Case C-520/18

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

2 August 2018

Referring court:

Cour constitutionnelle (Belgium)

Date of the decision to refer:

19 July 2018

Applicants:

Ordre des barreaux francophones et germanophone

Académie Fiscale ASBL

UA

Liga voor Mensenrechten ASBL

Ligue des Droits de l'Homme ASBL

VZ

WY

XX

Defendant:

Conseil des ministres (Belgian Government)

I. Subject matter and context of the main proceedings

1 The Ordre des barreaux francophones et germanophone (Order of French-speaking and German-speaking Bars) ('the OBFG'), the not-for-profit association 'Académie Fiscale', the not-for-profit association 'Liga voor Mensenrechten' and the not-for-profit association 'Ligue des Droits de l'Homme', and a number of

natural persons, have brought an action before the Cour constitutionnelle de Belgique (Constitutional Court, Belgium) ('the referring court') for annulment of the Law of 29 May 2016 on the collection and retention of data in the electronic communications sector (*Moniteur belge*, 18 July 2016, p. 44717) ('the contested law'). Those cases have been joined.

2 The contested law amends various provisions of the Law of 13 June 2005 on electronic communications (*Moniteur belge*, 20 June 2005, p. 28070) ('the Law of 13 June 2005'), the Code of Criminal Procedure ('the Code of Criminal Procedure') and the Institutional Law of 30 November 1998 on the intelligence and security services (*Moniteur belge*, 18 December 1998, p. 40312) ('the Law of 30 November 1998').

3 By the Law of 30 July 2013 amending Articles 2, 126, and 145 of the Law of 13 June 2005 on electronic communications and Article 90*decies* of the Code of Criminal Procedure (*Moniteur belge*, 23 August 2013, p. 56109) ('the Law of 30 July 2013), the Kingdom of Belgium had partially transposed into Belgian law Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54) and 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 (OJ 2002 L 201, p. 37) (Directive on privacy and electronic communications).

4 By its judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238) ('the judgment in *Digital Rights Ireland and Others*'), the Court declared Directive 2006/24 invalid.

5 The referring court, by judgment No 84/2015 of 11 June 2015, annulled Article 126 of the Law of 13 June 2005, as amended by the Law of 30 July 2013, on the same grounds as those on which the Court had declared Directive 2006/24 invalid.

6 By the contested law, the Belgian legislature intended to respond to the annulment of that provision.

II. Subject matter and legal basis of the request for a preliminary ruling

7 The contested law amends the Law of 13 June 2005, which transposes a number of directives, including Directive 2005/58, into Belgian law.

III. Legal framework of the questions for a preliminary ruling

1. European Union law

A. The EU Treaty

8 Article 5(4) of the TEU provides:

‘Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.

The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality’.

9 Article 6 TEU provides:

‘1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.

The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.

The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.

2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties. …’

B. The Charter of Fundamental Rights of the European Union

10 Article 4 of the Charter provides:

‘Prohibition of torture and inhuman or degrading treatment or punishment

No one shall be subjected to torture or to inhuman or degrading treatment or punishment’.

11 Article 6 of the Charter provides:

‘Right to liberty and security

Everyone has the right to liberty and security of person’.

12 Article 7 of the Charter provides:

‘Respect for private and family life

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

13 Article 8 of the Charter provides:

‘Protection of personal data

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

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

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

14 Article 11 of the Charter provides:

‘Freedom of expression and information

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected’.

15 Article 47 of the Charter provides:

‘Right to an effective remedy and to a fair trial

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.’

16 Article 52 of the Charter provides:

‘Scope of guaranteed rights

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others' ….

C. Directive 2002/58

17 Article 15(1) of Directive 2002/58 provides:

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

D. Regulation (EU) 2016/679

18 Article 95 of Regulation 2016/679 provides:

'Relationship with Directive 2002/58/EC

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

2. Domestic law

19 The main provisions of the relevant national legislation, as amended by the contested law, are the following:

A. Law of 13 June 2005 on electronic communications

20 By virtue of the contested law, the Law of 13 June 2005 is worded as follows:

'…

Article 126

§ 1. Without prejudice to the Law of 8 December 1992 on the protection of private life with respect to the processing of personal data, providers to the public of telephony services, including via the internet, of internet access, of email via the internet, operators providing public electronics communications networks and operators providing one of those services shall retain the data referred to in paragraph 3 which are generated or processed by them in the context of the provision of the communications services concerned.

The present article shall not concern the content of the communications.

…

§ 2. Only the following authorities may, on a simple request, obtain from the providers and operators referred to in paragraph 1, subparagraph 1, data retained pursuant to this article, for the purposes and on the conditions listed below:

(1) the judicial authorities, for the detection, investigation and prosecution of offences, for the enforcement of the measures referred to in Articles 46bis and 88bis of the Code of Criminal Procedure and on the conditions determined by those articles;

(2) the 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 [Law of 30 November 1998] …;

(3) any senior law-enforcement officer of the Institute, for the detection, investigation and prosecution of offences contrary to the [rules on network security] and to this Article;

(4) the emergency services providing call-out assistance where, following an emergency call, they do not obtain the caller's identification data from the provider or the operator concerned … or obtain incomplete or incorrect data. Only the caller's identification data may be requested, by no later than 24 hours after the call;

(5) the senior law-enforcement office of the Missing Persons Unit of the Federal Police, in the framework of his task of providing assistance to a person in danger, seeking persons whose disappearance gives cause for concern and where there are serious presumptions or indicia that the physical integrity of the missing person is in imminent danger. Only the data referred to in paragraph 3, subparagraphs 1 and 2, relating to the missing persons and retained during the 48 hours preceding the request for data may be requested from the operator or provider concerned via a supervisory service designated by the King;

(6) the Telecommunications Ombudsman, for the purpose of 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 paragraph 1, subparagraph 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 immediately and only to the authorities referred to in this paragraph.

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

§ 3. The data intended to identify the user or subscriber and the means of communication, to the exclusion of the data specifically referred to in paragraphs 2 and 3, shall be retained for 12 months from the date from which communication is possible for the last time with the assistance of the service used.

The data relating to access and the connection of the terminal device to the network and the service and to the location of that device, including the network termination point, shall be retained for 12 months from the date of the communication.

The communication data, apart from the content, including their origin and their destination, shall be retained for 12 months from the date of the communication.

The King shall fix, by decree deliberated in the Council of Ministers, on a proposal from the Justice Minister and the Minister, and after receiving the opinion of the Committee for the Protection of Privacy and the Institute, the data to be retained by type of categories referred to in paragraphs 1 to 3 and the requirements which those data must satisfy.

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

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

(2) ensure that the data retained are the subject of appropriate technical and organisational measures in order 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 retained data in response to the requests of the authorities referred to in paragraph 2 is given only by one or more members of the Coordination Unit referred to in Article 126/1, § 1;

(4) retain the data on the territory of the European Union;

(5) implement technological protection measures that render the retained data, immediately they are recorded, illegible and incapable of being used by any person who is 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 fixed in paragraph 3, without prejudice to Articles 122 and 123;

(7) ensure the traceability of the use of the retained data for each request to obtain those data submitted by an authority referred to in paragraph 2.

