeting of retention at a specific section of the public or a particular geographical area and the fact that it is impossible to know in advance who the perpetrators of criminal offences will be or where and when those offences will be committed.

90. Be that as it may, it is important not to rule out the possibility of finding some forms of targeted retention based on those criteria that will be useful in achieving the objectives set out above. It is for the legislature in each Member State or for the Union as a whole to design such formulas, ensuring that they are respectful of the protection of fundamental rights that the Court safeguards.

91. It would be a mistake to believe that the targeted retention of data belonging to a specific section of the public or a particular geographical area is the only formula which the Court finds compatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter.

92. It is possible, as I have said before, to find forms of targeted data retention other than ones focused on specific groups of persons or geographical areas. Indeed, this is the view taken by the Council working groups to which I referred earlier: the avenues for exploration they have considered include, in particular, limiting the categories of data retained;[71] pseudonymising data;[72] introducing limited retention periods;[73] excluding certain categories of provider of

[71] Data not strictly essential and objectively necessary for preventing and prosecuting crime and protecting public security would be excluded from the retention obligation. In particular, there would be a need to indicate, in accordance with the objective pursued, what types of subscriber data, traffic data and location data must compulsorily be retained in order to achieve that objective. More specifically, data not considered essential to the investigation and prosecution of crimes would be excluded.

[72] A method whereby names are replaced with an alias so that data are no longer linked to a name. Unlike anonymisation, pseudonymisation allows data to be relinked to names.

[73] Retention periods could conceivably be adjusted to the different categories of data involved, depending on the extent of their intrusiveness in individuals' private lives. In addition, there would have to be a requirement for the data to be erased at the end of the retention period.

electronic communications services;[74] renewable storage authorisations;[75] the obligation to retain data stored within the Union or the systematic and regular supervision by an independent administrative authority of the guarantees given by providers of electronic communications services against the misuse of data.

93. In my opinion, the preferred option, from the point of view of compatibility with the case-law of the Court, is the temporary retention of certain *categories* of traffic and location data, which would be limited according to the strict needs of security and which, taken as a whole, could not be used to obtain a clear and detailed picture of the lives of the persons concerned.

94. In practice, this means that, within the two main categories (traffic data and location data), retention should only be available, via the appropriate filters, for the *minimum* amount of data deemed absolutely essential for effectively preventing and monitoring crime and safeguarding national security.

95. It is for the Member States or the institutions of the European Union to conduct this selection exercise by way of legislation (with the assistance of their own experts), abandoning any attempt to prescribe the general and indiscriminate storage of all traffic and location data.

96. In addition to being limited by category, data retention must be available only for a given period so as to ensure that the data in question cannot be used to provide a detailed picture of the lives of the persons concerned. That retention period must also be adjusted according to the nature of the data, so that data providing more detailed information on the lifestyles and habits of those persons are stored for a shorter period of time.[76]

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

98. The European Data Protection Officer's submissions at the hearing were along the same lines: the more categories of stored metadata there are, and the longer they are stored for, the easier it will be to produce a detailed profile of an individual, and vice versa.[77]

74 Consideration could be given to the possibility of not imposing the obligation to retain data on all providers of electronic communications services but, instead, triggering that obligation on the basis of the size of the provider and the type of services supplied, providers of highly specialised services, for example, being excluded.

75 Authorisation systems could be based on periodic threat assessments in each Member State. It would have to be ensured that there is a link between the data retained and the objective pursued and that that link is adapted to the specific situation of each Member State. Retention authorisations granted to providers could therefore allow certain types of data to be retained for a certain period of time depending on the assessment of the threat. Such authorisations could be granted by a judge or an independent administrative authority and would be followed by a periodic review of the conditions of retention.

76 This appears to be the system employed in the Federal Republic of Germany, the government of which stated at the hearing that, under its legislation, the retention period for traffic data is 10 weeks, while the retention period for location data is only 4 weeks. In the French Republic, on the other hand, traffic and location data must be stored for a period of one year. According to the latter Member State, reducing that period to less than a year would diminish the effectiveness of the services provided by the judicial police.

