

Court of Justice EU, 21 December 2016, Tele2 Sverige and Tom Watson



## PRIVACY

**National legislation providing for general and indiscriminate retention of all traffic and location data of subscribers and registered users relating to all means of electronic communication in breach with Directive on privacy and electronic communications**

• [Article 15\(1\) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector \(Directive on privacy and electronic communications\), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52\(1\) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.](#)

**National legislation that gives competent national authorities access to retained data without providing that access is only granted to fight serious crime, not subject to prior review by a court or independent administrative authority and where there is no requirement that the data concerned should be retained within the European Union is in breach with Directive on privacy and electronic communications**

• [Article 15\(1\) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52\(1\) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of 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.](#)

Source: [curia.europa.eu](http://curia.europa.eu)

## Court of Justice EU, 21 December 2016

(K. Lenaerts, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, E. Juhász and M. Vilaras, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen, C. Lycourgos)

JUDGMENT OF THE COURT (Grand Chamber)

21 December 2016 (\*)

(Reference for a preliminary ruling — Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law)

In Joined Cases C-203/15 and C-698/15,

REQUESTS for a preliminary ruling under Article 267 TFEU, made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom), by decisions, respectively, of 29 April 2015 and 9 December 2015, received at the Court on 4 May 2015 and 28 December 2015, in the proceedings

Tele2 Sverige AB (C-203/15)

v

Post- och telestyrelsen,

and

Secretary of State for the Home Department (C-698/15)

v

Tom Watson,

Peter Brice,

Geoffrey Lewis,

interveners:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Tizzano, Vice-President, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, E. Juhász and M. Vilaras, Presidents of the Chamber, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen and C. Lycourgos, Judges,

Advocate General: H. Saugmandsgaard Øe,

Registrar: C. Strömholm, Administrator,

having regard to the decision of the President of the Court of 1 February 2016 that Case C-698/15 should be determined pursuant to the expedited procedure provided for in Article 105(1) of the Rules of Procedure of the Court,

having regard to the written procedure and further to the hearing on 12 April 2016,

after considering the observations submitted on behalf of:

- Tele2 Sverige AB, by M. Johansson and N. Torgerzon, advokater, and by E. Lagerlöf and S. Backman,
  - Mr Watson, by J. Welch and E. Norton, Solicitors, I. Steele, Advocate, B. Jaffey, Barrister, and D. Rose QC,
  - Mr Brice and Mr Lewis, by A. Suterwalla and R. de Mello, Barristers, R. Drabble QC, and S. Luke, Solicitor,
  - Open Rights Group and Privacy International, by D. Carey, Solicitor, and by R. Mehta and J. Simor, Barristers,
  - The Law Society of England and Wales, by T. Hickman, Barrister, and by N. Turner,
  - the Swedish Government, by A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren and L. Swedenborg, acting as Agents,
  - the United Kingdom Government, by S. Brandon, L. Christie and V. Kaye, acting as Agents, and by D. Beard QC, G. Facenna QC, J. Eadie QC and S. Ford, Barrister,
  - the Belgian Government, by J.-C. Halleux, S. Vanrie and C. Pochet, acting as Agents,
  - the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,
  - the Danish Government, by C. Thorning and M. Wolff, acting as Agents,
  - the German Government, by T. Henze, M. Hellmann and J. Kemper, acting as Agents, and by M. Kottmann and U. Karpenstein, Rechtsanwälte,
  - the Estonian Government, by K. Kraavi-Käerdi, acting as Agent,
  - Ireland, by E. Creedon, L. Williams and A. Joyce, acting as Agents, and by D. Fennelly BL,
  - the Spanish Government, by A. Rubio González, acting as Agent,
  - the French Government, by G. de Bergues, D. Colas, F.-X. Bréchet and C. David, acting as Agents,
  - the Cypriot Government, by K. Kleanthous, acting as Agent,
  - the Hungarian Government, by M. Fehér and G. Koós, acting as Agents,
  - the Netherlands Government, by M. Bulterman, M. Gijzen and J. Langer, acting as Agents,
  - the Polish Government, by B. Majczyna, acting as Agent,
  - the Finnish Government, by J. Heliskoski, acting as Agent,
  - the European Commission, by H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira and J. Vondung, acting as Agents,
- after hearing [the Opinion of the Advocate General](#) at the sitting on 19 July 2016,  
gives the following

### Judgment

1. These requests for a preliminary ruling concern the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (*'Directive 2002/58'*), read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union (*'the Charter'*).

2. The requests have been made in two proceedings between (i) Tele2 Sverige AB and Post- och telestyrelsen (the Swedish Post and Telecom Authority; *'PTS'*), concerning an order sent by PTS to Tele2 Sverige requiring the latter to retain traffic and location data in relation to its subscribers and registered users (Case C-203/15), and (ii) Mr Tom Watson, Mr Peter Brice and Mr Geoffrey Lewis, on the one hand, and the Secretary of State for the Home Department (United Kingdom of Great Britain and Northern Ireland), on the other, concerning the conformity with EU law of Section 1 of the Data Retention and Investigatory Powers Act 2014 (*'DRIPA'*) (Case C-698/15).

### Legal context

#### EU law

#### Directive 2002/58

3. Recitals 2, 6, 7, 11, 21, 22, 26 and 30 of Directive 2002/58 state:

*'(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.*

...

*(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.*

*(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.*

...

*(11) Like 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)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities*

relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

...

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. ...

...

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data ... may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. ...

...

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. ...'

4. Article 1 of Directive 2002/58, headed 'Scope and aim', provides:

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

2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

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

5. Article 2 of Directive 2002/58, headed 'Definitions', provides:

'Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.

The following definitions shall also apply:

...

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

...'

6. Article 3 of Directive 2002/58, headed 'Services concerned', provides:

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



7. Article 4 of that directive, headed 'Security of processing', is worded as follows:

*'1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.*

*1a. Without prejudice to Directive [95/46], the measures referred to in paragraph 1 shall at least:*

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,*
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and*
- ensure the implementation of a security policy with respect to the processing of personal data.*

*...*

8. Article 5 of Directive 2002/58, headed 'Confidentiality of the communications', provides:

*'1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.*

*...*

*3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'*

9. Article 6 of Directive 2002/58, headed 'Traffic data', provides:

*'1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the*

*purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).*

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

*3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.*

*...*

*5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.'*

10. Article 9(1) of that directive, that article being headed 'Location data other than traffic data', provides:

*'Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. ...'*

11. Article 15 of that directive, headed 'Application of certain provisions of Directive [95/46]', states:

*'1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. 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.

...

*Ib. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.*

*2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive [95/46] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.*

...'

#### **Directive 95/46**

12. Article 22 of Directive 95/46, which is in Chapter III of that directive, is worded as follows:

*'Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.'*

#### **Directive 2006/24/EC**

13. Article 1(2) of 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), that article being headed 'Subject matter and scope', provided:

*'This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.'*

14. Article 3 of that directive, headed 'Obligation to retain data', provided:

*'1. By way of derogation from Articles 5, 6 and 9 of [Directive 2002/58], Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.'*

*2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data*

*specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.'*

#### **Swedish law**

15. It is apparent from the order for reference in Case C-203/15 that the Swedish legislature, in order to transpose Directive 2006/24 into national law, amended the lagen (2003:389) om elektronisk kommunikation [Law (2003:389) on electronic communications; 'the LEK'] and the förordningen (2003:396) om elektronisk kommunikation [Regulation (2003:396) on electronic communications]. Both of those texts, in the versions applicable to the dispute in the main proceedings, contain rules on the retention of electronic communications data and on access to that data by the national authorities.

16. Access to that data is, in addition, regulated by the lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Law (2012:278) on gathering of data relating to electronic communications as part of intelligence gathering by law enforcement authorities: 'Law 2012:278') and by the rättegångsbalken (Code of Judicial Procedure; 'the RB').

#### **The obligation to retain electronic communications data**

17. According to the information provided by the referring court in Case C-203/15, the provisions of Paragraph 16a of Chapter 6 of the LEK, read together with Paragraph 1 of Chapter 2 of that law, impose an obligation on providers of electronic communications services to retain data the retention of which was required by Directive 2006/24. The data concerned is that relating to subscriptions and all electronic communications necessary to trace and identify the source and destination of a communication; to determine its date, time, and type; to identify the communications equipment used and to establish the location of mobile communication equipment used at the start and end of each communication. The data which there is an obligation to retain is data generated or processed in the context of telephony services, telephony services which use a mobile connection, electronic messaging systems, internet access services and internet access capacity (connection mode) provision services. The obligation extends to data relating to unsuccessful communications. The obligation does not however extend to the content of communications.

18. Articles 38 to 43 of Regulation (2003:396) on electronic communications specify the categories of data that must be retained. As regards telephony services, there is the obligation to retain data relating to

calls and numbers called and the identifiable dates and times of the start and end of the communication. As regards telephony services which use a mobile connection, additional obligations are imposed, covering, for example, the retention of location data at the start and end of the communication. As regards telephony services using an IP packet, data to be retained includes, in addition to data mentioned above, data relating to the IP addresses of the caller and the person called. As regards electronic messaging systems, data to be retained includes data relating to the numbers of senders and recipients, IP addresses or other messaging addresses. As regards internet access services, data to be retained includes, for example, data relating to the IP addresses of users and the traceable dates and times of logging into and out of the internet access service.

#### **Data retention period**

19. In accordance with Paragraph 16d of Chapter 6 of the LEK, the data covered by Paragraph 16a of that Chapter must be retained by the providers of electronic communications services for six months from the date of the end of communication. The data must then be immediately erased, unless otherwise provided in the second subparagraph of Paragraph 16d of that Chapter.

#### **Access to retained data**

20. Access to retained data by the national authorities is governed by the provisions of Law 2012:278, the LEK and the RB.

#### **– Law 2012:278**

21. In the context of intelligence gathering, the national police, the Säkerhetspolisen (the Swedish Security Service), and the Tullverket (the Swedish Customs Authority) may, on the basis of Paragraph 1 of Law 2012:278, on the conditions prescribed by that law and without informing the provider of an electronic communications network or a provider of an electronic communications service authorised under the LEK, undertake the collection of data relating to messages transmitted by an electronic communications network, the electronic communications equipment located in a specified geographical area and the geographical areas(s) where electronic communications equipment is or was located.

22. In accordance with Paragraphs 2 and 3 of Law 2012:278, data may, as a general rule, be collected if, depending on the circumstances, the measure is particularly necessary in order to avert, prevent or detect criminal activity involving one or more offences punishable by a term of imprisonment of at least two years, or one of the acts listed in Paragraph 3 of that law, referring to offences punishable by a term of imprisonment of less than two years. Any grounds supporting that measure must outweigh considerations relating to the harm or prejudice that may be caused to the person affected by that measure or to an interest opposing that measure. In accordance with Paragraph 5 of that law, the duration of the measure must not exceed one month.

23. The decision to implement such a measure is to be taken by the director of the authority concerned or by a

person to whom that responsibility is delegated. The decision is not subject to prior review by a judicial authority or an independent administrative authority.

24. Under Paragraph 6 of Law 2012:278, the Säkerhets och integritetsskyddsmyndigheten (the Swedish Commission on Security and Integrity Protection) must be informed of any decision authorising the collection of data. In accordance with Paragraph 1 of Lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Law (2007:980) on the supervision of certain law enforcement activities), that authority is to oversee the application of the legislation by the law enforcement authorities.

#### **– The LEK**

25. Under Paragraph 22, first subparagraph, point 2, of Chapter 6 of the LEK, all providers of electronic communications services must disclose data relating to a subscription at the request of the prosecution authority, the national police, the Security Service or any other public law enforcement authority, if that data is connected with a presumed criminal offence. On the information provided by the referring court in Case C-203/15, it is not necessary that the offence be a serious crime.

#### **– The RB**

26. The RB governs the disclosure of retained data to the national authorities within the framework of preliminary investigations. In accordance with Paragraph 19 of Chapter 27 of the RB, '*placing electronic communications under surveillance*' without the knowledge of third parties is, as a general rule, permitted within the framework of preliminary investigations that relate to, inter alia, offences punishable by a sentence of imprisonment of at least six months. The expression '*placing electronic communications under surveillance*', under Paragraph 19 of Chapter 27 of the RB, means obtaining data without the knowledge of third parties that relates to a message transmitted by an electronic communications network, the electronic communications equipment located or having been located in a specific geographical area, and the geographical area(s) where specific electronic communications equipment is or has been located.

27. According to what is stated by the referring court in Case C-203/15, information on the content of a message may not be obtained on the basis of Paragraph 19 of Chapter 27 of the RB. As a general rule, placing electronic communications under surveillance may be ordered, under Paragraph 20 of Chapter 27 of the RB, only where there are reasonable grounds for suspicion that an individual has committed an offence and that the measure is particularly necessary for the purposes of the investigation: the subject of that investigation must moreover be an offence punishable by a sentence of imprisonment of at least two years, or attempts, preparation or conspiracy to commit such an offence. In accordance with Paragraph 21 of Chapter 27 of the RB, the prosecutor must, other than in cases of urgency, request from the court with jurisdiction



authority to place electronic communications under surveillance.

### **The security and protection of retained data**

28. Under Paragraph 3a of Chapter 6 of the LEK, providers of electronic communications services who are subject to an obligation to retain data must take appropriate technical and organisational measures to ensure the protection of data during processing. On the information provided by the referring court in Case C-203/15, Swedish law does not, however, make any provision as to where the data is to be retained.

### **United Kingdom law**

#### **DRIPA**

29. Section 1 of DRIPA, headed ‘Powers for retention of relevant communications data subject to safeguards’, provides:

*‘(1) The Secretary of State may by notice (a “retention notice”) require a public telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of the Regulation of Investigatory Powers Act 2000 (purposes for which communications data may be obtained).*

*(2) A retention notice may:*

*(a) relate to a particular operator or any description of operators;*

*(b) require the retention of all data or any description of data;*

*(c) specify the period or periods for which data is to be retained;*

*(d) contain other requirements, or restrictions, in relation to the retention of data;*

*(e) make different provision for different purposes;*

*(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.*

*(3) The Secretary of State may by regulations make further provision about the retention of relevant communications data.*

*(4) Such provision may, in particular, include provision about:*

*(a) requirements before giving a retention notice;*

*(b) the maximum period for which data is to be retained under a retention notice;*

*(c) the content, giving, coming into force, review, variation or revocation of a retention notice;*

*(d) the integrity, security or protection of, access to, or the disclosure or destruction of, data retained by virtue of this section;*

*(e) the enforcement of, or auditing compliance with, relevant requirements or restrictions;*

*(f) a code of practice in relation to relevant requirements or restrictions or relevant power;*

*(g) the reimbursement by the Secretary of State (with or without conditions) of expenses incurred by public telecommunications operators in complying with relevant requirements or restrictions;*

*(h) the [Data Retention (EC Directive) Regulations 2009] ceasing to have effect and the transition to the retention of data by virtue of this section.*

*(5) The maximum period provided for by virtue of subsection (4)(b) must not exceed 12 months beginning with such day as is specified in relation to the data concerned by regulations under subsection (3).*

*...’*

30. Section 2 of DRIPA defines the expression ‘*relevant communications data*’ as meaning ‘*communications data of the kind mentioned in the Schedule to the [Data Retention (EC Directive) Regulations 2009] so far as such data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned*’.

#### **RIPA**

31. Section 21(4) of the Regulation of Investigatory Powers Act 2000 (‘RIPA’), that section being in Chapter II of that act and headed ‘*Lawful acquisition and disclosure of communications data*’, states:

*‘In this Chapter “communications data” means any of the following:*

*(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;*

*(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person:*

*(i) of any postal service or telecommunications service;*

*or*  
*(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;*

*(c) any information not falling within paragraph (a) or*

*(b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service’.*

32. On the information provided in the order for reference in Case C-698/15, that data includes ‘*user location data*’, but not data relating to the content of a communication.

33. As regards access to retained data, Section 22 of RIPA provides:

*‘(1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.*

*(2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary:*

*(a) in the interests of national security;*

*(b) for the purpose of preventing or detecting crime or of preventing disorder;*

*(c) in the interests of the economic well-being of the United Kingdom;*

*(d) in the interests of public safety;*

*(e) for the purpose of protecting public health;*

*(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;*

(g) or the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) or any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

...

(4) Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator:

(a) if the operator is not already in possession of the data, to obtain the data; and

(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

(5) The designated person shall not grant an authorisation under subsection (3) or give a notice under subsection (4), unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.'