The traceability referred to in paragraph 1(7) shall be effected with the help of a log. The Institute and Committee for the Protection of Privacy shall conclude into a collaboration agreement on consultation and inspection of the content of the journal.

…

Article 126/1

§ 1. Within each operator, and within each provider referred to in Article 126, § 1, subparagraph 1, a Coordination Unit shall be set up, responsible for providing the legally authorised Belgian authorities, at their request, with the data retained pursuant to Articles 122, 123 and 126, the caller identification data pursuant to Article 107, § 2, subparagraph 1, or the data which may be requested pursuant to Articles 46bis, 88bis and 90ter of the Code of Criminal Procedure and Articles 18/7, 18/8, 18/16 and 18/17 of the [Law of 30 November 1998].

….

Only the members of the Coordination Unit may respond to the authorities' requests relating to the data referred to in subparagraph 1. They may however, under their supervision and within the limits of what is strictly necessary, obtain technical assistance from officers of the operator or the provider.

The members of the Coordination Unit and the officers providing technical assistance shall be subject to professional privilege.

Each operator and each provider referred to in Article 126, § 1, subparagraph 1 shall ensure the confidentiality of the data processed by the

Coordination Unit and shall communicate forthwith to the Institute and the Committee for the Protection of Privacy the details of the Coordination Unit and its members and also any change to those data.

§ 2. Each operator and each provider referred to in Article 126, § 1, subparagraph 1 shall establish an internal procedure for responding to requests by the authorities for access to personal data concerning users. It shall make available to the Institute, on request, information concerning those procedures, the number of requests received, the legal basis relied on and the operator's or provider's response.

…

§ 3. Each provider and each operator referred to in Article 126, § 1, subparagraph 1 shall designate one or more personal data protection officers, who must meet all the conditions set out in paragraph 1, subparagraph 3.

This officer may not be part of the Coordination Unit.

…

In carrying out his tasks, the personal data protection officer shall act in complete independence, and shall have access to all the personal data transmitted to the authorities and also to all the relevant premises of the provider or operator.

The performance of his tasks cannot entail disadvantages for the officer. In particular, he may not be dismissed or replaced as officer because of the performance of the tasks entrusted to him, without detailed reasons being provided.

The officer must be able to communicate directly with the management of the operator or provider.

The data protection officer shall ensure that:

(1) the processing carried out by the Coordination Unit is carried out in accordance with the law;

(2) the provider or operator collects and retains only the data which it can lawfully retain;

(3) only the authorities authorised by law have access to the retained data;

(4) the personal data security and protection measures described in this Law and in the security policy of the provider or operator are implemented.

Each provider and each operator referred to in Article 126, § 1, subparagraph 1 shall communicate forthwith to the Institute and the

Committee for the Protection of Privacy the details of the personal data protection officer, and any change to those data.

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

…

(2) the requirements which the Coordination Unit must satisfy, taking into account the situation of operators and providers which receive few requests from the judicial authorities, have no establishment in Belgium or operate mainly abroad;

(3) the information to be provided to the Institute and the Committee for the Protection of Privacy pursuant to paragraphs 1 and 3 and the authorities which are to have access to that information;

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

Article 127:

§ 1. The King, after receiving the opinion of the Committee for the Protection of Privacy and the Institute, shall determine the technical and administrative measures which are to be imposed on the operators and providers referred to in Article 126, § 1, subparagraph 1, or on end users, in order to permit:

(1) calling-line identification in the context of an emergency call;

(2) end-user identification, tracking, location, tapping, monitoring, and recording of private communications in the conditions laid down in Articles 46bis, 88bis and 90ter to 90decies of the Code of Criminal Procedure and in the [Law of 30 November 1998].

…

§ 2. The following shall be prohibited: the supply or use of a service or a device which makes it difficult or impossible to carry out the operations referred to in § 1, with the exception of encryption systems that may be used in order to ensure the confidentiality of communications and the security of payments.

…

Article 145

§ 1. Any person who breaches Articles … 126, 126/1, 127 and the decrees adopted pursuant to Articles … 126, 126/1 and 127 shall be liable to a fine of between EUR 50 and EUR 50 000.

…’.

B. Code of Criminal Procedure

21 By virtue of the contested law, the Code of Criminal Procedure is worded as follows:

‘…

Article 46 bis

§ 1. In investigating serious offences and less serious offences, the Crown Prosecutor’s Office may, by a reasoned decision in writing, requiring, if necessary, the assistance of an operator of an electronic communications network as an electronic communication service provider or a police department designated by the King, and on the basis of any data retained by it, or by means of access to the files of the customers of the operator or service provider, obtain or have obtained:

(1) the identification of the subscriber or habitual user of an electronic communication service or of the means of electronic communications used;

(2) the identification of the electronic communication services to which a specific person subscribes or which are habitually used by a specific person.

The reasons stated shall reflect the fact that the measure is proportionate, having regard to respect for private life, and subsidiary to any other duty of investigation.

In the case of extreme urgency, any officer of the criminal police may, with the prior oral agreement of the Crown Prosecutor’s Office and by a reasoned decision in writing, require those data. The officer of the criminal police shall send, within 24 hours, that reasoned decision in writing and the information obtained to the Crown Prosecutor’s Office and 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’s Office, or, in extremely urgent cases, the officer of the criminal police, may request the data referred to in subparagraph 1 only in respect of a period of six months preceding his decision. …

§ 2. All operators of an electronic communication network and all electronic communication service providers required to provide the data referred to in the first paragraph shall provide the data required to the Crown Prosecutor's Office or the officer of the criminal police within a period to be fixed by the King…

…

Any person who, in performance of his duties, knows of the measure or assists with it shall maintain its confidentiality. All breach of confidentiality shall be penalised in accordance with Article 458 of the Criminal Code.

A refusal to provide the data shall be penalised by a fine of between EUR 26 and EUR ten thousand.

Article 88 bis

§ 1. Where there is strong circumstantial evidence that the offences are of such a kind 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 render the tracking of electronic communications or the location of the origin or the destination of electronic communications necessary for the establishment of the truth, he may order, requiring, if necessary, directly or via the police department designated by the King, the technical assistance of the operator of an electronic communication network or the electronic communication service provider:

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

(2) the location of the origin or the destination of electronic communications.

In the cases referred to in subparagraph 1, for each means of electronic communications the data of which are tracked, or the origin or destination of the telecommunication of which is located, the day, hour, duration and, if necessary, the 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 justify the measure, and that it is proportionate having regard to respect for private life, and subsidiary to any other duty of investigation, in a reasoned order.