77 It must of course be ensured that providers of electronic communications services permanently erase the data at the end of the retention period (the exception to this requirement being those data that they may continue to store for commercial purposes, in accordance with Directive 2002/58).

99. Furthermore, as also become apparent at the hearing, it is difficult to draw a dividing line between certain classes of metadata in electronic communications and the content of those communications. Some metadata can be as revealing as the content of the communication itself, if not more so: this can be the case with the addresses (URLs) of websites which have been visited.[78] It follows that this type of data and others like it should be given special attention so as to limit as much as possible the need for, and period of, their retention.

100. Finding a balanced solution is not easy, as the technique of cross-referencing and correlating stored data enables investigation and surveillance services to identify a suspect or a threat, as the case may be. Even so, there is a difference in degree between retaining data for the purposes of detecting a suspect or a threat and data retention that has the effect of providing a detailed portrait of an individual's life.

101. Pending common rules throughout the European Union in this particular field, I do not think it appropriate to ask the Court to take on a regulatory role and spell out which categories of data can be retained and for how long. It is for the EU institutions and the Member States, once the limits which the Court has defined as deriving from the Charter have been established, to point the cursor in the right direction for striking a balance between the preservation of security and the fundamental rights protected by the Charter.

102. It is true that dispensing with the information that can be inferred from a larger volume of retained data might make it more difficult in some cases to counter potential threats. This, however, is one of a number of prices which the public authorities have to pay when they impose on themselves the obligation to safeguard fundamental rights.

103. Just as nobody would support an *ex ante* obligation to engage in the general and indiscriminate retention of the *content* of private electronic communications (even if the law guaranteed that subsequent access to that content would be restricted), the metadata in those communications, which can disclose information as sensitive as the content itself, must not be allowed to be the subject of indiscriminate and general storage either.

104. The legislative difficulty — which I recognise — of providing a detailed definition of the circumstances and conditions under which targeted retention is feasible is no reason for the Member States, by turning the exception into a rule, to make the general retention of personal data the core principle of their legislation. To do so would be to lend indefinite validity to a significant infringement of the right to the protection of personal data.

105. I should add that there is no reason why, in genuinely *exceptional* situations characterised by an imminent threat or an extraordinary risk warranting the official declaration of a state of emergency in a Member State, national legislation should not make provision, for a limited period, for the possibility of imposing an obligation to retain data that is as extensive and general as is deemed necessary.

106. On that basis, legislation could be enacted which specifically permits more extensive retention of (and access to) data, in accordance with conditions and procedures ensuring that such measures are extraordinary in terms of their substantive scope and period of validity, and subject to the corresponding judicial guarantees.

[78] At the hearing, the French Government stated that URLs were excluded from the connection data in respect of which its legislation lays down a general duty of retention.

107. A comparative examination of legislative rules governing situations of constitutional emergency shows that it is not impossible to define factual circumstances capable of triggering the application of a particular set of legislative rules prescribing which authority may take such a decision, in what circumstances and under whose supervision. [79]

E. Specific answers to the three questions referred

1. Preliminary consideration

108. The referring court asks for an interpretation of Article 15(1) of Directive 2002/58 read in conjunction with various rights guaranteed by the Charter: the right to respect for private and family life (Article 7), the right to the protection of personal data (Article 8) and the right to freedom of expression and information (Article 11).

109. As I explain in my Opinion in Joined Cases C-511/18 and C-512/18, these are indeed the rights determined by the Court of Justice as being potentially adversely affected in such circumstances.

110. However, the Cour constitutionnelle (Constitutional Court) also mentions Articles 4 and 6 of the Charter, with which the second and first questions referred are respectively concerned.

111. Article 6 of the Charter, which guarantees the right to freedom and security, has also been relied on in Cases C-511/18 and C-512/18 and I have commented on the relevance of that article in my Opinion in those cases, to which I refer. [80]

112. As regards Article 4 of the Charter, since the answer depends not so much on an analysis of the domestic legislation in the light of EU law as on the interpretation of that provision, it seems appropriate for me to answer this question first.

2. The second question referred

113. The reference to the prohibition of torture and inhuman or degrading treatment, laid down in Article 4 of the Charter, is, after all, exclusive to this reference for a preliminary ruling and I must therefore address it.