34. Under Section 65 of RIPA, complaints may be made to the Investigatory Powers Tribunal (United Kingdom) if there is reason to believe that data has been acquired inappropriately.

#### **The Data Retention Regulations 2014**

35. The Data Retention Regulations 2014 ('the 2014 Regulations'), adopted on the basis of DRIPA, are divided into three parts, Part 2 containing regulations 2 to 14 of that legislation. Regulation 4, headed 'Retention notices', provides:

'(1) A retention notice must specify:

(a) the public telecommunications operator (or description of operators) to whom it relates,

(b) the relevant communications data which is to be retained,

(c) the period or periods for which the data is to be retained,

(d) any other requirements, or any restrictions, in relation to the retention of the data.

(2) A retention notice must not require any data to be retained for more than 12 months beginning with:

(a) in the case of traffic data or service use data, the day of the communication concerned, and

(b) in the case of subscriber data, the day on which the person concerned leaves the telecommunications service concerned or (if earlier) the day on which the data is changed.

...

36. Regulation 7 of the 2014 Regulations, headed 'Data integrity and security', provides:

'(1) A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must:

(a) secure that the data is of the same integrity and subject to at least the same security and protection as the data on any system from which it is derived,

(b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and

(c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.

(2) A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must destroy the data if the retention of the data ceases to be authorised by virtue of that section and is not otherwise authorised by law.

(3) The requirement in paragraph (2) to destroy the data is a requirement to delete the data in such a way as to make access to the data impossible.

(4) It is sufficient for the operator to make arrangements for the deletion of the data to take place at such monthly or shorter intervals as appear to the operator to be practicable.'

37. Regulation 8 of the 2014 Regulations, headed 'Disclosure of retained data', provides:

'(1) A public telecommunications operator must put in place adequate security systems (including technical and organisational measures) governing access to communications data retained by virtue of section 1 of [DRIPA] in order to protect against any disclosure of a kind which does not fall within section 1(6)(a) of [DRIPA].

(2) A public telecommunications operator who retains communications data by virtue of section 1 of [DRIPA] must retain the data in such a way that it can be transmitted without undue delay in response to requests.'

38. Regulation 9 of the 2014 Regulations, headed 'Oversight by the Information Commissioner', states:

'The Information Commissioner must audit compliance with requirements or restrictions imposed by this Part in relation to the integrity, security or destruction of data retained by virtue of section 1 of [DRIPA].'

#### **The Code of Practice**

39. The Acquisition and Disclosure of Communications Data Code of Practice ('the Code of Practice') contains, in paragraphs 2.5 to 2.9 and 2.36 to 2.45, guidance on the necessity for and proportionality of obtaining communications data. As explained by the referring court in Case C-698/15, particular attention must, in accordance with paragraphs 3.72 to 3.77 of that code, be paid to necessity and proportionality where the communications data sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information.

40. Under paragraph 3.78 to 3.84 of that code, a court order is required in the specific case of an application for communications data that is made in order to identify a journalist's source. Under paragraphs 3.85 to 3.87 of that code, judicial approval is required when an application for access is made by local authorities. No authorisation, on the other hand, need be obtained from a court or any independent body with respect to access to communications data protected by legal professional



privilege or relating to doctors of medicine, Members of Parliament or ministers of religion.

41. Paragraph 7.1 of the Code of Practice provides that communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of that data, must be handled and stored securely. In addition, the requirements of the Data Protection Act must be adhered to.

42. In accordance with paragraph 7.18 of the Code of Practice, where a United Kingdom public authority is considering the possible disclosure to overseas authorities of communications data, it must, *inter alia*, consider whether that data will be adequately protected. However, it is stated in paragraph 7.22 of that code that a transfer of data to a third country may take place where that transfer is necessary for reasons of substantial public interest, even where the third country does not provide an adequate level of protection. On the information given by the referring court in Case C-698/15, the Secretary of State for the Home Department may issue a national security certificate that exempts certain data from the provisions of the legislation.

43. In paragraph 8.1 of that code, it is stated that RIPA established the Interception of Communications Commissioner (United Kingdom), whose remit is, *inter alia*, to provide independent oversight of the exercise and performance of the powers and duties contained in Chapter II of Part I of RIPA. As is stated in paragraph 8.3 of the code, the Commissioner may, where he can ‘*establish that an individual has been adversely affected by any wilful or reckless failure*’, inform that individual of suspected unlawful use of powers.

#### **The disputes in the main proceedings and the questions referred for a preliminary ruling**

##### **Case C-203/15**

44. On 9 April 2014, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the PTS that, following the ruling in [the judgment of 8 April 2014, Digital Rights Ireland and Others \(C-293/12 and C-594/12; ‘the Digital Rights judgment’](#), [EU:C:2014:238](#)) that Directive 2006/24 was invalid, it would cease, as from 14 April 2014, to retain electronic communications data, covered by the LEK, and that it would erase data retained prior to that date.

45. On 15 April 2014, the Rikspolisstyrelsen (the Swedish National Police Authority, Sweden) sent to the PTS a complaint to the effect that Tele2 Sverige had ceased to send to it the data concerned.

46. On 29 April 2014, the justitieminister (Swedish Minister for Justice) appointed a special reporter to examine the Swedish legislation at issue in the light of [the Digital Rights judgment](#). In a report dated 13 June 2014, entitled ‘*Datalagring, EU-rätten och svensk rätt, Ds 2014:23*’ (Data retention, EU law and Swedish law; ‘*the 2014 report*’), the special reporter concluded that the national legislation on the retention of data, as set out in Paragraphs 16a to 16f of the LEK, was not incompatible with either EU law or the European Convention for the Protection of Human Rights and

Fundamental Freedoms, signed in Rome on 4 November 1950 (*‘the ECHR’*). The special reporter emphasised that [the Digital Rights judgment](#) could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. From his perspective, neither should [the Digital Rights judgment](#) be understood as meaning that the Court had established, in that judgment, a set of criteria all of which had to be satisfied if legislation was to be able to be regarded as proportionate. He considered that it was necessary to assess all the circumstances in order to determine the compatibility of the Swedish legislation with EU law, such as the extent of data retention in the light of the provisions on access to data, on the duration of retention, and on the protection and the security of data.

47. On that basis, on 19 June 2014 the PTS informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data covered by the LEK for six months, for the purpose of combating crime. By an order of 27 June 2014, the PTS ordered Tele2 Sverige to commence, by no later than 25 July 2014, the retention of that data.

48. Tele2 Sverige considered that the 2014 report was based on a misinterpretation of [the Digital Rights judgment](#) and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter, and therefore brought an action before the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) challenging the order of 27 June 2014. Since that court dismissed the action, by judgment of 13 October 2014, Tele2 Sverige brought an appeal against that judgment before the referring court.

49. In the opinion of the referring court, the compatibility of the Swedish legislation with EU law should be assessed with regard to Article 15(1) of Directive 2002/58. While that directive establishes the general rule that traffic and location data should be erased or made anonymous when no longer required for the transmission of a communication, Article 15(1) of that directive introduces a derogation from that general rule since it permits the Member States, where justified on one of the specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data. Accordingly, EU law allows, in certain situations, the retention of electronic communications data.

50. The referring court nonetheless seeks to ascertain whether a general and indiscriminate obligation to retain electronic communications data, such as that at issue in the main proceedings, is compatible, taking into consideration [the Digital Rights judgment](#), with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Given that the opinions of the parties differ on that point, it is necessary that the Court give an unequivocal ruling on whether, as maintained by Tele2 Sverige, the general and indiscriminate retention of electronic communications data is per se incompatible with Articles 7 and 8 and Article 52(1) of the Charter, or whether, as stated in the 2014 Report, the compatibility

of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention.

51. In those circumstances the Kamarrätten i Stockholm (Administrative Court of Appeal of Stockholm, Sweden) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

*'(1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime ... compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?*

*(2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:*

*(a) access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference], and*

*(b) data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference], and*

*(c) all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]?'*

#### **Case C-698/15**

52. Mr Watson, Mr Brice and Mr Lewis each lodged, before the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) (United Kingdom), applications for judicial review of the legality of Section 1 of DRIPA, claiming, inter alia, that that section is incompatible with Articles 7 and 8 of the Charter and Article 8 of the ECHR.

53. By judgment of 17 July 2015, the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) held that [the Digital Rights judgment](#) laid down 'mandatory requirements of EU law' applicable to the legislation of Member States on the retention of communications data and access to such data. According to the High Court of Justice, since the Court, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. It follows from the underlying logic of [the Digital Rights judgment](#) that legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, Section 1 of DRIPA is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body.

54. The Secretary of State for the Home Department brought an appeal against that judgment before the Court of Appeal (England & Wales) (Civil Division) (United Kingdom).

55. That court states that Section 1(1) of DRIPA empowers the Secretary of State for the Home Department to adopt, without any prior authorisation from a court or an independent administrative body, a general regime requiring public telecommunications operators to retain all data relating to any postal service or any telecommunications service for a maximum period of 12 months if he/she considers that such a requirement is necessary and proportionate to achieve the purposes stated in the United Kingdom legislation. Even though that data does not include the content of a communication, it could be highly intrusive into the privacy of users of communications services.

56. In the order for reference and in its judgment of 20 November 2015, delivered in the appeal procedure, wherein it decided to send to the Court this request for a preliminary ruling, the referring court considers that the national rules on the retention of data necessarily fall within the scope of Article 15(1) of Directive 2002/58 and must therefore conform to the requirements of the Charter. However, as stated in Article 1(3) of that directive, the EU legislature did not harmonise the rules relating to access to retained data.

57. As regards the effect of [the Digital Rights judgment](#) on the issues raised in the main proceedings, the referring court states that, in the case that gave rise to that judgment, the Court was considering the validity of Directive 2006/24 and not the validity of any national legislation. Having regard, inter alia, to the close relationship between the retention of data and access to that data, it was essential that that directive should incorporate a set of safeguards and that [the Digital Rights judgment](#) should analyse, when examining the lawfulness of the data retention regime established by that directive, the rules relating to access to that data. The Court had not therefore intended to lay down, in that judgment, mandatory requirements applicable to national legislation on access to data that does not implement EU law. Further, the reasoning of the Court was closely linked to the objective pursued by Directive 2006/24. National legislation should, however, be assessed in the light of the objectives pursued by that legislation and its context.

58. As regards the need to refer questions to the Court for a preliminary ruling, the referring court draws attention to the fact that, when the order for reference was issued, six courts in other Member States, five of those courts being courts of last resort, had declared national legislation to be invalid on the basis of [the Digital Rights judgment](#). The answer to the questions referred is therefore not obvious, although the answer is required to give a ruling on the cases brought before that court.

59. In those circumstances, the Court of Appeal (England & Wales) (Civil Division) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

*'(1) Does [the Digital Rights judgment] (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter]?'*

*'(2) Does [the Digital Rights judgment] expand the scope of Articles 7 and/or 8 of [the Charter] beyond that of Article 8 of the European Convention of Human Rights ... as established in the jurisprudence of the European Court of Human Rights ...?'*

#### **The procedure before the Court**

60. By order of 1 February 2016, *Davis and Others* (C-698/15, not published, EU:C:2016:70), the President of the Court decided to grant the request of the Court of Appeal (England & Wales) (Civil Division) that Case C-698/15 should be dealt with under the expedited procedure provided for in Article 105(1) of the Court's Rules of Procedure.

61. By decision of the President of the Court of 10 March 2016, Cases C-203/15 and C-698/15 were joined for the purposes of the oral part of the procedure and the judgment.

#### **Consideration of the questions referred for a preliminary ruling**

##### **The first question in Case C-203/15**

62. By the first question in Case C-203/15, the *Kammarrätten i Stockholm* (Administrative Court of Appeal, Stockholm) seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation such as that at issue in the main proceedings that provides, for the purpose of fighting crime, for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications.

63. That question arises, in particular, from the fact that Directive 2006/24, which the national legislation at issue in the main proceedings was intended to transpose, was declared to be invalid by [the Digital Rights judgment](#), though the parties disagree on the scope of that judgment and its effect on that legislation, given that it governs the retention of traffic and location data and access to that data by the national authorities.

64. It is necessary first to examine whether national legislation such as that at issue in the main proceeding falls within the scope of EU law.

##### **The scope of Directive 2002/58**

65. The Member States that have submitted written observations to the Court have differed in their opinions as to whether and to what extent national legislation on the retention of traffic and location data and access to that data by the national authorities, for the purpose of combating crime, falls within the scope of Directive 2002/58. Whereas, in particular, the Belgian, Danish, German and Estonian Governments, Ireland and the Netherlands Government have

expressed the opinion that the answer is that it does, the Czech Government has proposed that the answer is that it does not, since the sole objective of such legislation is to combat crime. The United Kingdom Government, for its part, argues that only legislation relating to the retention of data, but not legislation relating to the access to that data by the competent national law enforcement authorities, falls within the scope of that directive.

66. As regards, finally, the Commission, while it maintained, in its written observations submitted to the Court in Case C-203/15, that the national legislation at issue in the main proceedings falls within the scope of Directive 2002/58, the Commission argues, in its written observations in Case C-698/15, that only national rules relating to the retention of data, and not those relating to the access of the national authorities to that data, fall within the scope of that directive. The latter rules should, however, according to the Commission, be taken into consideration in order to assess whether national legislation governing the retention of data by providers of electronic communications services constitutes a proportionate interference in the fundamental rights guaranteed in Articles 7 and 8 of the Charter.

67. In that regard, it must be observed that a determination of the scope of Directive 2002/58 must take into consideration, *inter alia*, the general structure of that directive.

68. Article 1(1) of Directive 2002/58 indicates that the directive provides, *inter alia*, for the harmonisation of the provisions of national law required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector.

69. Article 1(3) of that directive excludes from its scope '*activities of the State*' in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (see, by analogy, with respect to the first indent of Article 3(2) of Directive 95/46, [judgments of 6 November 2003, Lindqvist, C-101/01, EU:C:2003:596, paragraph 43](#), and of [16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 41](#)).

70. Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices ('*electronic communications services*'). Consequently, that directive must be regarded as regulating the activities of the providers of such services.

71. Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, '*legislative measures to restrict the scope of*



*the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 [of that directive]*'. The second sentence of Article 15(1) of that directive identifies, as an example of measures that may thus be adopted by Member States, measures '*providing for the retention of data*'.

72. Admittedly, the legislative measures that are referred to in Article 15(1) of Directive 2002/58 concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active (see, to that effect, [judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraph 51](#)). Moreover, the objectives which, under that provision, such measures must pursue, such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that directive.

73. However, having regard to the general structure of Directive 2002/58, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

74. Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1), read together with Article 3 of that directive, must be interpreted as meaning that such legislative measures fall within the scope of that directive.

75. The scope of that directive extends, in particular, to a legislative measure, such as that at issue in the main proceedings, that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.

76. The scope of that directive also extends to a legislative measure relating, as in the main proceedings, to the access of the national authorities to the data retained by the providers of electronic communications services.

77. The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications,

including '*any data related to such communications*', in order to protect the confidentiality of electronic communications.

78. In those circumstances, 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.

79. Further, since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services.

80. That interpretation is confirmed by Article 15(1b) of Directive 2002/58, which provides that providers are to establish internal procedures for responding to requests for access to users' personal data, based on provisions of national law adopted pursuant to Article 15(1) of that directive.

81. It follows from the foregoing that national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15, falls within the scope of Directive 2002/58.

The interpretation of Article 15(1) of Directive 2002/58, in the light of Articles 7, 8, 11 and Article 52(1) of the Charter

82. It must be observed that, according to Article 1(2) of Directive 2002/58, the provisions of that directive '*particularise and complement*' Directive 95/46. As stated in its recital 2, Directive 2002/58 seeks to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter. In that regard, it is clear from the explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which led to Directive 2002/58, that the EU legislature sought '*to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used*'.

83. To that end, Directive 2002/58 contains specific provisions designed, as is apparent from, in particular, recitals 6 and 7 of that directive, to offer to the users of electronic communications services protection against risks to their personal data and privacy that arise from new technology and the increasing capacity for automated storage and processing of data.

84. In particular, Article 5(1) of that 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 services, and the confidentiality of the related traffic data.

85. The principle of confidentiality of communications established by Directive 2002/58 implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication (see, to that effect, [judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraph 47](#)).

86. Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services (see, to that effect, [judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraphs 47 and 48](#)). As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.

87. The scope of Article 5, Article 6 and Article 9(1) of Directive 2002/58, which seek to ensure the confidentiality of communications and related data, and to minimise the risks of misuse, must moreover be assessed in the light of recital 30 of that directive, which states: ‘*Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum*’.

88. Admittedly, Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to in Articles 6 and 9 of that directive (see, to that effect, [judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraph 50](#)).

89. Nonetheless, in so far as Article 15(1) of Directive 2002/58 enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court’s settled case-law, be interpreted strictly (see, by analogy, judgment of 22 November 2012, Probst, C-119/12, EU:C:2012:748, paragraph 23). That provision 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.

90. It must, in that regard, be observed that 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.

91. Further, the third sentence of Article 15(1) of Directive 2002/58 provides that ‘*[a]ll the measures referred to [in Article 15(1)] shall be in accordance with the general principles of [European Union] law, including those referred to in Article 6(1) and (2) [EU]*’, which include the general principles and fundamental rights now guaranteed by the Charter. Article 15(1) of Directive 2002/58 must, therefore, be interpreted in the light of the fundamental rights guaranteed by the Charter (see, by analogy, in relation to Directive 95/46, [judgments of 20 May 2003, Österreichischer Rundfunk and Others, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68](#); of [13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 68](#), and of [6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 38](#)).

92. In that regard, it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraphs 25 and 70](#)).

93. Accordingly, the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 of the Charter, as derived from the Court’s case-law (see, to that effect, [judgment of 6 October](#)

[2015, Schrems, C-362/14, EU:C:2015:650, paragraph 39](#) and the case-law cited), must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society. That fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 12 June 2003, Schmidberger, C-112/00, EU:C:2003:333, paragraph 79, and of 6 September 2011, Patriciello, C-163/10, EU:C:2011:543, paragraph 31).

94. In that regard, it must be recalled that, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, paragraph 50).

95. With respect to that last issue, the first sentence of Article 15(1) of Directive 2002/58 provides that 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.

96. Due regard to the principle of proportionality also derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary ([judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 56](#); of 9 November 2010, Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, paragraph 77; [the Digital Rights judgment, paragraph 52](#), and of [6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 92](#)).

97. As regards whether national legislation, such as that at issue in Case C-203/15, satisfies those conditions, it must be observed that that legislation 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 that data systematically and continuously, with no exceptions. As stated in the order for reference, the categories of data covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24.

98. The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, [the Digital Rights judgment, paragraph 26](#)).

99. That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 27](#)). In particular, that data provides the means, as observed by the Advocate General in [points 253, 254 and 257 to 259](#) of his Opinion, 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.

100. The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 37](#)).

101. Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 39](#)), the retention of traffic and location data could nonetheless



have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 28](#)).

102. Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 60](#)).

103. Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 51](#)).

104. In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.

105. Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraphs 57 and 58](#)).

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

to Directive 2006/24, [the Digital Rights judgment, paragraph 59](#)).

107. National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

108. However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 54](#) and the case-law cited).

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing 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 commission of such offences.

112. Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is 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 which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

**The second question in Case C-203/15 and the first question in Case C-698/15**

113. It must, at the outset, be noted that the Kamarrätten i Stockholm (Administrative Court of Appeal, Stockholm) referred the second question in Case C-203/15 only in the event that the answer to the first question in that case was negative. That second question, however, arises irrespective of whether retention of data is generalised or targeted, as set out in paragraphs 108 to 111 of this judgment. Accordingly, the Court must answer the second question in Case C-203/15 together with the first question in Case C-698/15, which is referred regardless of the extent of the obligation to retain data that is imposed on providers of electronic communications services.

114. By the second question in Case C-203/15 and the first question in Case C-698/15, the referring courts seek, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 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 more particularly, the access of the competent national authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that 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.

115. As regards objectives that are capable of justifying national legislation that derogates from the principle of confidentiality of electronic communications, it must be borne in mind that, since, as stated in paragraphs 90 and 102 of this judgment, the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, access to the retained data must correspond, genuinely and strictly, to one of those objectives. Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.

116. As regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent

national authorities access to the retained data must ensure, in accordance with what was stated in paragraphs 95 and 96 of this judgment, that such access does not exceed the limits of what is strictly necessary.

117. Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, '*be subject to adequate safeguards*', a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.

118. In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment, paragraph 61](#)).

119. Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015, *Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.

120. In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request

by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment](#), paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).

121. Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, [judgments of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293, paragraph 52](#), and of [6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 95](#)).

122. With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, [the Digital Rights judgment](#), [paragraphs 66 to 68](#)).

123. In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, [the Digital Rights judgment](#), [paragraph 68](#),

and [the judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 41 and 58](#)).

124. It is the task of the referring courts to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgment, with respect to both the access of the competent national authorities to the retained data and the protection and level of security of that data.

125. Having regard to all of the foregoing, the answer to the second question in Case C-203/15 and to the first question in Case C-698/15 is 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 of 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.

#### **The second question in Case C-698/15**

126. By the second question in Case C-698/15, the Court of Appeal (England & Wales) (Civil Division) seeks in essence to ascertain whether, in [the Digital Rights judgment](#), the Court interpreted Articles 7 and/or 8 of the Charter in such a way as to expand the scope conferred on Article 8 ECHR by the European Court of Human Rights.

127. As a preliminary point, it should be recalled that, whilst, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of EU law, the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (see, to that effect, judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, paragraph 45 and the case-law cited).

128. Accordingly, the interpretation of Directive 2002/58, which is at issue in this case, must be undertaken solely in the light of the fundamental rights guaranteed by the Charter (see, to that effect, judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, paragraph 46 and the case-law cited).

129. Further, it must be borne in mind that the explanation on Article 52 of the Charter indicates that paragraph 3 of that article is intended to ensure the necessary consistency between the Charter and the ECHR, *'without thereby adversely affecting the autonomy of Union law and ... that of the Court of Justice of the European Union'* (judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, paragraph 47). In particular, as expressly stated in the second sentence of Article 52(3) of the Charter, the first sentence of Article 52(3) does not preclude Union law



from providing protection that is more extensive than the ECHR. It should be added, finally, that Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.

130. However, in accordance with the Court's settled case-law, the justification for making a request for a preliminary ruling is not for advisory opinions to be delivered on general or hypothetical questions, but rather that it is necessary for the effective resolution of a dispute concerning EU law (see, to that effect, judgments of 24 April 2012, *Kamberaj*, C-571/10, EU:C:2012:233, paragraph 41; of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 42, and of 27 February 2014, *Pohotovost*, C-470/12, EU:C:2014:101 paragraph 29).

131. In this case, in view of the considerations set out, in particular, in paragraphs 128 and 129 of the present judgment, the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter, which is the matter in dispute in the proceedings in Case C-698/15.

132. Accordingly, it does not appear that an answer to the second question in Case C-698/15 can provide any interpretation of points of EU law that is required for the resolution, in the light of that law, of that dispute.

133. It follows that the second question in Case C-698/15 is inadmissible.

#### Costs

134. Since these proceedings are, for the parties to the main proceedings, a step in the actions pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

#### On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of 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.

3. The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible.

[signatures]

\*\* Languages of the case: English and Swedish.

#### OPINION OF ADVOCATE GENERAL SAUGMANDSGAARD ØE

delivered on 19 July 2016 (1)

Joined Cases C-203/15 and C-698/15

Tele2 Sverige AB

v

Post- och telestyrelsen (C-203/15)

and

Secretary of State for the Home Department

v

Tom Watson,

Peter Brice,

Geoffrey Lewis (C-698/15)

Interveners:

Open Rights Group,

Privacy International,

The Law Society of England and Wales

(Requests for a preliminary ruling from the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom)) (Reference for a preliminary ruling — Directive 2002/58/EC — Processing of personal data and the protection of privacy in the electronic communications sector — National legislation imposing a general obligation to retain data relating to electronic communications — Article 15(1) — Charter of Fundamental Rights of the European Union — Article 7 — Right to respect for private life — Article 8 — Right to the protection of personal data — Serious interference — Justification — Article 52(1) — Conditions — Legitimate objective of fighting serious crime — Requirement for a legal basis in national law — Requirement of strict necessity — Requirement of proportionality in a democratic society)

#### Table of contents

I – Introduction

II – Legal framework

A – Directive 2002/58

B – Swedish law

1. The scope of the retention obligation

2. Access to retained data

a) The LEK

b) The RB

c) Law 2012:278

3. The period for which data are retained

4. The protection and security of the data retained

C – United Kingdom law

1. The scope of the retention obligation
  2. Access to retained data
  3. The period for which data are retained
  4. The protection and security of the data retained
- III – The disputes in the main proceedings and the questions referred for a preliminary ruling

A – Case C-203/15

B – Case C-698/15

IV – Procedure before the Court

V – Assessment of the questions referred for a preliminary ruling

A – The admissibility of the second question referred in Case C-698/15

B – The compatibility of a general data retention obligation with the regime established by Directive 2002/58

1. The inclusion of general data retention obligations within the scope of Directive 2002/58

2. The possibility of derogating from the regime established by Directive 2002/58 in order to create a general data retention obligation

C – The applicability of the Charter to general data retention obligations

D – The compatibility of a general data retention obligation with the requirements laid down in Article 15(1) of Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter

1. The requirement for a legal basis in national law

2. Observance of the essence of the rights enshrined in Articles 7 and 8 of the Charter

3. The existence of an objective of general interest recognised by the European Union that is capable of justifying a general data retention obligation

4. The appropriateness of general data retention obligations with regard to the fight against serious crime

5. The necessity of general data retention obligations in the fight against serious crime

a) The strict necessity of general data retention obligations

b) The mandatory nature of the safeguards described by the Court in paragraphs 60 to 68 of *Digital Rights Ireland* in the light of the requirement of strict necessity

6. The proportionality, within a democratic society, of a general data retention obligation in the light of the fight against serious crime

VI – Conclusion

## I – Introduction

1. In 1788, James Madison, one of the authors of the United States Constitution, wrote: *'If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.'* (2)

2. The present cases lead us into the heart of this 'great difficulty' identified by Madison. They concern the compatibility with EU law of national regimes which

impose on providers of publicly accessible electronic communications services ('*service providers*') an obligation to retain data relating to electronic communications ('*communications data*') in relation to all means of communication and all users ('*a general data retention obligation*').

3. On the one hand, the retention of communications data enables '*the government to control the governed*' by providing the competent authorities with a means of investigation that may prove useful in fighting serious crime, and in particular in combating terrorism. In substance, the retention of communications data gives the authorities a certain ability to '*examine the past*' by accessing data relating to communications which a person has effected even before being suspected of involvement in a serious crime. (3)

4. However, on the other hand, it is imperative to '*oblige [the government] to control itself*', with respect to both the retention of data and access to the data retained, given the grave risks engendered by the existence of databases which encompass all communications made within the national territory. Indeed, these enormous databases give anyone having access to them the power instantly to catalogue every member of the population in question. (4) These risks must be scrupulously addressed, inter alia, by means of an examination of the strict necessity and proportionality of general data retention obligations, such as those at issue in the main proceedings.

5. Thus, in the present cases, the Court of Justice and the referring courts are prevailed upon to pinpoint the correct balance between the obligation which Member States are under to ensure the security of individuals within their territory and observance of the fundamental rights to privacy and the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('*the Charter*').

6. I shall be mindful of Madison's '*great difficulty*' as I examine the questions referred to the Court in the present cases, which concern, more specifically, the compatibility with Directive 2002/58/EC (5) and Articles 7 and 8 of the Charter of national regimes establishing a general data retention obligation. In order to answer those questions, the Court will in particular need to clarify how its judgment in *Digital Rights Ireland and Others*, (6) ('*Digital Rights Ireland*'), in which the Grand Chamber of the Court held Directive 2006/24/EC (7) to be invalid, is to be interpreted in the national context.

7. For the reasons which I shall set out below, I have the feeling that a general data retention obligation imposed by a Member State may be compatible with the fundamental rights enshrined in EU law, provided that it is strictly circumscribed by a series of safeguards, and I shall identify these in the course of my analysis.

## II – Legal framework

### A – Directive 2002/58

8. Article 1 of Directive 2002/58, entitled '*Scope and aim*', provides:

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

*2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.*

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

9. Article 15(1) of Directive 2002/58, entitled 'Application of certain provisions of Directive [95/46]', is worded as follows:

*'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]. 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 [European Union] law, including those referred to in Article 6(1) and (2) [TEU].'*

#### **B – Swedish law**

10. Directive 2006/24, which has now been held to be invalid, was transposed into Swedish law by the amendments made to Lagen (2003:389) om elektronisk kommunikation (Law 2003:389 on electronic communications) ('the LEK') and to Förordningen (2003:396) om elektronisk kommunikation (Regulation 2003:396 on electronic communications) ('the FEK'), both of which entered into force on 1 May 2012.

#### **1. The scope of the retention obligation**

11. It is clear from the provisions of Paragraph 16a of Chapter 6 of the LEK that service providers are required to retain the communications data necessary to identify the source and destination of communications, the date, time, duration and type of each communication, the communications equipment used and the location of mobile communication equipment used at the start and end of each communication. The

types of data that must be retained are specified in further detail in Paragraphs 38 to 43 of the FEK.

12. This retention obligation relates to data processed in the context of telephony services, telephony services which use a mobile connection, electronic messaging systems, internet access services and internet access capacity provision services.

13. The data to be retained include not only all the data that had to be retained pursuant to Directive 2006/24, but also data relating to unsuccessful communications as well as data relating to the location at which mobile telephone communications are ended. As under the regime laid down in the directive, the data to be retained do not include the content of communications.

#### **2. Access to retained data**

14. Access to retained data is governed by three laws, namely the LEK, the Rättegångsbalken (Code of Judicial Procedure) ('the RB') and the Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Law 2012:278 on the collection of data on electronic communications in the law enforcement authorities' investigative activities) ('Law 2012:278').

##### **a) The LEK**

15. Under the provisions of point 2 of the first subparagraph of Paragraph 22 of Chapter 6 of the LEK, every service provider must communicate subscription data, on request, to the prosecuting authority, to the police, to the Säkerhetspolisen (the Swedish security service, 'the Säpo') and to any other public law enforcement authority, if the data relate to a suspected crime. Under those provisions, it is not necessary for the crime in question to be a serious crime.

16. Subscription data means, in substance, data relating to the name, title, postal address, telephone number and IP address of the subscriber.

17. Under the LEK, the communication of subscription data is not subject to any prior review, although it may be the subject of an ex post facto administrative review. In addition, there are no limits on the number of authorities that may have access to the data.

##### **b) The RB**

18. The RB governs the surveillance of electronic communications in the course of preliminary investigations.

19. In substance, the surveillance of electronic communications may be ordered only where there is credible evidence to suggest that a person has committed an offence punishable by a term of imprisonment of not less than six months or some other specifically identified offence, if such a measure is particularly necessary for the investigation.

20. In addition to the cases just mentioned, such surveillance may be carried out for the purposes of investigating any person where there is a serious suspicion that he has committed an offence that is punishable by a term of imprisonment of not less than two years, if such a measure is particularly necessary for the investigation.



21. Under Paragraph 21 of Chapter 27 of the RB, the prosecuting authority must normally obtain the authorisation of a competent court before commencing the surveillance of electronic communications.

22. Notwithstanding, if it appears that making an application to a competent court before commencing the surveillance of electronic communications — where such a measure is of vital importance to the investigation — is incompatible with the urgency of the investigation or would hinder it, authorisation may be granted by the prosecuting authority pending a decision of a competent court. The prosecuting authority must immediately inform the court thereof in writing and the court must then promptly consider whether the measure is justified.

#### c) Law 2012:278

23. In the context of information gathering, under Paragraph 1 of Law 2012:278, the national police, the Säpo and the Tullverket (the Swedish customs authority) may, subject to the conditions laid down in that law, collect communications data without the knowledge of the service provider.

24. Under Paragraphs 2 and 3 of Law 2012:278, data may be collected where the circumstances are such that it is particularly necessary to do so in order to avert, prevent or detect criminal activity involving one or more offences punishable by a term of imprisonment of no less than two years or one of the acts listed in Paragraph 3 (which include, in particular, various forms of sabotage and espionage).

25. A decision to collect data in this way is taken by the head of the authority concerned or by another person to whom that power is delegated.