He shall also specify the period during which the measure may be applied for the future; such period shall not exceed two months from the order,

without prejudice to renewal and, where appropriate, the period in the past over which the order extends in accordance with paragraph 2.

…

§ 2. As regards the application of the measure referred to in paragraph 1, subparagraph 1 to the traffic or location data retained on the basis of Article 126 of the Law of 13 June 2005 on electronic communications, the following provisions shall apply:

- for an offence referred to in Book II, Title I ter of the Criminal Code, the investigating judge may request in his order the data for a period of 12 months preceding the order;

- for another offence referred to in Article 90 ter, §§ 2 to 4, which is not referred to in the first indent, or for an offence committed in the framework of a criminal organisation referred to in Article 324 of the Criminal Code, or for an offence punishable by a custodial sentence of five years or a more severe penalty, the investigating judge may request in his order data for a period of nine months preceding the order;

- for other offences, the investigating judge may request data only for a period of six months preceding 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 suspected of having committed an offence referred to in paragraph 1 or of having participated in such an offence, or if specific facts suggest that third parties suspected of having committed an offence referred to in paragraph 1 use his means of electronic communication.

The measure may not be enforced unless the Chairman of the Bar or the representative of the Provincial Medical Association, as the case may be, is advised. Those persons shall be informed by the investigating judge of the matters which he deems to be covered by professional privilege. Those matters shall not be recorded in the report. Any person who, in the performance of his duties, knows of the measure or assists with it, shall maintain its confidentiality. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

…’

C. Law of 30 November 1998

22 By virtue of the contested law, the Law of 30 November 1998 is worded as follows:

‘…

Article 13

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

The information contained in the documents must be connected with the purpose of the file and be limited to the requirements resulting therefrom.

The intelligence and security services shall ensure the security of the data connected with their sources and those of the information and the personal data supplied by those sources.

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

Article 18/3

§ 1. The specific data-gathering methods referred to in Article 18/2, § 1, may be implemented taking account 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 task to be gathered. The specific method must be chosen according to the degree of gravity of the potential threat in respect of which it is employed.

The specific method may be employed only after a reasoned decision in writing from the director of the service and after notification of that decision to the Committee.

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

(1) the nature of the specific method;

(2) depending on the case, the natural or legal persons, the associations or groups, the objects, the places, the events or the information subject to the specific method;

(3) the potential threat that justifies the specific method;

(4) the factual circumstances that justify the specific method, the reasoning in relation to subsidiarity and proportionality, including the link between (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 serious indicia showing that the lawyer, doctor or journalist is participating or has participated personally and actively in the origination or the development of the potential threat;

(10) where Article 18/8 is applied, the grounds for the duration of the period during which the collection of data applies;

…

§ 8. The director of the service shall terminate the specific method when the potential threat that justified has ceased to exist, when the method is no longer of use for the purpose for which it had been employed, or when he has found an illegality. He shall inform the Committee of his decision as soon as possible. …

Article 18/8

§ 1. The intelligence and security services may, in the interest of performing their tasks, as necessary and requesting for that purpose the technical assistance of an electronic communication network or the provider of an electronic communication network, order:

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

(2) the location of the origin or the destination of electronic communications.

…

§ 2. As regards the application of the method referred to in paragraph 1 to the data retained on the basis of Article 126 of the Law of 13 June 2005 on electronic communications, 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 request in his decision only the data for a period of six months preceding the decision;

(2) for a potential threat other than those referred to in [paragraphs] (1) and (3), the director of the service may request in his decisions the data for a period of nine months preceding 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 request in his decision the data for a period of 12 months preceding the decision. …'.

IV. Other provisions and principles relied on by the parties or cited in the grounds of the order of the referring court

23 Apart from the provisions cited above, the following provisions and principles are relied on by the parties or cited in the grounds of the order of the referring court:

– Articles 5, 6, 8, 9, 10, 11, 14, 15, 17 and 18 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950 ('the ECHR');

Article 17 of the International Covenant on Civil and Political Rights, concluded in New York on 16 December 1966 ('the Covenant');

– Article 2(a) and Article 13(1) of Directive 95/46/EC 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);

– Articles 10, 11, 12, 15, 19, 22, 29 and the first subparagraph of Article 151(1) of the Belgian Constitution;

– the general principles of legal certainty, proportionality, legality in criminal matters, reasonableness, the presumption of innocence, the right to a fair hearing, professional privilege, equal treatment of citizens and self-determination in relation to information.

VI. The parties' essential arguments

1. The applicants' submissions

24 The applicants rely on the infringement of several articles of the Constitution, whether or not in conjunction with several articles of the EU Treaty, of the Charter, of Directive 2002/58 and other provisions of EU law, with several provisions of the ECHR, Article 17 of the Covenant and with the general principles of law.

25 The contested law places on electronic communications operators a general obligation to retain users' traffic and location data for certain periods. The contested law also covers access to those data by the judicial authorities and the intelligence and security services.

– *(i) The obligation to collect and retain data*

26 The applicants complain that the contested law treats in the same way, without justification, the users of telecommunications or electronic communications services who are subject to professional privilege, including, in particular, lawyers, and other users of those services, without taking account of the particular

status of lawyers, the fundamental nature of the professional privilege to which lawyers are subject and the necessary relationship of trust that must exist between lawyers and their clients, or of the particular status of accountants and tax professionals, of the fundamental nature of the professional privilege to which they are subject or of the necessary relationship of trust that must exist between them and their clients, or, last, of the obligations of confidentiality borne by other persons who are not subject to professional privilege in the strict sense.

27 The discriminatory situation created by the contested law is as harmful to lawyers as to private individuals, as the lawyer's professional privilege is of general interest. Anyone who consults a lawyer in confidence must be certain that the existence and the circumstances of that consultation and the secrets entrusted to his counsel will not be revealed or used against him. The principle of the lawyer's professional privilege directly affects the right to a fair hearing and the right to respect for private life. There can therefore be a breach of that principle only in exceptional cases, subject to compliance with appropriate and sufficient guarantees against misuse.

28 Even if the data gathered do not relate to the content of the communications, they make it possible to create a real digital identity card of the person concerned. It will thus be possible to determine whether a person suspected of having committed an offence has contacted a lawyer, to know the date, time and duration of the communication, and the communication devices used, the place where the mobile equipment was used, etc. Those data are even more specific than the data recorded in a lawyer's professional diary, which is none the less a confidential document.

29 The failure to distinguish between persons whose communications are subject to professional privilege and others was criticised by the Court in the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970) ('the judgment in *Tele2 Sverige and Watson and Others*').

30 From a technical aspect, it would be simple to distinguish between ordinary metadata and those relating to a person holding professional secrets, by means of a filtering mechanism on entry. In fact, the legislature could compel operators to take note of the fact that some of their customers hold professional secrets and to share that information among them. Thus, operators would not place the metadata generated by lawyers' communications and those of other persons whose activities are covered by professional privilege in the databases which they create.