114. In citing Article 4 of the Charter, the referring court wishes to make it clear that the national legislation also has the purpose of complying with the *positive obligation* incumbent on the public authority to establish 'a legal framework which allows the effective criminal investigation and the effective punishment of sexual abuse of minors and which permits the effective identification of the perpetrator of the offence, even where electronic communications systems are used'. [81]

[79] Ackerman, B., 'The Emergency Constitution', *Yale Law Journal*, vol. 113, 2004, pp. 1029 to 1092; Ferejohn, J. and Pasquino, P., 'The Law of the Exception: A typology of Emergency Powers', *International Journal of Constitutional Law*, vol. 2, 2004, pp. 210 to 239.

[80] Opinion in Joined Cases C-511/18 and C-512/18, point 95 et seq.

[81] Wording of the second question, *in fine*. That reference to electronic means of communication explains why the question mentions a second *positive obligation* incumbent on those States, that imposed by Article 8 of the Charter with respect to the protection of personal data. The dual reference to Article 8 of the Charter shows that the referring court considers the rights under the Charter, depending on their nature, to perform a dual role: as a *limit* on the obligation at issue and as a *justification* for that obligation.

115. In my opinion, that particular *positive obligation* is not very different from each of the specific duties which the establishment of a range of fundamental rights imposes on the State. The rights to life (Article 2 of the Charter), to the integrity of the person (Article 3 of the Charter) or to the protection of personal data (Article 8 of the Charter), like the freedoms of expression (Article 11 of the Charter) or of thought, conscience and religion (Article 10 of the Charter), entail for the State an obligation to create a legislative framework guaranteeing the effective enjoyment of those rights and freedoms, if necessary by using the force vested in the public authorities alone as against anyone who seeks to prevent it from doing so or to make it more difficult for it to do so. [82]

116. As regards the sexual abuse of minors, the European Court of Human Rights (ECtHR) takes the view that children and other vulnerable persons have a qualified right to State protection in the form of the adoption of criminal-law provisions which penalise and act as a deterrent to the commission of such offences. [83]

117. That qualified right to protection is enshrined not only in Article 4 of the Charter, since Article 1 (human dignity) or Article 3 (right to physical and mental integrity) could of course be relied on to that end.

118. Although the positive obligation on the public authorities to ensure the protection of children and other vulnerable persons cannot be left out of account when it comes to weighing up the legal interests affected by the national legislation, [84] neither can it give rise to 'excessive burdens' for the public authorities [85] or be fulfilled without regard to legality or respect for other fundamental rights. [86]

3. The first question referred

119. The referring court wishes to ascertain, in essence, whether EU law precludes the national law on which it has been called upon to give a ruling in the course of an action for a declaration of unconstitutionality.

120. As the Court has already provided an interpretation of Directive 2002/58 which is consistent with the corresponding provisions of the Charter, the answer to this question must take into account the case-law established in the judgment in *Tele2 Sverige and Watson*, together with any refinements to be incorporated here.

82 That obligation of effectiveness amounts to a mandate to achieve results for the public authorities in a social or welfare State, in which what matters is not only the formal recognition of rights but also the practical implementation of their substance.

83 ECtHR, judgment of 2 December 2008, *K.U. v. Finland* (ECHR:2008:1202JUD000287202, § 46).

84 In this regard, I take the view that to the rights cited by the referring court (as *limits* on, not *justifications* for, the obligation at issue) one could add the right to an effective remedy (Article 47 of the Charter) or the right of defence (Article 48 of the Charter), the possible infringement of which was also discussed in the main proceedings. However, the operative part of the order for reference mentions only Articles 7, 8 and 11 and Article 52(1) of the Charter.

85 ECtHR, judgment of 28 October 1998, *Osman v. the United Kingdom* (CE:ECHR:1998:1028JUD002345294, § 116).

86 *Ibidem* § 116 *in fine*: '[it is necessary] to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime'. See also the ECtHR, judgment of 2 December 2008, *K.U. v. Finland* (CE:ECHR:2008:1202JUD000287202, § 48). To the same effect, the Court held in the judgment of 29 July 2019, *Gambino and Hyka* (C-38/18, EU:C:2019:628, paragraph 49), that rights in favour of the victim cannot detract from the effective enjoyment of those conferred on the defendant.