26. The decision must indicate the criminal activity in question, the period covered and the telephone number, any other address, the electronic communications equipment and the geographical area concerned. The duration of the authorisation must not be longer than is necessary. The period following the date of an authorisation decision may not exceed one month.

27. This type of measure is not subject to any prior review. However, pursuant to Paragraph 6 of Law 2012:278, the Säkerhets- och integritetsskyddsmyndigheten (the Commission on Security and Integrity Protection, Sweden) must be informed of any decision authorising the collection of data. Under Paragraph 1 of Lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Law 2007:980 on the supervision of certain law enforcement activities), that body must supervise the application of the law by the law enforcement authorities.

#### 3. The period for which data are retained

28. It is clear from the provisions of Paragraph 16d of Chapter 6 of the LEK that the data referred to in Paragraph 16a thereof must be retained for a period of six months from the day on which the communication is terminated, after which they must immediately be erased, unless otherwise provided for in the second subparagraph of Paragraph 16d of Chapter 6 of the LEK. Pursuant to those last provisions, data that has been requested before the expiry of the retention period

but not communicated must be erased immediately after it is communicated.

#### 4. The protection and security of the data retained

29. The first subparagraph of Paragraph 20 of Chapter 6 of the LEK prohibits the unauthorised dissemination or use of communications data.

30. Pursuant to the provisions of Paragraph 3a of Chapter 6 of the LEK, service providers must take appropriate technical and organisational measures to ensure that processed data are protected. The preparatory work relating to that provision indicates that it is not permissible to determine the level of protection by weighing technical considerations against costs and the risk of infringement of privacy.

31. Further rules on data protection are set out in Paragraph 37 of the FEK and in the regulations and guidelines of the Post- och telestyrelsen (Swedish Post and Telecommunications Authority, *the PTS*) on safeguards in the retention and processing of data for law enforcement purposes (PTSFS No 2012:4). Those texts state, inter alia, that service providers must take measures to protect data against unintentional or unauthorised destruction, against unauthorised retention, processing and access and against unauthorised disclosure. Service providers must also continually and systematically ensure the security of data, having regard to the particular risks associated with the retention obligation.

32. Swedish law contains no provisions concerning the place where the data are to be stored.

33. Under Chapter 7 of the LEK, the regulatory authority has power, where service providers fail to fulfil their obligations, to issue orders and prohibitions, which may carry a penalty, and to order a partial or total cessation of business.

#### C – United Kingdom law

34. The provisions governing the retention of data are set out in the Data Retention and Investigatory Powers Act 2014 (*the DRIPA*), the Data Retention Regulations 2014 (SI 2014/2042) (*the 2014 Regulations*) and the Retention of Communications Data Code of Practice (*the Retention Code of Practice*).

35. The provisions governing access to communications data are to be found in Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (*the RIPA*), the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480), as amended by the Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015 (SI 2015/228) (*the RIPA Amendment Order*) and the Acquisition and Disclosure of Communications Data Code of Practice (*the Acquisition Code of Practice*).

#### 1. The scope of the retention obligation

36. Under section 1 of the DRIPA, the Secretary of State for the Home Department (*the Home Secretary*) may require service providers to retain relevant communications data. In substance, that obligation may extend to all the data generated as a result of communications using a postal service or a

telecommunication system, with the exception of the content of the communication. The data may include, in particular, the location of the user of the service and data identifying the IP address (Internet Protocol address) or any other identifier belonging to the sender or recipient of a communication.

37. The purposes which may justify the issuing of a retention notice include the interests of national security, the prevention or detection of crime or the prevention of disorder, the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security, the interests of public safety, the protection of public health, the assessment or collection of any tax, contribution or other sum payable to the government, the prevention of harm to physical or mental health in urgent cases, providing assistance in investigations into alleged miscarriages of justice, the identification of persons who have died or who are unable to identify themselves because of a condition other than one resulting from a crime (such as a natural disaster or an accident), exercising functions relating to the regulation of financial services and markets or to financial stability and any other purpose specified in an order made by the Home Secretary under section 22(2) of the DRIPA.

38. There is no requirement in the national legislation for the issue of a retention notice to be subject to prior judicial or independent authorisation. The Home Secretary must ensure that the retention obligation is *'necessary and proportionate'* to one or more of the purposes that is to be achieved by retaining the relevant communications data.

## **2. Access to retained data**

39. Under section 22(4) of the RIPA, the public authorities may, by notice, require service providers to disclose communications data to them. The form and content of such notices is governed by section 23(2) of the RIPA. Such notices are limited in time by provisions governing cancellation and renewal.

40. The acquisition of communications data must be necessary and proportionate to one or more of the purposes set out in section 22 of the RIPA, which correspond to the purposes which may justify the retention of data described in [point 37 of this Opinion](#).

41. It is clear from the Acquisition Code of Practice that a court order is necessary in the case of an application for access which is made in order to identify a journalist's source, as in the case of applications for access made by local authorities.

42. Leaving aside those cases, before public authorities can access data it is necessary for authorisation to be given by the designated person within the relevant authority. A designated person is the person holding the prescribed office, rank or position within the relevant public authority that has been designated for the purpose of acquiring communications data in the RIPA Amendment Order.

43. No judicial or independent authorisation is specifically required in order to access communications data that is subject to legal professional privilege or

communications data relating to medical doctors, Members of Parliament or ministers of religion. The Acquisition Code of Practice merely states that special consideration must be given to the necessity and proportionality of applications for access to such data.

## **3. The period for which data are retained**

44. Section 1(5) of the DRIPA and Regulation 4(2) of the 2014 Regulations provide for a maximum data retention period of 12 months. In accordance with the Retention Code of Practice, the period must be only as long as is necessary and proportionate. Regulation 6 of the 2014 Regulations requires the Home Secretary to keep retention notices under review.

## **4. The protection and security of the data retained**

45. Under section 1 of the DRIPA, service providers are prohibited from disclosing retained data unless such disclosure is in accordance with Chapter II of Part I of the RIPA, a court order or other judicial authorisation or warrant or a regulation adopted by the Home Secretary under section 1 of the DRIPA.

46. In accordance with Regulations 7 and 8 of the 2014 Regulations, service providers must ensure the integrity and security of retained data, protect them from accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful retention, processing, access or disclosure. They must destroy the data so as to make it impossible to access if the retention of the data ceases to be authorised and must put in place adequate security systems. Regulation 9 of the 2014 Regulations imposes a duty on the Information Commissioner to audit compliance by service providers with these requirements.

47. The authorities to which service providers transmit communications data must handle and store the data, and all copies, extracts and summaries of it, securely. In accordance with the Acquisition Code of Practice, the requirements of the Data Protection Act, which transposed Directive 95/46, must be observed.

48. The RIPA provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the exercise and performance of the powers and duties set out in Chapter II of Part I of the RIPA. The Commissioner does not provide any oversight of the use of section 1 of the DRIPA. He must make regular reports to the public and to Parliament (section 57(2) and section 58 of the RIPA) and track record keeping and reporting by public authorities (Acquisition Code of Practice, paragraphs 6.1 to 6.8). Complaints may be made to the Investigatory Powers Tribunal if there is reason to believe that data have been acquired inappropriately (section 65 of the RIPA).

49. It is apparent from the Acquisition Code of Practice that the Interception of Communications Commissioner has no power to refer cases to the Investigatory Powers Tribunal. He may merely inform persons of a suspected unlawful use of powers if he is able to *'establish that an individual has been adversely affected by any wilful or reckless failure'*. However, he is not permitted to disclose information if national security could be

threatened by such disclosure, even if he is satisfied that there has been a wilful or reckless failure.

### **III – The disputes in the main proceedings and the questions referred for a preliminary ruling**

#### **A – Case C-203/15**

50. On 9 April 2014, the day after the judgment in Digital Rights Ireland was handed down, Tele2 Sverige notified the PTS of its decision to cease retaining the data referred to in Chapter 6 of the LEK. Tele2 Sverige also proposed to delete the data which had been retained until then in accordance with that chapter. Tele2 Sverige had concluded that the Swedish legislation transposing Directive 2006/24 was not in conformity with the Charter.

51. On 15 April 2014, the Rikspolisstyrelsen (the National Police Board, Sweden, ‘the RPS’) complained to the PTS that Tele2 Sverige had ceased transmitting to it data relating to certain electronic communications. In its complaint, the RPS stated that Tele2 Sverige’s refusal to do so would have serious consequences for the police’s law enforcement activities.

52. By decision of 27 June 2014, the PTS ordered Tele2 Sverige to resume the retention of data in accordance with Paragraph 16a of Chapter 6 of the LEK and Paragraphs 37 to 43 of the FEK by 25 July 2014 at the latest.

53. Tele2 Sverige brought an appeal before the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm, Sweden) against the PTS’s decision. By judgment of 13 October 2014, the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) dismissed that appeal.

54. Tele2 Sverige brought an appeal against the judgment of the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) before the referring court, seeking the setting aside of the contested decision.

55. Finding that there were arguments both in favour of and against the view that such an extensive retention obligation as that provided for in Paragraph 16a of Chapter 6 of the LEK was compatible with Article 15(1) of Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter, the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) decided to stay the proceedings and refer the following questions to the Court of Justice for a preliminary ruling:

*‘(1) Is a general obligation to retain data in relation to all persons and all means of electronic communication and extending to all traffic data, without any distinction, limitation or exception being made by reference to the objective of fighting crime [as described in paragraphs 13 to 18 of the order for reference] compatible with Article 15(1) of Directive 2002/58, taking into account Articles 7, 8 and 52(1) of the Charter?’*

*‘(2) In the event that the first question is answered in the negative, may such a retention obligation nevertheless be permitted where:*

*(a) access by the national authorities to the retained data is governed in the manner specified in paragraphs 19 to 36 [of the order for reference], and*

*(b) the protection and security of the data are regulated in the manner specified in paragraphs 38 to 43 [of the order for reference], and*

*(c) all relevant data must be retained for a period of six months from the date on which the communication was terminated before then being deleted, as described in paragraph 37 [of the order for reference]?’*

#### **B – Case C-698/15**

56. Messrs Watson, Brice and Lewis have brought before the High Court of Justice (England and Wales), Queen’s Bench Division (Administrative Court), applications for judicial review of the lawfulness of the data retention regime in section 1 of DRIPA, which empowers the Home Secretary to require public telecommunications operators to retain communications data for a maximum period of 12 months, retention of the content of the communications concerned being excluded.

57. Open Rights Group, Privacy International and the Law Society of England and Wales were granted leave to intervene in each of those applications.

58. By judgment of 17 July 2015, the High Court of Justice declared that the regime in question was inconsistent with EU law in that it did not satisfy the requirements laid down in Digital Rights Ireland, which it regarded as applying to the rules in the Member States on the retention of data relating to electronic communications and on access to such data. The Home Secretary brought an appeal against that judgment before the referring court.

59. In its judgment of 20 November 2015, the Court of Appeal (England and Wales) (Civil Division) expressed the provisional view that, in Digital Rights Ireland, the Court of Justice was not laying down specific mandatory requirements of EU law with which national legislation must comply, but was simply identifying and describing protections that were absent from the harmonised EU regime.

60. Nevertheless, considering that the answers to those questions of EU law were not clear and were necessary in order for it to give judgment in the proceedings, the Court of Appeal (England & Wales) (Civil Division) decided to stay the proceedings and refer the following questions to the Court of Justice for a preliminary ruling:

*‘(1) Does the judgment of the Court of Justice in Digital Rights Ireland (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State’s domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of the [Charter]?’*

*‘(2) Does the judgment of the Court of Justice in Digital Rights Ireland expand the scope of Articles 7 and/or 8 of the Charter beyond that of Article 8 of the European Convention of Human Rights (“ECHR”) as established in the jurisprudence of the European Court of Human Rights (“ECtHR”)?’*



#### **IV – Procedure before the Court**

61. The requests for a preliminary ruling were registered at the Registry of the Court of Justice on 4 May 2015 (Case C-203/15) and 28 December 2015 (Case C-698/15).

62. By order of 1 February 2016, the Court decided that Case C-698/15 should be dealt with under the expedited procedure provided for in Article 105(1) of the Rules of Procedure of the Court of Justice.

63. In Case C-203/15, written observations were submitted by Tele2 Sverige, the Belgian, Czech, Danish, German, Estonian, Irish, Spanish, French, Hungarian, Netherlands, Swedish and United Kingdom Governments and the European Commission.

64. In Case C-698/15, written observations were submitted by Messrs Watson, Brice and Lewis, Open Rights Group, Privacy International, the Law Society of England and Wales, the Czech, Danish, German, Estonian, Irish, French, Cypriot, Polish, Finnish and United Kingdom Governments and the Commission.

65. By decision of the Court of 10 March 2016, the two cases were joined for the purposes of the oral part of the procedure and the judgment.

66. The representatives of Tele2 Sverige, Messrs Watson, Brice and Lewis, Open Rights Group, Privacy International, the Law Society of England and Wales, the Czech, Danish, German, Estonian, Irish, Spanish, French, Finnish, Swedish and United Kingdom Governments and the Commission attended the hearing, held on 12 April 2016, and presented oral argument.

#### **V – Assessment of the questions referred for a preliminary ruling**

67. By the first question referred in Case C-203/15, the national court asks the Court of Justice whether, in the light of Digital Rights Ireland, Article 15(1) of Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter are to be interpreted as precluding Member States from imposing on service providers a general obligation to retain data such as that at issue in the main proceedings, regardless of any safeguards that might accompany such an obligation.

68. In the event that that question is answered in the negative, the second question referred in Case C-203/15 and the first question referred in Case C-698/15 seek to establish whether those provisions are to be interpreted as precluding Member States from imposing on service providers a general data retention obligation where that obligation is not accompanied by all the safeguards laid down by the Court in paragraphs 60 to 68 of Digital Rights Ireland in connection with access to the data, the period of retention and the protection and security of the data.

69. Since these three questions are closely interlinked, I shall examine them together in the assessment that follows.

70. On the other hand, the second question referred in Case C-698/15 must be addressed separately. By that question, the referring court asks the Court of Justice whether Digital Rights Ireland extended the scope of

Article 7 and/or Article 8 of the Charter beyond that of Article 8 of the ECHR. I shall set out in the following section the reasons for which I consider that this question must be rejected as inadmissible.

71. Before commencing my examination of the questions referred, I think it useful to set out again the types of data that are covered by the retention obligations at issue in the main proceedings. According to the information provided by the referring courts, the scope of the obligations at issue is essentially the same as that of the obligation which was provided for in Article 5 of Directive 2006/24. (8) The communications data covered by the retention obligations may be arranged schematically into four categories: (9)

– data identifying both the source and the destination of communications;

– data identifying the location of both the source and the destination of communications;

– data relating to the date, time and duration of communications and

– data identifying the type of each communication and the type of equipment used.

72. The content of communications is excluded from the general data retention obligations at issue in the main proceedings, as was required by Article 5(2) of Directive 2006/24.

#### **A – The admissibility of the second question referred in Case C-698/15**

73. The second question referred in Case C-698/15 invites the Court to clarify whether Digital Rights Ireland extended the scope of Article 7 and/or Article 8 of the Charter beyond that of Article 8 of the ECHR, as interpreted by the ECtHR.

74. That question reflects, in particular, an argument raised by the Home Secretary before the referring court, according to which the case-law of the ECtHR does not require that access to data should be subject to prior authorisation by an independent body or that the retention of such data and access to it must be confined to the sphere of fighting serious crime.

75. I think that this question must be rejected as inadmissible, for the following reasons. Clearly, the reasoning and the approach adopted by the Court in Digital Rights Ireland are of crucial importance to the resolution of the disputes in the main proceedings. However, the fact that that judgment may possibly have extended the scope of Article 7 and/or Article 8 of the Charter beyond that of Article 8 of the ECHR is not in itself relevant to the resolution of those disputes.

76. It must be borne in mind in this connection that, in accordance with Article 6(3) TEU, fundamental rights, as guaranteed by the ECHR, constitute general principles of EU law. However, as the European Union has not acceded to the ECHR, the latter does not constitute a legal instrument which has been formally incorporated into the legal order of the European Union. (10)

77. Admittedly, the first sentence of Article 52(3) of the Charter lays down a rule of interpretation according to which, in so far as the Charter contains rights which

correspond to rights guaranteed by the ECHR, *'the meaning and scope of those rights [must] be the same as those laid down by the said Convention'*.