31 Furthermore, no provision is made for any control mechanism that would enable those whose activities are covered by professional privilege and those benefiting from professional privilege to object to the collection, retention or checking of data covered by professional privilege. The checking of the data, even if those data are not subsequently produced in support of a case, is sufficient to undermine professional privilege. The rights guaranteed by Article 6 of the ECHR and by

Article 47 of the Charter are not respected, since the contested law does not provide for any judicial oversight.

32 In addition, the contested provisions treat in the same way individuals who are under investigation or facing prosecution for offences liable to give rise to criminal convictions and those who are not. Criminal law relies on the principle of the presumption of innocence, with the corollary that the burden of proof is borne by the prosecution and that any doubt operates in favour of the accused. It is therefore not relevant to claim that the measure may just as equally benefit the victim of an offence. Thus, the retention obligations which the contested law imposes are excessive by reference to the objectives pursued by the legislature.

33 The general retention of data, including for persons who have no connection with crime, therefore constitutes a breach of the principle of proportionality. That breach is confirmed by the judgments of the Court in *Digital Rights Ireland and Others* and in *Tele2 Sverige and Watson and Others* and by the Opinion of Advocate General Cruz Villalón in Joined Cases *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2013:845), and also by judgment No 84/2015 of the referring court of 11 June 2015.

34 The general and indiscriminate retention of identification data, connection data and location data and personal communication data imposed by the contested law also constitutes an interference with the right to protection of private life which is not strictly necessary in a democratic society in order to safeguard national security, that is to say, the security of the State, national defence, public security or the prevention, investigation, detection and prosecution of criminal offences or the unauthorised use of the electronic communication system, as provided for in Article 13(1) of Directive 95/46.

35 In the judgment in *Tele2 Sverige and Watson and Others*, the Court held that EU law precluded national legislation which provided for the general and indiscriminate retention of data. On the assumption that such a general retention obligation cannot in itself be considered to exceed the limits of what is strictly necessary, it must be accompanied by all the guarantees to which the Court referred in the judgment in *Digital Rights Ireland and Others* and in the judgment in *Tele2 Sverige and Watson and Others*. Those guarantees are mandatory, cumulative and minimum (Opinion of Advocate General Saugmandsgaard Øe in Joined Cases *Tele2 Sverige and Others*, C-203/15 and C-698/15, EU:C:2016:572).

36 The data retention obligation laid down in the contested law corresponds largely to the data retention obligation provided for in Directive 2006/24, as the Court stated in paragraph 97 of the judgment in *Tele2 Sverige and Watson and Others*.

37 The general obligation to retain data laid down in the contested law therefore constitutes a particularly serious breach of the right to respect for private and family life and the right to protection of personal data. It also has an impact on the use of means of electronic communication and therefore on the way in which

users of those means of communication make use of their freedom of expression. It also results in a violation of the international and constitutional provisions which safeguard that freedom of expression. In view of the gravity of the breach of those fundamental rights, only the fight against serious crime could justify that measure. However, the fight against serious crime cannot in itself justify the general and indiscriminate retention of all traffic data and all location data (judgment in *Tele2 Sverige and Watson and Others*, paragraph 103). That would mean that the retention of those data would become the rule, whereas, according to Directive 2002/58, the prohibition of the retention of those data is the rule, while their retention is an exception. In addition, the judgment in *Tele2 Sverige and Watson and Others* concerns any national legislation aimed at the fight against crime that imposes a general obligation to retain data, and not only the fight against serious crime. Although any citizen may be encounter that type of crime as an accused, a victim or a witness, the legislation at issue falls within the scope of Article 15 of Directive 2002/58. The judgment in *Tele2 Sverige and Watson and Others* is therefore applicable.

38 In the judgment in *Tele2 Sverige and Watson and Others*, the Court made clear that national legislation permitting the targeted retention of traffic and location data for the purpose of fighting serious crime could be accepted to the strictly limited extent set out in that judgment. The legislature asserts in the *travaux préparatoires* that such a targeted retention would be impossible. The Belgian State's reasoning is based in reality on a political will to pursue at any price the route of general retention of those data on the pretext of a context of the risk of terrorism and in spite of the unconstitutionality of the general surveillance system put in place. If it is accepted that it is impossible in reality to determine at the outset categories of persons who would not be liable to be concerned by or involved in serious offences, that cannot justify such a serious interference with the private life of citizens. The logical consequence should be not to put such a measure in place.

39 Last, while the statement of reasons on which the law is based refers to the importance of communication data for the investigation of terrorism, child pornography, drug trafficking, the sale of counterfeit medicinal products on the internet, the incitement to hatred or violence, harassment, the hacking of bank accounts and identity theft, a number of studies question the need for a general retention obligation for the purposes of the fight against serious crime (Opinion of Advocate General Saugmandsgaard Øe in Joined Cases *Tele2 Sverige and Others*, C-203/15 and C-698/15, EU:C:2016:572).

40 In the alternative, the applicants claim that the judgment in *Digital Rights Ireland and Others* may be interpreted in two ways: according to the first interpretation, the unlawfulness of the general and indiscriminate data retention obligation is the result of the absence of sufficient guarantees relating to access to the retained data and to the retention period; and according to the second interpretation, the retention obligation is unlawful, precisely because of its general and indiscriminate nature. The statement of reasons on which the law is based also

recognises that the general and indiscriminate data retention obligation did not comply with that judgment but considers that that may be offset by stricter legislation concerning the other aspects, namely differentiation according to the categories of retained data and the usefulness of those data, rules relating to access by the authorities to the data concerned and rules on the data security within the operators. It must therefore be stated that the general data retention obligation also fails to correspond to the flexible interpretation which has been made of that judgment owing to the absence of guarantees to limit the interference to what is strictly necessary.

41 Indeed, the operators already retain data for billing purposes. However, the contested law prohibits them from using the data retained pursuant to that law for purposes other than those provided for in the law, therefore including the use of those data for the purpose of billing for their services. In addition, the contested law requires them to retain elements which they would not retain, not in that form and, in any event, not for the same period.

42 In addition, there is an appreciable risk that the relevant databases will be managed in a casual fashion by reluctant operators in view of the monitoring which that new obligation entails.

43 There is no independent authority to monitor compliance by the operators with the level of safeguarding and protection of the retained data. The responsible persons designated by the contested law in that respect are all members of the operators' staff, who are in a subordinate position.

44 In addition, the contested law allows operators to transfer data collected for retention purposes and for reasons of sub-processing to other Member States of the European Union in spite of the sensitive and confidential nature of certain data, which considerably increases the risk that third parties will have access to those data or that the data will be disclosed. In addition, the national legislation applicable in other Member States, for example the French legislation, authorises the intelligence services to obtain information from operators about the data which they handle.

– *(ii) The retention period*

45 As regards the retention period, the contested law provides in essence that that period is to be 12 months, which in itself is excessive. Admittedly, for offences which are not of such a kind as to entail a custodial sentence of one year or more, the data requested can relate only to the six months preceding the request. However, those offences are few in number.