121. On that premiss, the interpretative guidance that may be provided to the Cour constitutionnelle (Constitutional Court) to enable it to undertake its own review of the conformity of the domestic legislation with EU law must deal separately with the retention of, and access to, data as regulated in that national legislation.

(a) The conditions governing data retention

122. The Belgian Government states that it wished to establish a clear legal framework that included the guarantees necessary to protect privacy, rather than to take as its basis the practice of operators of electronic communications services in relation to the retention of data for the purposes of billing and processing requests for information from customers.

123. In its view, the general and preventive obligation to retain data has as its purpose not only to assist the investigation, detection and prosecution of serious criminal offences, but also to safeguard national security, defence of the territory and public security, investigate, detect and prosecute offences other than serious criminal offences and prevent the prohibited use of electronic communications systems,[87] and to pursue any other objective identified in Article 23(1) of Regulation 2016/679.

124. According to the Belgian Government:

– The retention of data does not, per se, allow very precise conclusions to be drawn with respect to the private lives of the persons concerned: drawing such conclusions would become a possibility only if access to the data retained were also made available.

– The law contains safeguards intended to protect privacy, including: the fact that retention of data does not affect the content of communications; guarantees with respect to justification for retention, rights of access, rights of rectification and so on are fully applicable; providers and operators must subject retained data to the same obligations and security and protection measures as those that apply to data on the network, and ensure that they are not accidentally or unlawfully destroyed or accidentally lost or altered.

– Data may be stored for 12 months (at the end of which it must be destroyed) and only in the territory of the European Union.

– Providers and operators must employ technological protection measures which ensure that, as soon as retained data is recorded, it is illegible to and unusable by anyone not authorised to have access to it.

– In any event, such operations are carried out under the supervision of the Belgian regulator for the postal and telecommunications sectors and the Data Protection Authority.

125. Notwithstanding those guarantees, it is true that the Belgian legislation imposes on operators and providers of electronic communications services a general and indiscriminate obligation to retain traffic and location data, within the meaning of Directive 2002/58, processed

[87] That obligation is also justified for the purposes of responding to calls made to the emergency services or finding missing persons whose physical integrity is in imminent danger.

in the course of the provision of those services. The retention period is, as I have already said, 12 months in general: there is no provision for limiting that period depending on the category of data retained.

126. That general and indiscriminate retention obligation applies permanently and continuously. Even where its objective is to prevent, investigate and prosecute any kind of criminal offence (from those relating to national security, defence or other very serious criminal acts to those that carry a prison sentence of less than a year), an obligation of this description is not consistent with the case-law of the Court and, for that reason, cannot be considered compatible with the Charter.

127. In order to be consistent with that case-law, the Belgian legislature will have to explore other avenues (such as those I mentioned earlier) based on limited retention formulas. Those formulas, which vary according to the category of data involved, must comply with the principle that only the *minimum* amount of data required is to be kept, depending on the risk or threat in question, and for a limited period of time that will be dictated by the nature of the information stored. In any event, retention must not provide a detailed *mapping* of the private lives, habits, behaviour and social relations of the persons concerned.

(b) Conditions governing access by the public authorities to retained data

128. In my opinion, the conditions set out in the judgment in *Tele2 Sverige and Watson* [88] are still relevant in relation to access too: the national legislation must lay down the substantive and procedural conditions governing access by the competent authorities to retained data. [89]

129. The Belgian Government states that Article 126(2) of the 2005 Law (on electronic communications) [90] stipulates restrictively the national authorities that may receive data stored in accordance with paragraph 1 of that article.

130. Those authorities include the judiciary itself and the Public Prosecutor's Office; the State security forces; the general intelligence and security services, under the supervision of their respective independent commissions; the judicial police officers attached to the Belgian Institute for Postal Services and Telecommunications; the emergency services; the judicial police officers attached to the Missing Persons Unit of the Federal Police; the Telecommunications Ombudsman; and the supervisory body for the financial sector.