78. However, according to the second sentence of Article 52(3) of the Charter, *'this provision [does] not prevent Union law providing more extensive protection'*. To my mind, it is clear from that sentence that the Court is entitled, if it regards it as necessary in the context of EU law, to extend the scope of the provisions of the Charter beyond that of the corresponding provisions of the ECHR.

79. I would add, as a subsidiary point, that Article 8 of the Charter, which was interpreted by the Court in Digital Rights Ireland, establishes a right that does not correspond to any right guaranteed by the ECHR, namely the right to the protection of personal data, as is confirmed, moreover, by the explanations relating to Article 52 of the Charter. (11) Thus, the rule of interpretation laid down in the first sentence of Article 52(3) of the Charter does not, in any event, apply to the interpretation of Article 8 of the Charter, as has been pointed out by Messrs Brice and Lewis, Open Rights Group, Privacy International, the Law Society of England and Wales and the Czech, Irish and Finnish Governments.

80. It follows from the foregoing that EU law does not preclude Articles 7 and 8 of the Charter from providing more extensive protection than that provided for in the ECHR. Therefore, whether or not Digital Rights Ireland extended the scope of those provisions of the Charter beyond that of Article 8 of the ECHR is not, in itself, relevant to the resolution of the disputes in the main proceedings. The decision that is taken on these disputes will essentially depend on the circumstances under which a general data retention obligation may be regarded as consistent with Article 15(1) of Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter, interpreted in the light of Digital Rights Ireland, which is precisely the subject of the three other questions referred in the present cases.

81. According to consistent case-law, a reference from a national court may be refused only if it is quite obvious that the interpretation of EU law sought bears no relation to the actual facts of the main action or to its purpose, or where the problem is hypothetical or the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it. (12)

82. In this instance, for the reasons which I have set out, the second question referred in Case C-698/15 seems to me to be of purely theoretical interest, inasmuch it would not be possible to glean from any answer to that question any factors necessary for an interpretation of EU law which the referring court might usefully apply in order to resolve, in accordance with that law, the dispute before it. (13)

83. That being so, I consider that the question must be rejected as inadmissible, as Mr Watson, the Law Society of England and Wales and the Czech Government have rightly contended.

## **B – The compatibility of a general data retention obligation with the regime established by Directive 2002/58**

84. In this section I shall address the question whether the Member States are entitled to avail themselves of the possibility offered by Article 15(1) of Directive 2002/58 in order to impose a general data retention obligation. I shall not, however, examine the particular requirements that must be observed by Member States wishing to avail themselves of that possibility, since I shall analyse those amply in a later section. (14)

85. Indeed, Open Rights Group and Privacy International have argued that such an obligation would be inconsistent with the harmonised regime established by Directive 2002/58 regardless of whether or not it meets the requirements which arise from Article 15(1) thereof, since it would completely undermine the substance of the rights and the regime established by that directive.

86. Before that argument may be considered, it is necessary first to establish whether general data retention obligations fall within the scope of the directive.

### **1. The inclusion of general data retention obligations within the scope of Directive 2002/58**

87. None of the parties that have submitted observations to the Court has disputed the fact that general data retention obligations, such as those at issue in the main proceedings, fall within the concept of the *'processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the [Union]'* for the purposes of Article 3 of Directive 2002/58.

88. However, the Czech, French, Polish and United Kingdom Governments have submitted that general data retention obligations fall within the ambit of the exclusion laid down in Article 1(3) of Directive 2002/58. First, the national provisions governing access to the data and its use by the police and judicial authorities of the Member States relate to public security, defence and State security, or at least fall within the ambit of criminal law. Secondly, the sole objective of retaining the data is to enable the police and judicial authorities to access it and use it. Therefore, data retention obligations are excluded from the scope of the directive as a result of the aforementioned provision.

89. I am not convinced by that reasoning, for the following reasons.

90. First of all, the wording of Article 15(1) of Directive 2002/58 confirms that retention obligations imposed by the Member States fall within the scope of the directive. Indeed, that provision states that *'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'*. I think it difficult, to say the least, to maintain that retention obligations are excluded from the scope of the directive when Article 15(1) of the directive governs the possibility of imposing such obligations.

91. In reality, as Messrs Watson, Brice and Lewis, the Belgian, Danish, German and Finnish Governments and the Commission have argued, a general data retention obligation, such as those at issue in the main proceedings, is a measure implementing Article 15(1) of Directive 2002/58.

92. Secondly, the fact that provisions governing access may fall within the scope of the exclusion laid down in Article 1(3) of Directive 2002/58 (15) does not mean that retention obligations must also fall within the scope of that exclusion, and thus outside the scope of the directive.

93. In this connection, the Court has already had occasion to clarify that the activities mentioned in the first indent of Article 3(2) of Directive 95/46/EC, (16) the wording of which is equivalent to that of Article 1(3) of Directive 2002/58, are activities of the State or of State authorities and unrelated to the fields of activity of individuals. (17)

94. The retention obligations at issue in the main proceedings, however, are imposed on private operators and concern the private business of providing electronic communications services, as the Commission has pointed out. Moreover, those obligations are imposed independently of any application for access on the part of the police or judicial authorities and, more generally, independently of any act on the part of State authorities relating to public security, defence, State security or criminal law.

95. Thirdly, the approach taken by the Court in its judgment in *Ireland v Parliament and Council* (18) confirms that general data retention obligations do not fall within the sphere of criminal law. Indeed, the Court held that Directive 2006/24, which established such an obligation, related not to criminal law but to the functioning of the internal market and that Article 95 EC (now Article 114 TFEU) was therefore the proper legal basis for the adoption of that directive.

96. In reaching that conclusion, the Court found, in particular, that the provisions of that directive were essentially limited to the activities of service providers and did not govern access to data or the use thereof by the police or judicial authorities of the Member States. (19) I infer from that that provisions of national law which lay down a similar retention obligation to that provided for in Directive 2006/24 do not fall within the sphere of criminal law either.

97. Having regard to the foregoing, I am of the opinion that general data retention obligations do not fall within the scope of the exclusion laid down in Article 1(3) of Directive 2002/58 and thus fall within the scope of the directive.

## **2. The possibility of derogating from the regime established by Directive 2002/58 in order to create a general data retention obligation**

98. It now falls to be determined whether general data retention obligations are consistent with the regime established by Directive 2002/58.

99. The question which therefore arises is whether the Member States are entitled to avail themselves of the

option provided by Article 15(1) of Directive 2002/58 in order to impose a general data retention obligation.

100. Four arguments have been put forward against such a possibility, in particular by Open Rights Group and Privacy International.

101. According to the first argument, granting the Member States power to impose general data retention obligations would undermine the harmonisation objective which is the very purpose of Directive 2002/58. Indeed, according to Article 1(1) thereof, that directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Union.

102. Article 15(1) of Directive 2002/58, it is alleged, cannot therefore be interpreted as giving the Member States power to adopt a derogation from the regime established by that directive that is so broad as to deprive this endeavour to achieve harmonisation of all practical effect.

103. According to the second argument, the wording of Article 15(1) of Directive 2002/58 also militates against such a broad conception of the Member States' power to derogate from the regime established by that directive. That provision states that '*Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of [the] directive*' (my italics).

104. However, a general data retention obligation would not merely '*restrict the scope*' of the rights and obligations mentioned in that provision, it would in fact nullify them. That applies to:

- the duty to ensure the confidentiality of traffic data and the duty to ensure that the storage of information is subject to the agreement of the user, provided for in Article 5(1) and (3) of Directive 2002/58 respectively;
- the duty to erase traffic data or make it anonymous, provided for in Article 6(1) of that directive; and
- the duty to make location data anonymous or to obtain the consent of the user in order for it to be processed, which is imposed by Article 9(1) of the directive.

105. It seems to me that these first two arguments must be rejected, for the following reasons.

106. First of all, the wording of Article 15(1) of Directive 2002/58 refers to the Member States' entitlement to adopt '*legislative measures providing for the retention of data for a limited period*'. That express reference to data retention obligations confirms that such obligations are not in themselves inconsistent with the regime established by Directive 2002/58. Although the form of words used does not expressly provide for the possibility of imposing general data retention obligations, it must be observed that it does not preclude that possibility either.



107. Secondly, recital 11 of Directive 2002/58 states that the directive does not alter ‘the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of [the] directive necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law’. Consequently, ‘[the] directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the [ECHR]’.

108. It follows, in my opinion, from recital 11 that the intention of the EU legislature was not to affect the Member State’s right to adopt the measures referred to in Article 15(1) of Directive 2002/58, but to make that entitlement subject to certain requirements relating, in particular, to the aims pursued and the proportionality of the measures. In other words, general data retention obligations are not, in my view, inconsistent with the regime established by the directive, provided that they satisfy certain conditions.

109. According to the third argument, Article 15(1) of Directive 2002/58 should, as a derogation from the regime established by that directive, be interpreted strictly, in accordance with the rule of interpretation laid down in the consistent case-law of the Court. That requirement of strict interpretation precludes the interpretation of that provision as offering the possibility of adopting a general data retention obligation.

110. To my mind, the option provided for in Article 15(1) of Directive 2002/58 cannot be classified as a derogation, and consequently should not be interpreted strictly, as the Commission has rightly argued. Indeed, I think it difficult to classify that option as a derogation, given that recital 11 of the directive, which I have just mentioned, states that the directive does not affect the Member States’ entitlement to adopt the measures referred to in Article 15(1). I would also point out that Article 15 of the directive is headed ‘Application of certain provisions of Directive [95/46]’, while Article 10 thereof is entitled ‘Exceptions’ (‘Dérégations’ in the French-language version.) Those headings persuade me that the option referred to in Article 15 cannot be classified as a ‘derogation’.

111. According to the fourth and last argument, the fact that a general data retention obligation is inconsistent with the regime established by Directive 2002/58 is borne out by the insertion of a new Article 15(1a) into that directive by Directive 2006/24, which was held to be invalid in Digital Rights Ireland. It is argued that it was this incompatibility that led the EU legislature to declare that Article 15(1) of Directive 2002/58 did not apply to the general retention regime established by Directive 2006/24.

112. This argument appears to me to be based on a misapprehension of the effect of Article 15(1a) of Directive 2002/58. According to that provision,

*‘[Article 15(1) of Directive 2002/58] shall not apply to data specifically required by Directive [2006/24] to be retained for the purposes referred to in Article 1(1) of that directive’.*

113. My reading of that provision is as follows. In so far as concerns data required to be retained pursuant to Directive 2006/24 for the purposes laid down in that directive, the Member States no longer had the option, provided for in Article 15(1) of Directive 2002/58, to restrict further the scope of the rights and obligations referred to in that provision, in particular by the imposition of additional data retention obligations. In other words, Article 15(1a) provided for exhaustive harmonisation as regards the data required to be retained pursuant to Directive 2006/24 for the purposes laid down in that directive.

114. I find confirmation of that interpretation in recital 12 of Directive 2006/24, which states that ‘Article 15(1) of Directive [2002/58] continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive’ (my italics).

115. Thus, the insertion of Article 15(1a) of Directive 2002/58 attests not to the fact that general retention obligations are inconsistent with the regime established by that directive, but to the EU legislature’s intention, when adopting Directive 2006/24, to bring about an exhaustive harmonisation.

116. In light of the foregoing, I consider that general data retention obligations are consistent with the regime established by Directive 2002/58 and that Member States are therefore entitled to avail themselves of the possibility offered by Article 15(1) of that directive in order to impose a general data retention obligation. (20) Recourse to that option is, however, subject to compliance with strict requirements which flow not only from Article 15(1) but also from the relevant provisions of the Charter, read in the light of Digital Rights Ireland, which I shall examine later on. (21)

#### **C – The applicability of the Charter to general data retention obligations**

117. Before considering the content of the requirements that are imposed by the Charter, together with Article 15(1) of Directive 2002/58, where a Member State chooses to introduce a general data retention obligation, it is necessary to establish that the Charter is indeed applicable to such an obligation.

118. The applicability of the Charter to general data retention obligations depends essentially on the applicability of Directive 2002/58 to such obligations.

119. Indeed, in accordance with the first sentence of Article 51(1) of the Charter, ‘the provisions of [the] Charter are addressed to the ... Member States only when they are implementing Union law’. The explanations relating to Article 51 of the Charter refer, in this connection, to the case-law of the Court of Justice, according to which the obligation to observe

the fundamental rights defined in the Union is binding on the Member States only when they are acting within the scope of application of EU law. (22)

120. The Czech, French, Polish and United Kingdom Governments, which dispute the applicability of Directive 2002/58 to general data retention obligations, (23) have also submitted that the Charter is not applicable to such obligations.

121. I have already set out the reasons for which I consider that a general data retention obligation constitutes a measure implementing the option provided for in Article 15(1) of Directive 2002/58. (24)

122. Consequently, I consider that the provisions of the Charter are applicable to national measures introducing such an obligation, in accordance with Article 51(1) of the Charter, as Messrs Watson, Brice and Lewis, Open Rights Group and Privacy International, the Danish, German and Finnish Governments and the Commission have argued. (25)

123. That conclusion is not called into question by the fact that national provisions governing access to retained data do not, as such, fall within the scope of application of the Charter.

124. Admittedly, to the extent that they concern '*activities of the State in areas of criminal law*', national provisions governing the access of police and judicial authorities to retained data for the purpose of fighting serious crime fall, in my opinion, within the scope of the exclusion laid down in Article 1(3) of Directive 2002/58. (26) Consequently, national provisions of that kind do not implement EU law and the Charter therefore does not apply to them.

125. Nevertheless, the *raison d'être* of a data retention obligation is to enable law enforcement authorities to access the data retained, and so the issue of the retention of data cannot be entirely separated from the issue of access to that data. As the Commission has rightly emphasised, provisions governing access are of decisive importance when assessing the compatibility with the Charter of provisions introducing a general data retention obligation in implementation of Article 15(1) of Directive 2002/58. More precisely, provisions governing access must be taken into account in the assessment of the necessity and proportionality of such an obligation. (27)

**D – The compatibility of a general data retention obligation with the requirements laid down in Article 15(1) of Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter**

126. It now remains for me to tackle the difficult question of whether a general data retention obligation is compatible with the requirements laid down in Article 15(1) of Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter, read in the light of Digital Rights Ireland. That question raises the broader issue of the necessary adaptation of existing laws circumscribing the capacity of States to conduct surveillance, a capacity which has increased significantly with recent advancements in technology. (28)

127. The first step in any analysis of this question is a finding of interference with the rights enshrined in

Directive 2002/58 and in the fundamental rights enshrined in Articles 7 and 8 of the Charter.

128. General data retention obligations are in fact a serious interference with the right to privacy, enshrined in Article 7 of the Charter, and the right to the protection of personal data guaranteed by Article 8 of the Charter. I think it unnecessary to linger over that conclusion, which was clearly posited by the Court in paragraphs 32 to 37 of Digital Rights Ireland. (29) Equally, general data retention obligations are an interference with several rights enshrined in Directive 2002/58. (30)

129. The second step in the analysis is to establish whether, and if so on what conditions, such a serious interference with the rights enshrined in Directive 2002/58 and in Articles 7 and 8 of the Charter may be justified.

130. Two provisions lay down conditions that must be satisfied in order for this twofold interference to be justified: Article 15(1) of Directive 2002/58, which circumscribes the right of Member States to restrict the scope of certain rights established in that directive, and Article 52(1) of the Charter, read in the light of Digital Rights Ireland, which circumscribes all restrictions on the rights enshrined in the Charter.

131. I would emphasise that those requirements are cumulative. Compliance with the requirements laid down in Article 15(1) of Directive 2002/58 does not in itself mean that the requirements laid down in Article 52(1) of the Charter are also satisfied, and vice versa. (31) Consequently, a general data retention obligation may be regarded as consistent with EU law only if it complies with both the requirements laid down in Article 15(1) of Directive 2002/58 and those laid down in Article 52(1) of the Charter, as the Law Society of England and Wales has emphasised. (32)

132. Together, those two provisions establish six requirements that must be satisfied in order for the interference caused by a general data retention obligation to be justified:

- the retention obligation must have a legal basis;
- it must observe the essence of the rights enshrined in the Charter;
- it must pursue an objective of general interest;
- it must be appropriate for achieving that objective;
- it must be necessary in order to achieve that objective;
- it must be proportionate, within a democratic society, to the pursuit of that same objective.