46 Nor are the starting parts of the retention period related to the circumstances that may justify the retention. Furthermore, the identification data may de facto be retained for a much longer period than 12 months, since the retention period

begins to run on 'the date from which a communication is possible for the last time with the assistance of the service used'.

47 Other European countries apply shorter retention periods. The applicants refer to a judgment of the German Constitutional Court which annulled the German law on data retention and also to the judgment in *Digital Rights Ireland and Others*.

48 The data retention period is also open to criticism in that it is the same for all categories of data, whereas a distinction should be drawn according to the categories of data, their usefulness for the aim pursued or the persons concerned and provided that the period is limited to what is strictly necessary. That equal treatment of unequal categories of retained data is not reasonably justified and is therefore discriminatory.

49 Last, the contested law does not require the authority which has had access to data to destroy those data if they have no connection with the aim for which they were gathered or where they are no longer strictly necessary for the fight against serious crime.

– *(iii) Access to the data*

50 The contested law allows six different authorities to access the retained data instead of strictly limiting that access to the authorities involved in the fight against crime, at least against serious crime.

51 The contested law allows the authorities to access the retained data without that access being limited to serious crime. The additional guarantees provided for by the contested law in matters of professional privilege do not apply to persons subject to professional privilege other than lawyers, doctors and journalists. However, Article 458 of the Criminal Code [a provision which requires respect for professional privilege] applies to more persons than those who practise those three professions. Furthermore, certain persons, authorities and organisations are not subject to professional privilege although communications with them should benefit from a certain confidentiality in application of other provisions. In addition, the Crown Prosecutor's Office is not a judicial authority or an independent administrative authority.

52 The contested law also allows the intelligence and security services to access the retained data. The sphere of action of those services has been defined too broadly. The communication data of all citizens may be requested, depending on the nature of the potential threat, for a period of six, nine or 12 months preceding the access decision. The contested law may therefore result in misuse of powers, to the detriment of individuals or organisations critical of the Government or the political system. The freedom of the press is also jeopardised by the fact that the intelligence and security services may request all the telephone and internet communications of journalists. The contested law might also give rise to or reinforce self-censorship among citizens who have the vague feeling of being

monitored, which may affect the exercise of their freedom of opinion and to receive and impart information and may thus constitute an interference within the meaning of Article 11 of the Charter.

53 There is no precise description of the circumstances or the conditions relating to the grant of access. Nor is access subject to any substantive or procedural condition: providers are merely required to respond favourably to any request from the six designated authorities. However, in the judgment in *Tele2 Sverige and Watson and Others*, the Court stated that the national legislation must provide appropriate safeguards, that is to say, clear and precise rules indicating in what circumstances and under which conditions providers must grant the competent national authorities access. That judgment makes clear that as a general rule access can be granted 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. Access must also be subject to a prior review carried out either by a court or by an independent administrative body. Yet in the contested law no procedural rule is laid down and no authority has been designated to review the request to receive data. The only controls provided for are ex post facto controls.

54 Furthermore, the judgment in *Tele2 Sverige and Watson and Others* uses the expression 'serious risk to public security'. The contested law does not respect that criterion, since it refers to the normal and specific methods of the intelligence services and those methods relate to less serious breaches of security than special methods.

55 Last, the contested law imposes no obligation to warn individuals that access has been granted to their private data, which also deprives them of an efficient and effective remedy.

56 As regards the access period, the law establishes a distinction only as regards the nature of the offence and the threat but not as regards the nature of the retained data.

2. The Belgian State's submissions

57 The Council of Ministers contends that the contested law responds to the criticisms made by the Court and by the referring court concerning the legislation that was formerly applicable.

58 While lawyers' professional privilege is a matter of public policy, it is not absolute. The principle of proportionality 'must make it possible to assess the limits imposed by necessity or other principles or values that may conflict with that professional privilege'.

59 As regards access to data, the contested law lays down limits with respect to professional privilege, in particular lawyers' professional privilege. The law is

aimed only at metadata, to the exclusion of the content of communications. It therefore does not really affect the confidentiality of exchanges between a lawyer and his client. On the contrary, it would be disproportionate to allow communications to and from those practising in of professions subject to professional privilege to escape the legal provisions entirely. The fact that an email address is used by a person whose activities are covered by professional privilege does not mean that all the messages to or from that address are actually protected by professional privilege. Those whose activities are covered by professional privilege are themselves capable of committing serious offences.

60 As regards the individuals who might no longer confide in their lawyer, the legislature has taken every precaution to ensure that the objective pursued, the legitimacy of which is not disputed, may be achieved without entailing a disproportionate breach of the right to private life and the right to a fair hearing.

61 As to whether or not the data should be retained, depending on whether or not the person concerned is one whose activities are covered by professional privilege, the *travaux préparatoires* of the law emphasised the technical difficulties of such solutions and the fact that other Member States of the European Union have been unable to find a technical formula for differentiation. In addition, such differentiation would not protect professional privilege itself so much as the actual person with whom, because of his profession, secrets are deposited. That differentiation would have the effect of excluding from the scope of the law not only what is covered by professional privilege but also what is not at all covered, on the pretext that the information gathered would use the same channel as the information covered by professional privilege.

62 As regards the absence of any possibility of appeal against the decision prescribing the measure allowing consultation of the retained data and also of the measures adopted on the basis of that decision, access to the retained data is in fact subject to judicial review in the context of the criminal investigation, which is carried out by the Commission BIM [administrative commission responsible for monitoring specific and exceptional data-gathering methods employed by the intelligence and security services], composed of independent law officers, where it is the intelligence services that have access to the information. The Crown Prosecutor's Office is indeed an independent body, since it exercises its investigative powers in the framework of the Code of Criminal Procedure and provides a guarantee that the exercise of its powers will not amount to an unreasonable breach of the right to protection of private life.

63 As regards the data retention period, the law provides, in relation to access, for a variation based in essence on the gravity of the offence. The retention obligation logically precedes access to the retained information. Only the request for access will allow the gravity of the offence or the threat to be determined. Since the law provides that access to the information concerned is to vary according to the gravity of the offence or the threat, it is difficult to determine in advance, for each category of information, how useful it will be for a particular investigation. Last,

the applicant does not indicate how the periods thus prescribed by law would in themselves be disproportionate.

64 The legislature examined all the possible ways of complying with the Court's case-law. A difference in treatment in the data retention period seemed impossible after a thorough examination of that question. It appeared that a period of 12 months is necessary in order to combat terrorist offences.

65 As regards the failure to distinguish between individuals according to whether or not they are the subject of investigation or prosecution, the operative part of the contested law specifically allows the investigators to access certain metadata relating to a person who is the subject of such an investigation. That assumes that those metadata have been retained before the investigation and therefore at a time when such a distinction could not be drawn.