131. In general, the Belgian Government states that the domestic legislation does not allow the various services to have access to data in order to engage in the active pursuit of threats which are unidentified or unsupported by specific evidence. The national authorities could not therefore simply access raw communications data and process them automatically in order to obtain information and actively avert security risks.

132. According to the Belgian Government, access to data is subject to strict conditions, depending on the status of each of the competent national authorities.

88 See point 60 of this Opinion.

89 Judgment in *Tele2 Sverige and Watson*, paragraph 118.

90 Article 126, as amended by the Law of 29 May 2016.

133. The answer to the first question referred does not, in my opinion, require the Court to carry out an exhaustive analysis of the conditions under which each of those authorities may obtain retained data. That task falls rather to the referring court, which must carry it out in the light of the guidance contained in the case-law in *Tele2 Sverige and Watson* and *Ministerio Fiscal*.

134. Furthermore, according to the information provided by the Belgian Government, there are notable differences between the conditions of access applicable to the judicial authorities and the Public Prosecutor's Office,[91] for the purposes of the investigation, detection and prosecution of criminal offences under Articles 46*bis*[92] and 88*bis*[93] of the Code of Criminal Procedure, and those applicable to other authorities.

135. As regards the intelligence and security services, the 1998 Law provides that requests for access to traffic and location data held by operators must be based on objective criteria, in order to ensure that they are confined to what is strictly necessary, and a previously identified threat.[94] Various access periods (6, 9 or 12 months) are available, depending on the potential threat, and requests must comply with the principles of proportionality and subsidiarity. Provision is also made for a supervisory mechanism operated by an independent authority.[95]

136. As regards the judicial police officers attached to the Belgian Institute for Postal Services and Telecommunications (BIPT), although they may access data held by telecommunications operators, under the supervision of the Public Prosecutor's Office, in a very limited number of specific cases,[96] their activities, according to the Belgian Government, do not extend to the persons whose data are retained.

137. Emergency services that provide on-site assistance are permitted to request data relating to the person having made an emergency call in the case where, after receiving such a call, they cannot obtain identification data for that person from the provider or operator, or where those data are incomplete or incorrect.

138. The judicial police officers attached to the Missing Persons Unit of the Federal Police may ask the operator for the data necessary to find a missing person whose physical integrity is in imminent danger. Access, which is subject to strict conditions, is confined to data that can be

91 The suitability of the Public Prosecutor's Office for issuing measures of this kind is discussed in the reference for a preliminary ruling in Case C-746/18, *HK* v *Prokuratur*, pending.

92 The Public Prosecutor's Office is responsible for requesting identification data, by means of a reasoned, written decision (or a verbal decision in urgent cases) demonstrating that the measure is proportionate in relation to respect for privacy and subsidiary to any other investigative obligation. In the case of offences that do not carry a principal penalty of one year's imprisonment or a more serious penalty, the Public Prosecutor's Office may only ask for data in respect of a period of six months prior to its decision.

93 Responsibility for asking operators to track electronic communications or retained traffic and location data lies with the investigating judge, who may grant that measure if there are strong indications of the commission of an offence punishable by certain penalties, in the form of a reasoned, written decision (or a verbal decision in urgent cases) subject to the same requirements of proportionality and subsidiarity as apply to the Public Prosecutor's Office. There are some exceptions where the measure is directed against certain protected professional categories (lawyers or doctors, for example).

94 The decision must set out, as the case may be, the natural or legal persons, or de facto associations or groups, objects, locations, events or information subject to the specific method. It must also explain the relationship between the purpose of the data requested and the potential threat warranting this particular method.

95 The Administrative Commission for the Supervision of Specific and Exceptional Methods of Data Collection by the Intelligence and Security Services (BIM Commission) and the Standing Committee for Supervision of the Intelligence Services (R Committee). The Belgian Government states that the BIM Commission is responsible for monitoring the search methods employed by the intelligence and security services, over which it exercise first-line scrutiny. That commission, made up of judges, carries out its work on an entirely independent basis. Second-line scrutiny is undertaken by the R Committtee.