133. Several of those conditions were mentioned by the Court in Digital Rights Ireland. For the sake of clarity and given the facts which distinguish the present cases from Digital Rights Ireland, I would nevertheless like to revisit each of them and examine in greater detail the requirements concerning the legal basis for, and the necessity and proportionality within a democratic society of general data retention obligations.

**1. The requirement for a legal basis in national law**

134. Both Article 52(1) of the Charter and Article 15(1) of Directive 2002/58 lay down requirements concerning the legal basis to which Member States

must have recourse when imposing a general data retention obligation.

135. First of all, any limitation on the exercise of the rights recognised by the Charter must, in accordance with Article 52(1) of the Charter, be *'provided for by law'*. That requirement was not formally examined by the Court in *Digital Rights Ireland*, a case which concerned interference pursuant to a directive.

136. Until its recent judgment in *WebMindLicenses*, (33) the Court had never given a ruling on the precise scope of this requirement, not even on those occasions when it expressly held that the requirement had been satisfied (34) or had not been satisfied. (35) In paragraph 81 of the aforementioned judgment, the Third Chamber of the Court stated as follows:

*'In that regard, the requirement that any limitation on the exercise of that right must be provided for by law implies that the legal basis which permits the tax authorities to use the evidence referred to in the preceding paragraph must be sufficiently clear and precise and that, by defining itself the scope of the limitation on the exercise of the right guaranteed by Article 7 of the Charter, it affords a measure of legal protection against any arbitrary interferences by those authorities (see, inter alia, European Court of Human Rights, Malone v. the United Kingdom, 2 August 1984, § 67, Series A no. 82, and Gillan and Quinton v. the United Kingdom, 12 January 2010, no. 4158/05, § 77, ECHR 2010).'*

137. I would invite the Grand Chamber of the Court to confirm that interpretation in the present cases, for the following reasons.

138. As Advocate General Cruz Villalón rightly pointed out in his Opinion in *Scarlet Extended*, (36) the European Court of Human Rights had developed a substantial body of case-law on this requirement, with reference to the ECHR, according to which the term *'law'* must be understood in the substantive, rather than the formal sense of the term. (37)

139. According to that body of case-law, the expression *'provided for by law'* means that the legal basis must be adequately accessible and foreseeable, that is to say, formulated with sufficient precision to enable the individual — if need be with appropriate advice — to regulate his conduct. The legal basis must also provide adequate protection against arbitrary interference and, consequently, must define with sufficient clarity the scope and manner of exercise of the power conferred on the competent authorities (the principle of the supremacy of the law). (38)

140. In my view, the meaning of that expression *'provided for by law'* used in Article 52(1) of the Charter needs to be the same as that ascribed to it in connection with the ECHR, for the following reasons.

141. First of all, pursuant to Article 53 of the Charter and the explanations relating to that provision, the level of protection afforded by the Charter must never be inferior to that guaranteed by the ECHR. This rule that the *'ECHR standard'* must be attained means that the Court's interpretation of the expression *'provided for by law'* used in Article 52(1) of the Charter must be at

least as stringent as that given to it by the European Court of Human Rights in connection with the ECHR. (39)

142. Secondly, in view of the horizontal nature of this requirement for a legal basis, which applies to a variety of types of interference, with reference both to the Charter and to the ECHR, (40) it would be inappropriate to impose different criteria on the Member States depending on which of those two instruments was under consideration. (41)

143. I therefore think that, as the Estonian Government and the Commission have argued, the expression *'provided for by law'* used in Article 52(1) of the Charter must, in light of the case-law of the European Court of Human Rights referred to in point 139 above, be interpreted as meaning that general data retention obligations such as those at issue in the main proceedings must be founded on a legal basis that is adequately accessible and foreseeable and provides adequate protection against arbitrary interference.

144. Secondly, it is necessary to determine the content of the requirements laid down by Article 15(1) of Directive 2002/58 concerning the legal basis to which Member States must have recourse if they wish to avail themselves of the possibility offered by that provision.

145. I must, in this connection, point to certain differences between the various language versions of the first sentence of Article 15(1).

146. In the English (*'legislative measures'*), French (*'mesures législatives'*), Italian (*'disposizioni legislative'*), Portuguese (*'medidas legislativas'*), Romanian (*'măsură legislative'*) and Swedish versions (*'genom lagstiftning vidta åtgärder'*), the first sentence of Article 15(1) of Directive 2002/58 refers, in my opinion, to the adoption of measures emanating from a legislative authority.

147. On the other hand, the Danish (*'retsforskrifter'*), German (*'Rechtsvorschriften'*), Dutch (*'wettelijke maatregelen'*) and Spanish versions (*'medidas legales'*) of that sentence may be interpreted as calling for the adoption either of measures emanating from a legislative authority or of regulatory measures emanating from an executive authority.

148. It is settled case-law that the need for uniform application and, accordingly, for uniform interpretation of a European Union measure makes it impossible to consider one version of the text in isolation, but requires that the measure be interpreted on the basis of both the real intention of its author and the aim the latter seeks to achieve, in the light, in particular, of the versions existing in all the other official languages. Where there is divergence between the various language versions, the provision in question must be interpreted by reference to the purpose and general scheme of the rules of which it forms part. (42)

149. In this instance, Article 15(1) of Directive 2002/58 governs the option available to the Member States of derogating from the fundamental rights enshrined in Articles 7 and 8 of the Charter, the protection of which is implemented in the directive. I therefore regard it as appropriate to interpret the requirement for a legal basis



imposed by Article 15(1) of Directive 2002/58 in the light of the Charter, and in particular Article 52(1) thereof.

150. Accordingly, it is imperative that the ‘*measures*’ required by Article 15(1) of Directive 2002/58 have the characteristics to which I referred in [point 143 of this Opinion](#), namely accessibility and foreseeability and providing adequate protection against arbitrary interference. It follows from those characteristics, and in particular from the requirement for adequate protection against arbitrary interference, that the measures must be binding on the national authorities upon which the power to access the retained data is conferred. It would not be sufficient, for example, if the safeguards surrounding access to data were provided for in codes of practice or internal guidelines having no binding effect, as the Law Society of England and Wales has rightly pointed out.

151. Moreover, the words ‘*Member States may adopt ... measures*’, which are common to all the language versions of the first sentence of Article 15(1) of Directive 2002/58, seem to me to exclude the possibility of national case-law, even settled case-law, providing a sufficient legal basis for the implementation of that provision. I would emphasise that, in this respect, the provision is more stringent than the requirements arising from the case-law of the European Court of Human Rights. (43)

152. I would add that, given the seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that a general data retention obligation entails, it would appear desirable for the essential content of the regime in question, and in particular the safeguards surrounding the obligation, to be laid down in a measure adopted by the legislative authority and to leave the executive authority with responsibility for the detailed rules governing its implementation.

153. Having regard to the foregoing, I consider that Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter must be interpreted as meaning that a regime establishing a general data retention obligation, such as those at issue in the main proceedings, must be established in legislative or regulatory measures possessing the characteristics of accessibility, foreseeability and adequate protection against arbitrary interference.

154. It is for the referring courts, which are in a privileged position to evaluate their respective national regimes, to verify compliance with that requirement.

## **2. Observance of the essence of the rights enshrined in Articles 7 and 8 of the Charter**

155. Article 52(1) of the Charter provides that any limitation on the exercise of the rights recognised by the Charter must ‘*respect the essence of those rights and freedoms*’. (44) That aspect, which the Court examined in paragraphs 39 and 40 of Digital Rights Ireland, with reference to Directive 2006/24, does not seem to me to raise any particular problem in the context of the present cases, as the Spanish and Irish Governments and the Commission have submitted.

156. In paragraph 39 of Digital Rights Ireland, the Court held that Directive 2006/24 did not adversely affect the essence of the right to privacy or of the other rights enshrined in Article 7 of the Charter, since it did not permit the acquisition of knowledge of the content of the electronic communications as such.

157. In my view, that finding could equally apply to the national regimes at issue in the main proceedings, since they also do not permit the acquisition of knowledge of the content of the electronic communications as such. (45)

158. In paragraph 40 of Digital Rights Ireland, the Court held that Directive 2006/24 did not adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, given the principles of data protection and data security that had to be observed by service providers pursuant to Article 7 of that directive, with the Member States being responsible for ensuring that appropriate technical and organisational measures were adopted against accidental or unlawful destruction and accidental loss or alteration of the data.

159. Again, I consider that that finding could equally apply to the national regimes at issue in the main proceedings, since they too, it seems to me, provide for comparable safeguards in so far as concerns the protection and security of the data retained by service providers, inasmuch as those safeguards must effectively protect personal data against the risk of abuse and against any unlawful access and use of that data. (46)

160. It is nevertheless for the referring courts to verify, in the light of the foregoing considerations, whether the national regimes at issue in the main proceedings do indeed observe the essence of the rights recognised in Articles 7 and 8 of the Charter.

## **3. The existence of an objective of general interest recognised by the European Union that is capable of justifying a general data retention obligation**

161. Both Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter require that any interference with the rights enshrined in those instruments should be in the pursuit of an objective in the general interest.

162. In paragraphs 41 to 44 of Digital Rights Ireland, the Court held that the general data retention obligation imposed by Directive 2006/24 contributed ‘*to the fight against serious crime and thus, ultimately, to public security*’ and that the fight against serious crime was an objective of general interest to the European Union.

163. Indeed, it is clear from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest to the Union. The same may be said of the fight against serious crime in order to ensure public security. Furthermore, it should be noted, in this connection, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security. (47)

164. That observation applies equally to the general data retention obligations at issue in the main

proceedings, which are liable to be justified by the objective of fighting serious crime.

165. Nevertheless, having regard to some of the arguments submitted to the Court, it is necessary to determine whether such an obligation may also be justified by an objective in the general interest other than the fight against serious crime.

166. Article 52(1) of the Charter makes a general reference to '*objectives of general interest recognised by the Union*' and to '*the need to protect the rights and freedoms of others*'.

167. The wording of Article 15(1) of Directive 2002/58 is more precise regarding the objectives which may justify interference with the rights laid down in that directive. In accordance with that provision, the measures in question must contribute to '*[safeguarding] 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]*'.

168. In addition, in its judgment in *Promusicae*, (48) the Court held that that provision had to be interpreted in the light of Article 13(1) of Directive 95/46, which authorises derogations from the rights provided for in that directive when they are justified by '*the protection of the rights and freedoms of others*'. Consequently, the Court held that Article 15(1) of Directive 2002/58 offered Member States the possibility of laying down an obligation, for service providers, to disclose personal data so that it could be established, in the context of civil proceedings, whether there has been an infringement of copyright in musical or audiovisual recordings.

169. The United Kingdom Government has drawn from that judgment the argument that a general data retention obligation may be justified by any of the objectives mentioned in either Article 15(1) of Directive 2002/58 or Article 13(1) of Directive 95/46. According to that government, such an obligation could be justified by the utility of retained data in combating '*ordinary*' (as opposed to '*serious*') offences, or even in proceedings other than criminal proceedings, with regard to the objectives mentioned in those provisions.

170. I am not convinced by that argument, for the following reasons.

171. First of all, as Mr Watson and Open Rights Group and Privacy International have emphasised, the approach adopted by the Court in *Promusicae* (49) is not relevant to the present cases, since that case concerned a request made by an organisation representing copyright holders for access to data retained spontaneously by a service provider, namely Telefónica de España. In other words, that judgment did not address the question of what objectives were capable of justifying the serious interference with fundamental rights which general data retention obligations, such as those at issue in the main proceedings, entail.

172. Secondly, I think that the requirement of proportionality within a democratic society prevents the combating of ordinary offences and the smooth conduct of proceedings other than criminal proceedings from constituting justifications for a general data retention obligation. The considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences and in the conduct of proceedings other than criminal proceedings. (50)

173. In light of the foregoing, I consider that Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter must be interpreted as meaning that the fight against serious crime is an objective in the general interest that is capable of justifying a general data retention obligation, whereas combating ordinary offences and the smooth conduct of proceedings other than criminal proceedings are not.

174. Consequently, it is necessary to assess the appropriateness, necessity and proportionality of such obligations with reference to the objective of fighting serious crime.

#### **4. The appropriateness of general data retention obligations with regard to the fight against serious crime**

175. The requirements of appropriateness, necessity (51) and proportionality (52) flow from both Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter.

176. In accordance with the first of those requirements, general data retention obligations, such as those at issue in the main proceedings, must be liable to contribute to the objective of general interest that I have just identified, namely the fight against serious crime.

177. This requirement poses no particular difficulty in the present cases. Indeed, as the Court stated, in substance, in paragraph 49 of *Digital Rights Ireland*, the data retained provide the national authorities having competence in criminal matters with an additional means of investigation to prevent or shed light on serious crime. Consequently, such obligations contribute to the fight against serious crime.

178. I would nevertheless like to be clear about the usefulness of general data retention obligations in the fight against serious crime. As the French Government has rightly pointed out, such obligations, by contrast with targeted surveillance measures, enable law enforcement authorities to '*examine the past*', so to speak, by consulting retained data.

179. Targeted surveillance measures are focused on persons who have already been identified as being potentially connected, even indirectly or remotely, with a serious crime. Such targeted measures enable the competent authorities to access data relating to communications effected by such persons, and even to access the content of their communications. However, that access will be limited only to communications effected after the persons have been identified.

180. General data retention obligations, on the other hand, relate to all communications effected by all users, without requiring any connection whatsoever with a serious crime. Such obligations enable competent

authorities to access the communications history of persons who have not yet been identified as being potentially connected with a serious crime. It is in this sense that general data retention obligations give law enforcement authorities a certain ability to examine the past, allowing them to access communications effected by such persons before they have been so identified. (53)

181. In other words, the usefulness of general data retention obligations in the fight against serious crime lies in this limited ability to examine the past by consulting data that retraces the history of communications effected by persons even before they are suspected of being connected with a serious crime. (54)

182. When presenting the proposal for a directive which led to the adoption of Directive 2006/24, the Commission illustrated this usefulness by giving several specific examples of investigations into terrorism, murder, kidnapping and child pornography. (55)

183. Several similar examples have been given to the Court in the present cases, in particular by the French Government, which has emphasised the positive obligation which Member States are under to ensure the security of persons within their territory. According to that government, in the investigations aimed at dismantling the networks which organise the departure of French residents to conflict zones in Iraq and Syria, access to retained data plays a crucial role in identifying the people who facilitate those departures. The French Government adds that access to the communications data of persons who were involved in the recent terrorist attacks of January and November 2015 in France was extremely useful in helping the investigators discover the authors of those attacks and their accomplices. Similarly, in the search for missing persons, data relating to the location of such persons when effecting communications prior to their disappearance can play a crucial role in the investigation.

184. In light of the foregoing considerations, I think that general data retention obligations are liable to contribute to the fight against serious crime. It nevertheless remains to be verified whether such obligations are both necessary in order to achieve that objective and proportionate to the pursuit of that objective.

##### **5. The necessity of general data retention obligations in the fight against serious crime**

185. It is settled case-law that a measure may be regarded as necessary only if no other measures exist that would be equally appropriate and less restrictive. (56)

186. The requirement of appropriateness calls for an evaluation of the *'absolute'* effectiveness — independently of any other possible measures — of a general data retention obligation in the fight against serious crime. The requirement of necessity calls for an assessment of the efficiency — or *'relative'*

effectiveness of that obligation, that is to say, in comparison with all other possible measures. (57)

187. In the present cases, the test of necessity demands an assessment of whether other measures could be as effective as a general data retention obligation in the fight against serious crime and whether such other measures would interfere to a lesser extent with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter. (58)

188. I would also recall the settled case-law, referred to in paragraph 52 of *Digital Rights Ireland*, according to which the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is *'strictly necessary'*. (59)

189. Two issues relating to the requirement of strict necessity in the context of the present cases have been extensively debated by the parties that have submitted observations to the Court. They correspond, in substance, to the two questions referred by the national court in Case C-203/15:

– first, in the light of paragraphs 56 to 59 of *Digital Rights Ireland*, should a general data retention obligation be regarded as, in itself, going beyond the bounds of what is strictly necessary for the purposes of fighting serious crime, irrespectively of any safeguards that might accompany such an obligation?

– secondly, assuming that such an obligation may be regarded as not, in itself, going beyond the bounds of what is strictly necessary, must it be accompanied by all of the safeguards mentioned by the Court in paragraphs 60 to 68 of *Digital Rights Ireland*, so as to limit the interference with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter to what is strictly necessary?