66 As for the risk that operators will treat the data that have been retained in a casual manner, compliance with the operators' legal obligations is subject to review by the sectoral regulator, such review being accompanied by penalties which go as far as withdrawal of a licence. The contested law provides numerous guarantees in relation to data security.

67 No other preventive system could avoid data covered by professional privilege being retained and, where necessary, being accessed. In order to determine whether information is covered by professional privilege, it must necessarily first be processed.

68 The national legislation in Sweden and in the United Kingdom examined by the Court in its judgment in *Tele2 Sverige and Watson and Others* was aimed at the fight against serious crime, while the contested law has a wider objective. Consequently, the Court's finding that the national legislation was inappropriate or disproportionate by reference to the objective of fighting serious crime cannot be transposed *mutatis mutandis* to national legislation having a different objective.

69 Admittedly, the Court held that legislation which authorised the collection and retention and access by the competent national authorities to data relating to electronic communications would not be contrary to EU law if that legislation was targeted. The door thus opened by the Court of Justice is theoretical, however. In fact, the Court did not examine in that judgment the conformity of specific legislation that would be thus targeted. It is doubtful that such a system might be put in place without entailing a breach of the principle of equal treatment of citizens.

70 It is apparent from the *travaux préparatoires* that the objective of the contested law differs from the specific situation examined by the Court in the judgments in *Digital Rights Ireland and Others* and in *Tele2 Sverige and Watson and Others*. In those judgments, the Court was required to rule on whether the obligation to retain general and indiscriminate data was necessary and proportionate by reference to the fight against serious crime. The contested law pursues a different aim, namely

to guarantee the integrity of the criminal system and also to improve the citizen's confidence in the functioning of the judicial system by seeking the truth, in the interests of the victim, the accused and all the individuals concerned.

71 There is a reasonable relationship of proportionality between the general obligation to retain data and the objective pursued by the legislature, which, moreover, is wholly consistent with Article 15(1) of Directive 2002/58. Although each citizen is not potentially a criminal, each citizen may encounter crime, whether as a victim, as an accused or as a witness, and may therefore have an interest in the search for the truth. In spite of the general obligation to retain the data, guarantees necessary for the protection of private life are introduced in terms of the retention of those data and in terms of access to those data. In the light of those guarantees, the obligation prescribed by law is not disproportionate. The contested law is not inconsistent with the Court's case-law.

72 The former legislation had been deemed to constitute a disproportionate breach of the right to respect for private life because of the combination of four factors: the fact that the retention of data concerned all individuals, the absence of difference in treatment according to the categories of data retained and the usefulness of those data, the absence or insufficiency of rules, which constitutes an interference with the right to protection of private life.

73 However, neither the Court nor the referring court held that those four factors were sufficient to substantiate a finding that the measure was disproportionate. A review of the principle of proportionality presumes a global approach. The general obligation to retain data is accompanied by sufficient safeguards in terms of access to the data, retention periods and data protection and security, so that the interference is limited to what is strictly necessary.

74 The contested law is consistent with Article 15(1) of Directive 2002/58, including in the matter of data retention and the communication of those data to the competent authorities for the examination, investigation and prosecution of forms of crime other than serious crime, where the life or physical integrity of persons or possessions is in danger, or where there is improper use of the electronic communications systems.

75 The judgment in *Tele2 Sverige and Watson and Others* does not require that the guarantees be cumulative and does not call that finding into question.

76 Last, the Belgian State refers to the *travaux préparatoires* relating to the contested law

VII. Brief presentation of the grounds of the reference

77 The former legislation, which the contested law is intended to replace, was annulled by the referring court in its judgment No 84/2015 of 11 June 2015, the grounds of which are abundantly cited in the present request for a preliminary

ruling. That judgment is available on the Belgian Constitutional Court's website: http://www.const-court.be/public/f/2015/2015-084f.pdf.

78 The referring court cites, next, the *travaux préparatoires* pertaining to the law (Doc. parl. Chambre, 2015-2016, DOC 54-1567), which are available at the address https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat= 54&dossierID= 1567).

79 The referring court emphasises that it follows from the *travaux préparatoires* pertaining to the contested law that the legislature thoroughly examined both the referring court's judgment, No 84/2015 of 11 June 2015, and the judgment of the Court in *Tele2 Sverige and Watson and Others*, on which the referring court's judgment is based.

80 It follows that the objective which the legislature pursues by means of the contested law is not only to combat terrorism and child pornography, but also to be able to use the retained data in a wide variety of situations in which those data may be both the starting part of and also a step in the criminal investigation.

81 The legislature considered that it was impossible, in the light of the objective pursued, to put a targeted and differentiated retention obligation in place, and that it chose to apply strict guarantees to the general and indiscriminate retention obligation, both in terms of protection of data retention and in terms of access, in order to keep to a minimum the interference with the right to respect for private life. In that regard, it was emphasised that it is quite simply impossible to differentiate in advance between persons, periods of time and geographical areas. That impossibility was explained in detail in the *travaux préparatoires* (see document 1, points 7 to 10, http://www.lachambre.be/FLWB/PDF/54/1567/54K1567001.pdf).

82 By its judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), that is to say, after the contested law had been adopted, the Court answered two questions for a preliminary ruling on the interpretation of Article 15(1) de Directive 2002/58.

83 The Court concludes in paragraph 78 of that judgment that 'a legislative measure whereby a Member State, on the basis of Article 15(1) of Directive 2002/58, requires providers of electronic communications services, for the purposes set out in that provision, to grant national authorities, on the conditions laid down in such a measure, access to the data retained by those providers, concerns the processing of personal data by those providers, and that processing falls within the scope of that directive'.

84 The Court recalls that Article 5(1) of the directive provides that the Member States must ensure, by means of their national legislation, the confidentiality of communications effected by means of a public communications network and publicly available electronic communications networks, and the confidentiality of

the related data traffic. The principle of confidentiality implies that any third party is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications (paragraphs 84 and 85).

85 The Court also recalls that Article 15(1) of the directive enables the Member States to introduce exceptions to the obligation of principle laid down in Article 5(1), exceptions which, in accordance with the Court's settled case-law, must be interpreted strictly. 'Article 15] cannot, therefore, permit 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, to become the rule, if the latter provision is not to be rendered largely meaningless' (paragraphs 88 and 89).

86 In that regard, 'the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be "to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system", or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 53). That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on "the grounds laid down" in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision' (paragraph 90).

87 The Court concludes, as regards the scope of Article 15(1) of the directive:

'Member States may adopt a measure that derogates from the principle of confidentiality of communications and related traffic data where it is a "necessary, appropriate and proportionate measure within a democratic society", in view of the objectives laid down in that provision. As regards recital 11 of that directive, it states that a measure of that kind must be "strictly" proportionate to the intended purpose. In relation to, in particular, the retention of data, the requirement laid down in the second sentence of Article 15(1) of that directive is that data should be retained "for a limited period" and be "justified" by reference to one of the objectives stated in the first sentence of Article 15(1) of that directive' (paragraph 95).