96 Access is permitted for the purposes of the investigation, detection and prosecution of offences under Article 114 (network security), 124 (confidentiality of electronic communications) and 126 (retention of, and access to, data) of the Law of 13 June 2005 on electronic communications.

used to identify the user, data relating to terminal access and connection to the network and the service, and data relating to the location of such equipment, and is restricted to data stored in the 48 hours prior to the request.

139. The Telecommunications Ombudsman may only request data identifying a person who has misused an electronic communications network or service. In this instance, there is no prior scrutiny by a judicial or independent administrative authority (separate from the ombudsman service itself).

140. Finally, for the purposes of combating financial crime, the supervisory body for the financial sector may obtain access to traffic and location data, subject to prior authorisation from the investigating judge.

141. The foregoing description of the forms and conditions of access to retained data by which each of the authorities permitted to obtain such data are bound reveals a variety of scenarios and safeguards the specific consistency of which with the criteria employed by the Court in its case-law [97] is a matter for the referring court.

142. I note, for example, that the legislation at issue does not appear to impose on the competent national authorities a duty systematically to inform the persons concerned (other than in cases where such information would jeopardise the investigations in progress) that their data have been consulted. It would also seem, at least in some cases such as financial offences, that there are no pre-determined rules on the seriousness of such offences that would warrant access to the relevant data. The relationship between the extent of the interference and the seriousness of the offence under investigation, within the meaning of the judgment in *Ministerio Fiscal*, is not made apparent in every scenario.

143. In any event, I am of the view that considerations in connection with the authorities' access to data take second place when, as is apparent from the foregoing, it is the general and indiscriminate retention of those data itself which is the main reason why the national legislation with which this reference is concerned is not consistent with EU law.

4. The third question referred

144. The Cour constitutionnelle (Constitutional Court) wishes to ascertain whether, in the event that, in the light of the answer given by the Court, the national legislation is declared incompatible with EU law, the effects of that legislation could be provisionally maintained. This would avoid any legal uncertainty and allow data obtained and retained to continue to be used in the interests of the objectives pursued.

145. It is settled case-law that 'the Court alone may, exceptionally and for overriding considerations of legal certainty, grant a provisional suspension of the ousting effect which a rule of EU law has on national law that is contrary thereto'. If 'national courts had the power to give national provisions primacy in relation to EU law contrary to those national provisions, even provisionally, the uniform application of EU law would be damaged'. [98]

97 I refer to point 60 of this Opinion.

98 Judgment of 28 July 2016, *Association France Nature Environnement* (C-379/15, EU:C:2016:603, paragraph 33).

146. The Commission takes the view that, since the Court did not limit the temporal effects of the interpretation of Article 15(1) of Directive 2002/58, the answer to the referring court's third question must be in the negative. [99]

147. However, in the judgment of 28 February 2012, *Inter-Environnement Wallonie and Terre wallonne*, [100] the Court held that, given the existence of an overriding consideration relating to the protection of the environment, a national court could exceptionally be authorised to apply the national provision empowering it to maintain certain effects of a national measure annulled in consequence of the infringement of a rule of EU law. [101]

148. That line of case-law was confirmed by the judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen*. [102] Whether it is adopted in the context of environmental protection or based on the security of electricity supply, I can see no reason why it should not be applied in other areas of EU law, in particular that with which we are concerned here.

149. If an 'overriding consideration relating to the protection of the environment' may, exceptionally, be a justification for the national courts to maintain certain effects of a domestic provision incompatible with EU law, this is because protection of the environment constitutes 'one of the essential objectives of the European Union and is both fundamental and cross-cutting in nature'. [103]

150. Now, the European Union also counts among its objectives the establishment of an area of security (Article 3 TEU), including respect for essential State functions, in particular maintaining law and order and safeguarding national security (Article 4(2) TEU). This is an objective no less 'cross-cutting and fundamental' than protection of the environment, since its attainment is a necessary precondition for the creation of a legislative framework capable of guaranteeing the effective enjoyment of fundamental rights and freedoms.

151. To my mind, overriding reasons relating to the protection of national security could provide a justification in this case for the Court, exceptionally, to authorise the referring court to maintain at least some of the effects of the law at issue.