190. Before addressing those issues, I think it appropriate to dismiss an argument put forward by the United Kingdom Government, according to which the criteria established in *Digital Rights Ireland* are irrelevant to the present cases because that case concerned not a national regime but a regime established by the EU legislature.

191. I would emphasise in this connection that, in *Digital Rights Ireland*, the Court interpreted Articles 7, 8 and 52(1) of the Charter and that those provisions are also the subject of the questions raised here in the main proceedings. In my opinion, it is not possible to interpret the provisions of the Charter differently depending on whether the regime under consideration was established at EU level or at national level, as Messrs Brice and Lewis and the Law Society of England and Wales have rightly emphasised. Once it has been established that the Charter is applicable, as it has been established in the present cases, (60) it must be applied in the same fashion regardless of the regime under consideration. Therefore, the criteria identified by the Court in *Digital Rights Ireland* are relevant in the assessment of the national regimes at issue in the present cases, as the Danish and Irish Governments and the Commission in particular have argued.



**a) The strict necessity of general data retention obligations**

192. According to one view, propounded by Tele2 Sverige, Open Rights Group and Privacy International, general data retention obligations must, following Digital Rights Ireland, be regarded as, in themselves, going beyond the bounds of what is strictly necessary for the purposes of fighting serious crime, irrespectively of any safeguards that might accompany such obligations.

193. According to the other view, propounded by the majority of the parties that have submitted observations to the Court, such obligations do not go beyond the bounds of what is strictly necessary, provided that they are accompanied by certain safeguards concerning access to the data, the period of retention and the protection and security of the data.

194. The following reasons lead me to endorse the latter view.

195. First of all, my reading of Digital Rights Ireland is that the Court held that a general data retention obligation goes beyond the bounds of what is strictly necessary where it is not accompanied by stringent safeguards concerning access to the data, the period of retention and the protection and security of the data. On the other hand, the Court did not rule on the compatibility with EU law of general data retention obligations which are accompanied by such safeguards, inasmuch as that type of regime was not the subject of the questions referred to the Court in that case.

196. I would emphasise in this connection that paragraphs 56 to 59 of Digital Rights Ireland contain no statement from the Court to the effect that general data retention obligations in themselves go beyond what is strictly necessary.

197. In paragraphs 56 and 57 of that judgment, the Court noted that the retention obligation provided for by Directive 2006/24 covered all means of electronic communication, all users and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting serious crime.

198. In paragraphs 58 and 59 of the judgment, the Court described in greater detail the practical implications of this absence of differentiation. First, the retention obligation even concerned persons for whom there was no evidence to suggest that their conduct might have a link, even an indirect or remote one, with serious crime. Secondly, the directive did not require any relationship between the data whose retention was provided for and a threat to public security and, in particular, was not restricted to a retention in relation to data pertaining to a particular time period and/or a particular geographical area and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime.

199. The Court therefore noted that general data retention obligations are characterised by their lack of differentiation by reference to the objective of fighting serious crime. It did not, however, hold that that absence of differentiation meant that such obligations,

in themselves, went beyond what was strictly necessary.

200. In reality, it was only after completing its examination of the regime established by Directive 2006/24 and after noting the absence of certain safeguards — which I shall come on to consider — (61) that the Court held, in paragraph 69 of Digital Rights Ireland:

*'Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter'* (my italics).

201. As the German and Netherlands Governments have argued, if a generalised data retention had, in and of itself, been sufficient to render Directive 2006/24 invalid, there would have been no need for the Court to examine — as it did, in detail — the absence of the safeguards mentioned in paragraphs 60 to 68 of that judgment.

202. Therefore, the general data retention obligation provided for by Directive 2006/24 did not, in itself, go beyond what was strictly necessary. That directive went beyond what was strictly necessary as a result of the combined effect of the generalised retention of data and the lack of safeguards aimed at limiting to what was strictly necessary the interference with the rights enshrined in Articles 7 and 8 of the Charter. Because of that combined effect, it was necessary to declare the directive invalid in its entirety. (62)

203. Secondly, I find confirmation for this interpretation in paragraph 93 of the judgment in Schrems, (63) which reads as follows:

*'Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive [2006/24, Digital Rights Ireland], paragraphs 57 to 61)'* (my italics).

204. Again, the Court did not find that the regime at issue in that case went beyond the bounds of what was strictly necessary for the sole reason that it authorised the generalised retention of personal data. In that case, the bounds of what was strictly necessary had been overstepped because of the combined effect of the possibility of such generalised retention and the lack of a safeguard in relation to access aimed at reducing the interference to what was strictly necessary.

205. I infer from the foregoing that a general data retention obligation need not invariably be regarded as, in itself, going beyond the bounds of what is strictly necessary for the purposes of fighting serious crime.

However, such an obligation will invariably go beyond the bounds of what is strictly necessary if it is not accompanied by safeguards concerning access to the data, the retention period and the protection and security of the data.

206. Thirdly, my feeling in this regard is corroborated by the need to verify, specifically, whether the requirement of strict necessity in the context of the national regimes at issue in the main proceedings has been observed.

207. As I stated in [point 187 of this Opinion](#), the requirement of strict necessity calls for an assessment of whether other measures could be as effective as a general data retention obligation in the fight against serious crime, while at the same time interfering to a lesser extent with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter.

208. That assessment must be carried out in the specific context of each national regime providing for a general data retention obligation. Moreover, it requires a comparison to be made between the effectiveness of such an obligation and that of any other possible national measure, with account being taken of the fact that such obligations give the competent authorities a certain ability to examine the past by consulting the data. (64)

209. Given the requirement of strict necessity, it is imperative that national courts do not simply verify the mere utility of general data retention obligations, but rigorously verify that no other measure or combination of measures, such as a targeted data retention obligation accompanied by other investigatory tools, can be as effectiveness in the fight against serious crime. I would emphasise in this connection that several studies that have been brought to the Court's attention call into question the necessity of this type of obligation in the fight against serious crime. (65)

210. Moreover, assuming that other alternative measures could be as effective in the fight against serious crime, it will still remain for the referring courts, in accordance with the settled case-law referred to in [point 185 of this Opinion](#), to determine whether those other measures would interfere with the fundamental rights at issue to a lesser extent than a general data retention obligation.

211. In the light of paragraph 59 of Digital Rights Ireland, it falls to the national courts to consider, in particular, whether it would be possible to limit the substantive scope of a retention obligation while at the same time preserving the effectiveness of such a measure in the fight against serious crime. (66) Retention obligations may indeed have a greater or lesser substantive scope, depending on the users, geographic area and means of communication covered. (67)

212. To my mind, it would be desirable, if the technology allowed, to exclude from the retention obligation data that is particularly sensitive in terms of the fundamental rights at issue in the main proceedings, such as data that is subject to professional privilege or

data which makes it possible to identify a journalist's source.

213. Nevertheless, it is important to bear in mind that any substantial limitation of the scope of a general data retention obligation may considerably reduce the utility of such a regime in the fight against serious crime. For one reason, as several governments have emphasised, it is difficult, not to say impossible, to determine in advance what data may be connected with a serious crime. Therefore such a limitation could result in the exclusion from retention of data that might have proved relevant in the fight against serious crime.

214. For another reason, as the Estonian Government has pointed out, serious crime is an evolving phenomenon, one that is capable of adapting to the investigatory tools at the disposal of law enforcement authorities. Thus, a limitation to a particular geographic area or to a particular means of communication could result in the shifting of activities relating to serious crime to a geographic area and/or a means of communication not covered by the regime.

215. Since it calls for a complex appraisal of the national regimes at issue in the main proceedings, I consider that this assessment (of whether other measures could be as effective) must be carried out by the national courts, as the Czech, Estonian, Irish, French and Netherlands Governments and the Commission have emphasised.

**b) The mandatory nature of the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland in the light of the requirement of strict necessity**

216. Assuming that a general data retention obligation may be regarded as strictly necessary in the context of the national regime in question, which is a matter for the national court to establish, it must still be determined whether that obligation must be accompanied by all the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland, with a view to limiting the interference with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter to what is strictly necessary.

217. The safeguards described concern the rules governing access to and use of the retained data by the competent authorities (paragraphs 60 to 62 of Digital Rights Ireland), the data retention period (paragraphs 63 and 64 of Digital Rights Ireland) and the security and protection of the data retained by service providers (paragraphs 66 to 68 of Digital Rights Ireland).

218. In the observations that have been submitted to the Court, two opposing views have been put forward on the nature of these safeguards.

219. According to the first view, propounded by Messrs Watson, Brice and Lewis, Open Rights Group and Privacy International, the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland are mandatory. According to this view, the Court established minimum safeguards that must all be present under the national regime in question so as to limit the interference with fundamental rights to what is strictly necessary.

220. According to the second view, propounded by the German, Estonian, Irish, French and United Kingdom Governments, the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland are merely illustrative. The Court gave an *'overall assessment'* of the safeguards that were absent from the regime provided for by Directive 2006/24, but none of those safeguards, taken in isolation, may be regarded as mandatory in the light of the requirement of strict necessity. To illustrate this view, the German Government has suggested the metaphor of *'communicating vessels'*: a more flexible approach to one of the three aspects identified by the Court (such as access to the retained data) may be compensated by a stricter approach to the other two aspects (the retention period and the security and protection of the data).

221. I am convinced that this *'communicating vessels'* argument must be rejected and that all the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland must be regarded as mandatory, for the following reasons.

222. First of all, the language used by the Court in its examination of the strict necessity of the regime laid down by Directive 2006/24 does not lend itself to such an interpretation. In particular, the Court made no allusion, in paragraphs 60 to 68 of the judgment, to any possibility of *'compensating'* a more flexible approach to one of the three aspects it identified by a stricter approach to the remaining two.

223. It seems to me that, in reality, the *'communicating vessels'* argument arises from confusion between the requirement of necessity and the requirement of proportionality *stricto sensu*, which the Court did not consider in Digital Rights Ireland. As I indicated in [point 186 of this Opinion](#), the requirement of necessity implies the rejection of any measure that is inefficient. In that context there can be no question of any *'overall assessment'*, or of *'compensation'* or of *'weighing up'*, which come into play only when proportionality *stricto sensu* is assessed. (68)

224. Secondly, this *'communicating vessels'* argument would deprive the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland of any practical effect, such that persons whose data have been retained would no longer have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data, as is necessary, according to paragraph 54 of that judgment.

225. The pernicious effect of the *'communicating vessels'* argument may be easily illustrated by the following examples. A national regime that rigorously restricts access to the service of the fight against terrorism and limits the retention period to three months (representing a strict approach to access and retention period), but does not require service providers to retain the data, in encrypted form, within the national territory (representing a flexible approach to security), would expose the entire population to a significant risk of the retained data being accessed unlawfully. Similarly, a national regime that provided for a

retention period of three months and the retention of the data in encrypted form within the national territory (representing a strict approach to retention period and security), but which allowed all employees of all public authorities access to the retained data (representing a flexible approach to access) would expose the entire population to a significant risk of abuse on the part of the national authorities.

226. To my mind, those examples show that, in order to preserve the practical effect of the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland, each of those safeguards must be regarded as mandatory. The European Court of Human Rights also emphasised the fundamental importance of these safeguards in its recent judgment in Szabó and Vissy v. Hungary, making express reference to Digital Rights Ireland. (69)

227. Thirdly, the implementation of these safeguards by those Member States that wish to impose a general data retention obligation would not seem to me to pose any major practical difficulties. In reality, these safeguards seem to me in many respects quite *'minimal'*, as Mr Watson has argued.

228. A number of these safeguards have been debated before the Court because of their possible absence from the national regimes at issue in the main proceedings.

229. First, it is clear from paragraphs 61 and 62 of Digital Rights Ireland that access to and the subsequent use of the retained data must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto.

230. According to Tele2 Sverige and the Commission, that requirement is not satisfied by the Swedish regime at issue in Case C-203/15, which allows the retained data to be accessed for the purpose of combating ordinary offences. A similar criticism has been levelled by Messrs Brice, Lewis and Watson against the United Kingdom regime at issue in Case C-698/15, which authorises access for the purpose of combating ordinary offences, and even in the absence of any offence.

231. Whilst it is not for this Court to reach a finding on the content of those national regimes, it falls within its remit to identify the objectives in the general interest that are capable of justifying serious interference with the rights enshrined in the directive and in Articles 7 and 8 of the Charter. I have already set out the reasons for which I consider that only the fight against serious crime is capable of justifying such interference. (70)

232. Secondly, according to paragraph 62 of Digital Rights Ireland, access to the data retained must be made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued. That prior review must also intervene following a reasoned request of the competent national authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.



233. According to the observations of Tele2 Sverige and the Commission, that safeguard of an independent review preceding access is partly absent from the Swedish regime at issue in Case C-203/15. The same observation, the veracity of which has not been disputed by the United Kingdom Government, has been made by Messrs Brice, Lewis and Watson and by Open Rights Group and Privacy International with regard to the United Kingdom regime at issue in Case C-698/15.

234. I see no reason to take a flexible attitude to this requirement for prior review by an independent body, which indisputably emerges from the language used by the Court in paragraph 62 of Digital Rights Ireland. (71) First of all, such a requirement is dictated by the severity of the interference and of the risks engendered by the establishment of databases covering practically the whole of the population in question. (72) I would note that several experts in the protection of human rights while countering terrorism have criticised the current trend of replacing traditional independent authorisation procedures and effective oversight with 'self-authorisation' systems for giving intelligence and police services access to data. (73)

235. Next, independent review preceding access to data is necessary so that data that is particularly sensitive in terms of the fundamental rights at issue in the main proceedings, such as data that is subject to professional privilege or data which makes it possible to identify a journalist's source, may be dealt with on a case-by-case basis, as indeed the Law Society of England and Wales and the French and German Governments have pointed out. Review preceding access is all the more necessary where it is technically difficult to exclude all data of this kind from retention. (74)

236. Lastly, I would add that, from a practical point of view, none of the three parties concerned by a request for access is in a position to carry out an effective review in connection with access to the retained data. Competent law enforcement authorities have every interest in requesting the broadest possible access. Service providers, who will be ignorant of the content of any investigation file, are incapable of checking that requests for access are limited to what is strictly necessary and persons whose data are consulted have no way of knowing that they are under investigation, even if their data is used abusively or unlawfully, as Messrs Watson, Brice and Lewis have emphasised. Given the nature of the various interests involved, the intervention of an independent body prior to the consultation of retained data, with a view to protecting persons whose data are retained from abusive access by the competent authorities, is to my mind imperative.

237. Having said that, it seems reasonable to me to consider that, in specific situations of extreme urgency, such as the United Kingdom Government has referred to, there may be justification for law enforcement authorities to have immediate access to retained data, without any prior review, in order to prevent the commission of a serious crime or so that the perpetrators can be prosecuted. (75) As far as possible, it is vital that the requirement for prior authorisation be

maintained and an emergency procedure introduced within the independent authority in order to deal with this type of request for access. Nevertheless, if it appears that making an application for access to an independent body is incompatible with the extreme urgency of the situation, there must be an ex post facto review by that body of access to and use of the data and it must be carried out as swiftly as possible.

238. Thirdly, in paragraph 68 of Digital Rights Ireland, the Court established that service providers are under an obligation to retain data within the European Union, in order to facilitate the review, required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security referred to in paragraphs 66 and 67 of that judgment.

239. Tele2 Sverige and the Commission have argued that the retention of data within the national territory is not guaranteed under the Swedish regime at issue in Case C-203/15. The same criticism has been levelled by Messrs Brice, Lewis and Watson against the United Kingdom regime at issue in Case C-698/15.

240. On this point, first of all, I see no reason to attenuate this requirement, established in paragraph 68 of Digital Rights Ireland, since, if data is retained outside the European Union, the level of protection offered by Directive 2002/58 and Articles 7, 8 and 52(1) of the Charter cannot be ensured for persons whose data are retained. (76)

241. Secondly, it seems reasonable to me to transpose this requirement, which the Court expressed with reference to Directive 2006/24, to national regimes and to provide for the retention of data within the national territory, as the German and French Governments and the Commission have submitted. Indeed, in accordance with Article 8(3) of the Charter, every Member State must ensure that an independent authority reviews compliance with the requirements of protection and security on the part of the service providers to which their national regimes apply. In the absence of coordination throughout the European Union, however, those national authorities might find it impossible to fulfil their supervisory duties in other Member States.