88 The Court then considers whether national legislation such as that which applies to the first case that gave rise to the questions referred to it for a preliminary ruling satisfies those conditions. It finds that the national legislation at issue provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an

obligation to retain those data systematically and continuously, with no exceptions. The data thus retained make it possible to trace and identify the source of a communication and its destination, the date, time and duration, to identify users' communication equipment and to establish the location of mobile communication equipment (paragraphs 97 and 98).

89 According to the Court, those data, taken as a whole, are liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained. Those data thus provide 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.

90 The referring court cites in their entirety paragraphs 100 to 112 of the judgment in *Tele2 Sverige and Watson and Others*.

91 In answer to the second question in Case C-203/15 and the first question in Case C-698/15, the Court observes that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access by the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union (paragraph 125).

92 The ECtHR, for its part, has in the meantime held that the Swedish legislation on the bulk interception of electronic communications was compatible with Article 8 of the ECHR (ECtHR, 19 June 2018, *Centrum för Rättvisa v. Sweden*, CE:ECHR:2018:0619JUD003525208). In order to conclude that there was no violation, it takes as a basis the criteria which it developed in its earlier case-law (ECtHR, 4 December 2015, *Roman Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306). It observes, in particular, that:

'The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106). In *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to

fall within States' margin of appreciation' (ECtHR, 19 June 2018, *Centrum för Rättvisa v. Sweden*, CE:ECHR:2018:0619JUD003525208, § 112).

93 The OBFG criticises the contested law for treating users of telecommunications or electronic communications services subject to professional privilege, including, in particular, lawyers, and other users of those services in the same way. It maintains that the law still entails a general obligation to record and retain certain metadata, which make it possible to determine whether a lawyer has been consulted by a natural or legal person, to identify that lawyer, identify the individuals which whom he was in correspondence, in particular his clients, and also the date and time of the communication. That general obligation is imposed on all suppliers to the public of fixed telephone services, mobile telephony, internet access, email via the internet, internet telephony and public electronic communications networks.

The OBFG also criticises the contested law for laying down a general data retention obligation without distinguishing between individuals according to whether or not they are the subject of investigation or prosecution in respect of acts liable to give rise to criminal convictions.

94 It further maintains that the categories of data covered by the law are extremely wide and varied, in that they relate to data aimed at identifying the user or subscriber and the means of communication, the data relating to access and connection of the terminal equipment to the network and to the service and the location of that equipment, including the network termination point, and also the communication data, even though the content of the data, on the other hand, is excluded.

95 The not-for-profit association Académie fiscale and one individual criticise the contested law for treating users of telecommunications or electronic communications services subject to professional privilege, including, in particular, accountants and tax professionals, and other users in the same way, without taking account of the special status of accountants and tax professions, of the fundamental nature of the professional privilege to which they are subject and of the necessary relationship of trust between them and their clients.

96 They also criticise the contested law for treating individuals who are facing investigation or prosecution for acts liable to come under the purposes of the retention of the electronic data at issue and those not facing such investigation or prosecution in the same way.

97 The Liga voor Mensenrechten and the Ligue des Droits de l'Homme criticise the contested law for laying down a general data retention obligation, which requires operators and providers of public telephone services (including internet telephony), internet access and email via the internet, and providers of public electronic communications networks, to retain for 12 months, in practice for all Belgians, whether under suspicion or not, the traffic data concerning fixed telephony, mobile telephony, internet telephony and data relating to internet

access, and to make those data available to the police and the judicial authorities, the intelligence and security services, the emergency services, the Missing Persons Unit and the Telecommunications Ombudsman.

98 A number of individuals living in Belgium who use various electronic communications services under a contract with an operator complain that the contested law places a general and undifferentiated obligation to retain identification, connection and location data and also personal communication data on providers of telephony services, including those provided via the internet, and data relating to internet access and email via the internet, on operators who provide public electronic communications networks and also on operators who provide one of those services.

99 The legislature intended to establish three categories of metadata that must be retained — identification data, access and connection data and communication data —, to reinforce the conditions of access to data by the competent authorities and to reinforce the security of the data retained by operators, in the interpretation of the judgments of the Court in which it was held that a general data retention obligation might be accepted if that obligation is accompanied by such guarantees.

100 Article 95 of Regulation 2016/679 provides that that regulation is not to impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58.

101 Article 15(1) of Directive 2002/58 provides that Member States may adopt legislative measures providing for the retention of data for a limited period for reasons set out in that paragraph, including to safeguard national security, defence and public security, or for the prevention, investigation, detection and prosecution of criminal offences or unauthorised use of the electronic communication system, on the conditions specified in that provision.

102 The contested law fixes, inter alia, the conditions on which the intelligence and security services may obtain data from providers and operators.

103 In that regard, it should be pointed out that, in the case of *Privacy International*, C-623/17, a court in the European Union has referred the following questions to the Court of Justice:

‘In circumstances where:

a. the SIAs’ capabilities to use BCD supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;

b. a fundamental feature of the SIA's use of the BCD is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the BCD in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;

c. the provider of an electronic communications network is not thereafter required to retain the BCD (beyond the period of their ordinary business requirements), which is retained by the State (the SIAs) alone;

d. the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of BCD by the SIAs are consistent with the requirements of the ECHR; and

e. the national court has found that the imposition of the requirements specified in §§119 to 125 of the judgment [of the Grand Chamber in joined cases C-203/15 and C-698/15, *Tele2 Sverige and Watson and Others* … ("the Watson Requirements"), if applicable, would frustrate the measures taken to safeguard national security by the SIAs, and thereby put the national security of the United Kingdom at risk;

1. Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the "e-Privacy Directive"), does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies (SIAs) of a Member State fall within the scope of Union law and of the e-Privacy Directive?

2. If the answer to Question (1) is "yes", do any of the Watson Requirements, or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?'

104 The referring court will have to take the answer to those questions into account in its examination.

105 The contested law also fixes the conditions on which the judicial authorities may obtain data with a view to the detection, investigation and prosecution of offences.

106 Consequently, it is also necessary to await the Court's answer to the question for a preliminary ruling referred to it in the case of *Ministerio Fiscal*, C-207/16:

'Can the sufficient seriousness of offences, as a criterion which justifies interference with the fundamental rights recognised by Articles 7 and 8 of the Charter, be determined taking into account only the sentence which may be

imposed in respect of the offence investigated, or is it also necessary to identify in the criminal conduct particular levels of harm to individual and/or collective legally-protected interests?

If it were in accordance with the constitutional principles of the European Union, used by the Court of Justice in its judgment [in *Digital Rights Ireland*] as standards for the strict review of the Directive declared invalid by that judgment to determine the seriousness of the offence solely on the basis of the sentence which may be imposed, what should the minimum threshold be? Would it be compatible with a general provision setting a minimum of three years' imprisonment?'