152. In order to maintain those effects, the referring court would be required, in the light of the ruling given by the Court, to consider the domestic legislation incompatible with EU law and to find that the repercussions which the immediate annulment of that legislation (if annulment were the consequence of such incompatibility in national law) or its non-application might have for public security or State security would be extremely disruptive.

99 Paragraph 100 of the Commission's written observations.

100 Case C-41/11, EU:C:2012:103.

101 Judgment of 28 February 2012, *Inter-Environnement Wallonie and Terre wallonne* (C-41/11, EU:C:2012:103, paragraph 58). In the judgment of 28 July 2016, *Association France Nature Environnement* (C-379/15, EU:C:2016:603, paragraph 34), the Court inferred from that statement that 'the Court intended to afford, case by case and by way of exception, a national court the power to restructure the effects of annulment of a national provision held to be incompatible with EU law'.

102 Case C-411/17 (EU:C:2019:622, paragraph 178).

103 Judgment of 28 February 2012, *Inter-Environnement Wallonie and Terre wallonne* (C-41/11, EU:C:2012:103, paragraph 57).

153. The provisional maintenance (of all or part) of the effects of the national legislation would also require:

– that that extension have as its purpose the avoidance of a legislative vacuum the effects of which would be as harmful as those arising from applying the contested legislation, which it would be impossible to fill by other means and which would have the consequence of divesting the national authorities of a valuable tool in ensuring State security; and

– that that state of affairs last only for the period of time strictly necessary to adopt the measures enabling the incompatibility with EU law which has been established to be remedied. [104]

154. Other factors that are conducive to the above approach are the difficulty of bringing national laws into line with the case-law established in *Tele2 Sverige and Watson* [105] and the fact that the Belgian legislature made clear its intention by amending its own legislation in order to comply with the judgment in *Digital Rights*. That precedent suggests that it will also amend the Law of 29 May 2016 (enacted prior to the delivery of the judgment in *Tele2 Sverige and Watson*) in accordance with the case-law established in the latter judgment.

V. Conclusion

155. In the light of the foregoing, I propose that the Court's answer to the Cour constitutionnelle (Constitutional Court, Belgium) should be as follows:

(1) Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), read in conjunction with Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that:

– It precludes national legislation which imposes on operators and providers of electronic communications services an obligation to retain, on a general and indiscriminate basis, the traffic and location data of all subscribers and users materialising in the context of all means of electronic communications.

– The foregoing is not affected by the fact that that national legislation has as its objectives not only the investigation, detection and prosecution of offences, whether serious or otherwise, but also the safeguarding of national security, defence of the territory and public security, prevention of the unauthorised use of the electronic communications system and any other objective provided for in Article 23(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

– Nor is the foregoing affected by the fact that access to retained data is subject to precisely regulated safeguards. It is for the referring court to ascertain whether the national legislation governing the conditions of access to retained data by the competent authorities limits such access to specific cases the seriousness of which makes interference

104 Judgment of 28 February 2012, *Inter-Environnement Wallonie and Terre wallonne* (C-41/11; EU:C:2012:103, paragraph 62).

105 Paragraph 45 of the Danish Government's written observations.

essential; makes such access conditional upon prior scrutiny (other than in cases of emergency) by a court or independent administrative authority; and provides that the persons concerned must be informed of such access, provided that this disclosure does not jeopardise the actions of those authorities.

(2) Articles 4 and 6 of the Charter of Fundamental Rights do not have a bearing on the interpretation of Article 15(1) of Directive 2002/58, read in conjunction with the other articles of that Charter as mentioned above, such as to make it impossible to determine the incompatibility with EU law of national legislation such as that at issue in the main proceedings.

(3) A national court may, if its domestic law so permits, maintain the effects of legislation such as that at issue in the main proceedings, on an exceptional and temporary basis, even where that legislation is incompatible with EU law, if maintaining those effects is justified by overriding considerations relating to threats to public security or national security that cannot be addressed by other means or other alternatives. Those effects may be maintained only for as long as is strictly necessary to correct the aforementioned incompatibility with EU law.