It is apparent from the Opinion of Advocate General Saugmandsgaard Øe in that case (C-207/16, EU:C:2018:300) that the relevant provisions are open to a number of interpretations.

107 For the remainder, the points of view of the parties before the referring court differ as to the interpretation to be given to a number of provisions, in particular Article 15(1) of Directive 2002/58 and Articles 7, 8, 11 and 52 of the Charter, which the referring court must incorporate in its review of the contested law.

108 As the applicants submit, the Court, however, held in its judgment in *Tele2 Sverige and Watson and Others* that Article 5(1) of Directive 2002/58 lays down an obligation of principle to ensure the confidentiality of communications and related traffic data and that Article 15(1) of that directive, which contains exceptions to that principle, must be interpreted strictly in order to ensure that the derogation from the obligation of principle provided for in Article 5 of the directive does not become the rule, as the latter provision would otherwise be rendered largely meaningless.

109 The Court also emphasised that only the objectives set out in Article 15 may justify such a measure that derogates from the principle of confidentiality of communications and the related traffic data, Article 15 requiring in that regard that data should be retained only for a limited period and only where such retention is justified on one of the grounds which it sets out.

110 Therefore, as the applicants emphasise, according to the Court, national legislation which requires the general and indiscriminate retention of all the traffic data and all the location data of all subscribers and registered users concerning all means of electronic communication, without the users being informed, constitutes a particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, so that only the fight against serious crime can justify such a measure. The Court adds that while that objective is of general interest, it cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and data location should be considered necessary for the purposes of that fight.

111 The Court concludes that national legislation which provides for no differentiation, limitation or exception according to the objective pursued, and which is comprehensive in that it affects all persons using electronic communication services, without distinction as to geography or time, without any regard to the fact that those persons are even indirectly in a situation that is liable to give rise to criminal proceedings or that the communication of the data concerns persons whose communications are subject to professional privilege or without requiring any relationship between the data retention of which is provided for and a threat to public security, exceeds the limits of what is strictly necessary and cannot be considered justified within a democratic society, as required by Article 15 of the directive, read in the light of Articles 7, 8, 11 and 52(1) of the Charter.

112 In the applicants' submission, the Court of Justice does indeed state that Article 15(1) of Directive 2002/58 does not preclude national legislation that permits the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of the data is limited, with respect to the categories of data to be retained, to the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary. That implies that the national legislation must lay down clear and precise rules and that the persons whose data have been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. The Court adds that the national legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may be adopted as a preventive measure. Such legislation must be based on objective evidence which makes it possible to identify a public whose data are likely to reveal a link with serious criminal offences or which presents a serious risk to public security; such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or perpetration of such offences.

113 However fact, by adopting the contested law, the legislature pursues wider objectives than the fight against serious crime or the risk of a serious breach of public security.

114 The legislature also indicated on a number of occasions in the *travaux préparatoires* that, as regards the very principle of the obligation to retain data, it was aimed at all persons, even if they are not yet involved in an investigation; nor did it draw any distinction according to the time period, the geographical area or a circle of persons, or provide for an exception with respect to persons whose communications are covered by professional privilege.

115 According to the applicants, although the conditions governing access were considerably reinforced in the contested law, the general data retention obligation which it lays down does not satisfy the requirements set out in Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and 52(1) of the Charter,

according to the interpretation given by the Court in its judgment in *Tele2 Sverige and Watson and Others*. Such an obligation exceeds the limits of what is strictly necessary and cannot be considered to be justified in a democratic society, as required by the abovementioned European provisions.

116 The Council of Ministers emphasises that the objective pursued by the contested legislation is a multiple objective. The legislature seeks, first of all, to reinforce the long-standing situation in which access to data in the telecommunications sector is obtained in the context of criminal investigations, by creating a legislative framework that offers the necessary guarantees with respect to the protection of private life. The retention obligation is also introduced with a view to seeking the truth in numerous forms of crime and thus aims to ensure the integrity of the penal system. That search for the truth is in the interest of both the victim and the accused (who will be able, for example, to prove that he was elsewhere at the material time) and of all the other persons concerned. The retention obligation is also dictated by the aims consisting in taking steps to follow up a call to the emergency services or to seek a missing person whose physical integrity is in imminent danger. That factor constitutes a significant difference by comparison with the situations relied on in the judgments of the Court of Justice cited above. There is therefore a relationship of proportionality between the general retention obligation and the aim which the legislature has set for itself.

117 The Council of Ministers again emphasises that the legislature did not consider that it was possible, in the light of the objective pursued, to put a targeted and differentiated retention obligation in place, and that it chose to provide that general and undifferentiated retention obligation with strict guarantees in terms of both the protection of retention data and access to the data, in order to limit to a minimum the interference with the right to protection of private life. In that regard, the Council of Ministers emphasises that it is quite simply impossible to differentiate in advance by reference to persons, time periods and geographical areas. It also refers in that respect to the Opinion of Advocate General Saugmandsgaard Øe in Joined Cases *Tele2 Sverige and Others*, C-203/15 and C-698/15, EU:C:2016:572.

118 It is apparent from the material available to the referring court that most of the Member States, moreover, experience great difficulties in ensuring that their data retention legislation is compatible with the requirements identified by the Court in its case-law (see: Data retention across the EU, http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention; letter from the Netherlands Minister for Justice and Security of 26 March 2018 to the President of the 'Tweede Kamer der Staten-Generaal', Second Chamber, session 2017-2018, 34 537, No 7).

119 Consequently, it is necessary to refer to the Court the first question for a preliminary ruling set out in the operative part.

120 The contested law also aims to permit an effective criminal investigation and an effective sanction in the event of the sexual abuse of minors and to permit the effective identification of the perpetrator of such an offence, even where electronic communications means are used. At the hearing, attention was drawn in that respect to the positive obligations that arise under Articles 3 and 8 of the ECHR as regards the protection of the physical and psychological integrity of minors and other vulnerable individuals, as interpreted by the ECtHR (ECtHR, 2 December 2008, *K.U. v. Finland*, CE:ECHR:2008:1202JUD000287202, §§ 46 to 49). Those obligations might also arise under the corresponding provisions of the Charter, which might have consequences for the interpretation of Article 15(1) of Directive 2002/58.

121 It is therefore necessary to refer the second question for a preliminary ruling set out in the operative part.

122 Last, it is appropriate to refer the third question for a preliminary ruling set out in the operative part.

VIII. Questions for a preliminary ruling

123 The Cour constitutionnelle (Constitutional Court) refers the following questions to the Court of Justice of the European Union:

1. Must Article 15(1) of Directive 2002/58/EC, read in conjunction with the right to security, guaranteed by Article 6 of the Charter of Fundamental Rights of the European Union, and the right to respect for personal data, as guaranteed by Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union, 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/EC, 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 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/EC, in conjunction with Articles 4, 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union, 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/EC, 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 answers 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 Law of 29 May 2016 on the collection and retention of data in the electronic communications sector 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?