242. Fourthly, in so far as the retention period is concerned, the referring courts must apply the criteria defined by the Court in paragraphs 63 and 64 of Digital Rights Ireland. They must determine whether the retained data may be distinguished on the basis of their usefulness and, if so, whether the retention period is adjusted on the basis of that criterion. The referring courts must also check whether the retention period is based on objective criteria such that it may be ensured that it is limited to what is strictly necessary.

243. I would emphasise that, in its recent judgment in Roman Zakharov v. Russia, the European Court of Human Rights held a maximum retention period of six months to be reasonable, while at the same time deploring the lack of any requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained. (77) I would add, in this connection, that the national regimes

at issue in the main proceedings must lay down an obligation to destroy definitively any retained data once it is no longer strictly necessary in the fight against serious crime. That obligation must be observed not only by service providers that retain data, but also by the authorities that have accessed the retained data.

244. Having regard to the foregoing considerations, I consider that all the guarantees described by the Court in paragraphs 60 to 68 of Digital Rights Ireland are mandatory and consequently must accompany any general data retention obligation in order to limit the interference with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter to what is strictly necessary.

245. It is for the referring courts to check that the national regimes at issue in the main proceedings include each of these safeguards.

**6. The proportionality, within a democratic society, of a general data retention obligation in the light of the fight against serious crime**

246. Having verified the necessity of the national regimes at issue in the main proceedings, it will still remain for the referring courts to verify their proportionality, within a democratic society, with reference to the fight against serious crime. This aspect was not examined by the Court in Digital Rights Ireland, since the regime established by Directive 2006/24 went beyond the bounds of what was strictly necessary for the purposes of fighting serious crime.

247. This requirement of proportionality within a democratic society — or proportionality *stricto sensu* — flows both from Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter, as well as from settled case-law: it has been consistently held that a measure which interferes with fundamental rights may be regarded as proportionate only if the disadvantages caused are not disproportionate to the aims pursued. (78)

248. By contrast with the requirements relating to the appropriateness and necessity of the measure in question, which call for an evaluation of the measure's effectiveness in terms of the objective pursued, the requirement of proportionality *stricto sensu* implies weighing the advantages resulting from the measure in terms of the legitimate objective pursued against the disadvantages it causes in terms of the fundamental rights enshrined in a democratic society. (79) This particular requirement therefore opens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in. (80)

249. Consequently, as I indicated in [point 223 of this Opinion](#), it is at the stage when proportionality in the strict sense is considered that it becomes necessary to conduct an overall assessment of the regime in question, and not when the necessity of that measure is examined, as the partisans of the '*communicating vessels*' theory have argued. (81)

250. In accordance with the case-law referred to in [point 247 of this Opinion](#), it is necessary to weigh in the balance the advantages and disadvantages, in a

democratic society, of general data retention obligations. These advantages and disadvantages are intimately linked to the essential characteristic of such obligations — of which they reflect the positive and negative aspects — which is that they relate to all communications effected by all users irrespectively of any connection whatsoever with a serious crime.

251. I have already set out, in [points 178 to 183 of this Opinion](#), the advantages which the retention of data relating to all communications effected within the national territory procure in the fight against serious crime.

252. The disadvantages of general data retention obligations arise from the fact that the vast majority of the data retained will relate to persons who will never be connected in any way with serious crime. It is important, in this connection, to clarify the nature of the disadvantages which those people will suffer. They are, in fact, different in nature depending on the degree of interference in the fundamental rights of those individuals to privacy and the protection of personal data.

253. In so far as concerns '*individual*' interference, affecting a given individual, the disadvantages resulting from a general data retention obligation were very accurately described by Advocate General Cruz Villalón in points 72 to 74 of his Opinion in Digital Rights Ireland. (82) In the words of the Advocate General, the use of such data makes it possible '*to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity*'.

254. In other words, in an individual context, a general data retention obligation will facilitate equally serious interference as targeted surveillance measures, including those which intercept the content of communications.

255. Whilst the severity of such individual interference should not be underestimated, it nevertheless seems to me that the specific risks engendered by a general data retention obligation become apparent in the context of '*mass*' interference.

256. Indeed, by contrast with targeted surveillance measures, a general data retention obligation is liable to facilitate considerably mass interference, that is to say interference affecting a substantial portion, or even all of the relevant population. This may be illustrated by the following examples.

257. Let us suppose, first of all, that a person who has access to retained data wishes to identify all the individuals in the Member State who have a psychological disorder. Analysing the content of all communications effected within the national territory for that purpose would require considerable resources. On the other hand, by using databases of communications data, it would be possible instantly to identify all the individuals who have contacted a psychologist during the data retention period. (83) I might add that that technique could be extended to any

of the fields of specialist medicine registered in a Member State. (84)

258. Now let us suppose that that same person wished to identify individuals opposed to the policies of the incumbent government. Again, analysing the content of communications for that purpose would require considerable resources, whereas, by using communications data it would be possible to identify all individuals on the distribution list of emails criticising government policy. Furthermore, such data would also make it possible to identify individuals taking part in any public demonstration against the government. (85)

259. I would emphasise that the risks associated with access to communications data (or ‘*metadata*’) may be as great or even greater than those arising from access to the content of communications, as has been pointed out by Open Rights Group, Privacy International and the Law Society of England and Wales, as well as in a recent report by the United Nations High Commissioner for Human Rights. (86) In particular, as the examples I have given demonstrate, ‘*metadata*’ facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not.

260. I would add that there is nothing theoretical about the risks of abusive or illegal access to retained data. The risk of abusive access on the part of competent authorities must be put in the context of the extremely high number of requests for access to which reference has been made in the observations submitted to the Court. In so far as the Swedish regime is concerned, Tele2 Sverige has stated that it was receiving approximately 10 000 requests monthly, a figure that does not include requests received by other service providers operating in Sweden. In so far as the United Kingdom regime is concerned, Mr Watson has reproduced a number of extracts from an official report which records 517 236 authorisations and 55 346 urgent oral authorisations for 2014 alone. The risk of illegal access, on the part of any person, is as substantial as the existence of computerised databases is extensive. (87)

261. In my view, it falls to the referring courts to determine, in accordance with the case-law referred to [in point 247 of this Opinion](#), whether the disadvantages caused by the general data retention obligations at issue in the main proceedings are not disproportionate, within a democratic society, to the objectives pursued. In carrying out that assessment, those courts must weigh the risks posed by such obligations against the advantages they offer, which are the following:

- the advantages associated with giving the authorities whose task it is to fight serious crime a certain ability to examine the past, (88) and

- the serious risks which, in a democratic society, arise from the power to catalogue the private lives of individuals and to catalogue a population in its entirety.

262. That assessment must take account of all the relevant characteristics of the national regimes at issue

in the main proceedings. I would emphasise, in this connection, that the mandatory safeguards described by the Court in paragraphs 60 to 68 of *Digital Rights Ireland* are no more than minimum safeguards aimed at limiting the interference with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter to what is strictly necessary. Consequently, a national regime which includes all of those safeguards may nevertheless be considered disproportionate, within a democratic society, as a result of a lack of proportion between the serious risks engendered by such an obligation, in a democratic society, and the advantages it offers in the fight against serious crime.

## VI – Conclusion

263. In light of the foregoing, I propose that the Court’s answer to the question referred for a preliminary ruling by the Kamarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) should be as follows:

Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (‘*Directive on privacy and electronic communications*’), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, and Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union are to be interpreted as not precluding Member States from imposing on providers of electronic communications services an obligation to retain all data relating to communications effected by the users of their services where all of the following conditions are satisfied, which it is for the referring courts to determine in the light of all the relevant characteristics of the national regimes at issue in the main proceedings:

- the obligation and the safeguards which accompany it must be provided for in legislative or regulatory measures possessing the characteristics of accessibility, foreseeability and adequate protection against arbitrary interference;

- the obligation and the safeguards which accompany it must observe the essence of the rights recognised by Articles 7 and 8 of the Charter of Fundamental Rights;

- the obligation must be strictly necessary in the fight against serious crime, which means that no other measure or combination of measures could be as effective in the fight against serious crime while at the same time interfering to a lesser extent with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter of Fundamental Rights;

- the obligation must be accompanied by all the safeguards described by the Court in paragraphs 60 to 68 of its judgment of 8 April 2014 in *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238) concerning access to the data, the period of retention and the protection and security of the data, in order to limit the interference with the rights enshrined in Directive 2002/58 and Articles 7



and 8 of the Charter of Fundamental Rights to what is strictly necessary; and

– the obligation must be proportionate, within a democratic society, to the objective of fighting serious crime, which means that the serious risks engendered by the obligation, in a democratic society, must not be disproportionate to the advantages which it offers in the fight against serious crime.

---

1 – Original language: French.

2 – Madison, J., ‘Federalist No. 51’, in Hamilton, A., Madison, J., and Jay, J., ed. *Genovese, M.A., The Federalist Papers*, Palgrave Macmillan, New York, 2009, p. 120. Madison was one of the principal authors and one of the 39 signatories of the United States Constitution (1787). He went on to become the fourth President of the United States (from 1809 to 1817).

3 – This ability to ‘examine the past’ may be especially helpful in identifying potential accomplices: see points 178 to 184 of this Opinion.

4 – See points 252 to 261 of this Opinion.

5 – Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (‘Directive on privacy and electronic communications’) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).

6 – Judgment of 8 April 2014 (C-293/12 and C-594/12, EU:C:2014:238).

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

8 – It is understandable that this should be so, given that the national regimes were intended to transpose the directive, which has now been declared invalid.

9 – See the description of the national regimes at issue in the main proceedings given in points 11 to 13 and 36 of this Opinion.

10 – Opinion 2/13 of 18 December 2014 (EU:C:2014:2454, paragraph 179), and the judgment of 15 February 2016 in *N.* (C-601/15 PPU, EU:C:2016:84, paragraph 45 and the case-law cited).

11 – In accordance with the third subparagraph of Article 6(1) TEU and Article 52(7) of the Charter, regard must be had to the explanations relating to the Charter when interpreting the Charter (see judgments of 26 February 2013 in *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 20, and 15 February 2016 in *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 47). According to those explanations, Article 7 of the Charter corresponds to Article 8 of the ECHR, while Article 8 of the Charter does not correspond to any right in the ECHR.

12 – See, inter alia, judgments of 9 November 2010 in *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 40 and the case-law cited), and 24 April 2012 in *Kamberaj* (C-571/10, EU:C:2012:233, paragraph 42 and the case-law cited).

13 – See, inter alia, judgment of 16 September 1982 in *Vlaeminck* (132/81, EU:C:1982:294, paragraph 13); order of 24 March 2011 in *Abt and Others* (C-194/10, EU:C:2011:182, paragraphs 36 and 37 and the case-law cited); and judgment of 24 October 2013 in *Stoilov i Ko* (C-180/12, EU:C:2013:693, paragraph 46 and the case-law cited).

14 – See points 126 to 262 of this Opinion.

15 – See points 123 to 125 of this Opinion.

16 – Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

17 – Judgment of 6 November 2003 in *Lindqvist* (C-101/01, EU:C:2003:596, paragraphs 43 and 44).

18 – Judgment of 10 February 2009 (C-301/06, EU:C:2009:68).

19 – Judgment of 10 February 2009 in *Ireland v Parliament and Council* (C-301/06, EU:C:2009:68, paragraph 80).

20 – Since Directive 2002/58 may be regarded as a *lex specialis vis-à-vis* Directive 95/46 (see Article 1(2) of Directive 2002/58), I do not think it necessary to verify the compatibility of general data retention obligations with the regime established by Directive 95/46, which, moreover, is not mentioned in the questions that have been referred to the Court. For the sake of completeness, I would nevertheless add that the wording of Article 13(1) of Directive 95/46 allows the Member States greater latitude than that of Article 15(1) of Directive 2002/58, the scope of which is limited to the sphere of the provision of publicly available electronic communications services. Since the possibility provided for in Article 15(1) of Directive 2002/58 enables the Member States to impose general data retention obligations, I infer that Article 13(1) of Directive 95/46 does also.

21 – See points 126 to 262 of this Opinion.

22 – The Court’s settled case-law indeed states that the fundamental rights guaranteed in the legal order of the European Union are applicable in all situations governed by EU law, but not outside such situations. Accordingly, the Court has already pointed out that it has no power to examine the compatibility with the Charter of national legislation lying outside the scope of EU law. On the other hand, if such legislation falls within the scope of EU law, the Court, when requested to give a preliminary ruling, must provide all the guidance as to interpretation needed in order for the national court to determine whether that legislation is compatible with the fundamental rights the observance of which the Court ensures (see judgment of 26 February 2013 in *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 19 and the case-law cited).

23 – See point 88 of this Opinion.

24 – See points 90 to 97 of this Opinion.

25 – To be more precise, the second sentence of Article 51(1) of the Charter provides that the Member States must observe the rights guaranteed by the Charter when they are implementing EU law.

26 – On the scope of this exclusion, see points 90 to 97 of this Opinion.

27 – See points 185 to 262 of this Opinion.

28 – See, in particular, United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of 17 April 2013, A/HRC/23/40, paragraph 33: ‘Technological advancements mean that the State’s effectiveness in conducting surveillance is no longer limited by scale or duration. ... As such, the State now has a greater capacity to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.’ See also paragraph 50: ‘Generally, legislation has not kept pace with the changes in technology. In most States, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment.’

29 – I shall nevertheless come back to the specific risks posed by the creation of such vast databases when I address the requirement of proportionality, within a democratic society, pertaining to general data retention obligations such as those at issue in the main proceedings. See points 252 to 261 of this Opinion.

30 – See, on this point, the argument put forward by Open Rights Group and Privacy International, summarised in point 104 of this Opinion.

31 – I find confirmation of the cumulative nature of the requirements in the last sentence of Article 15(1) of Directive 2002/58, which provides that ‘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) [TEU]’. Pursuant to Article 6(1) TEU, ‘The Union recognises the rights, freedoms and principles set out in the [Charter], which shall have the same legal value as the Treaties’.

32 – As a logical consequence of their cumulative nature, where the requirements of those two provisions overlap, the stricter of the two must be applied, that is to say, the requirement that affords greater protection of the right in question.

33 – Judgment of 17 December 2015 (C-419/14, EU:C:2015:832).

34 – See, inter alia, judgments of 17 October 2013 in Schwarz (C-291/12, EU:C:2013:670, paragraph 35) (interference provided for by an EU regulation); 27 May 2014 in Spasic (C-129/14 PPU, EU:C:2014:586, paragraph 57) (interference provided for by the Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, which was signed on 19 June 1990 and came into force on 26

March 1995); 6 October 2015 in Delvigne (C-650/13, EU:C:2015:648, paragraph 47) (interference provided for by the French Electoral Code and the French Criminal Code); and 17 December 2015 in Neptune Distribution (C-157/14, EU:C:2015:823, paragraph 69) (interference provided for by an EU regulation and an EU directive).

35 – Judgment of 1 July 2010 in Knauf Gips v Commission (C-407/08 P, EU:C:2010:389, paragraphs 87 to 92) (interference having no legal basis).

36 – C-70/10, EU:C:2011:255, paragraphs 94 to 100.

37 – See, in particular, ECtHR, 14 September 2010, Sanoma Uitgevers B.V. v. The Netherlands, EC:ECHR:2010:0914JUD003822403, § 83.

38 – See, in particular, ECtHR, 26 March 1987, Leander v. Sweden, EC:ECHR:1987:0326JUD000924881, § 50 and 51; ECtHR, 26 October 2000, Hassan and Tchaouch v. Bulgaria, CE:ECHR:2000:1026JUD003098596, § 84; ECtHR, 4 December 2008, S. and Marper v. United Kingdom, EC:ECHR:2008:1204JUD003056204, § 95; ECtHR, 14 September 2010, Sanoma Uitgevers B.V. v. The Netherlands, EC:ECHR:2010:0914JUD003822403, §§ 81 to 83; ECtHR, 31 March 2016, and Stoyanov and Others v. Bulgaria, EC:ECHR:2016:0331JUD005538810, § 124 to 126.

39 – More precisely, the Court cannot, in my view, adopt an interpretation of the requirement for a legal basis that is more permissive than that of the ECtHR, one that would allow more instances of interference than would result from the ECtHR’s interpretation of that requirement.

40 – The concept of ‘provided for by law’ is used in Article 8(2) ECHR (right to respect for private and family life) (‘in accordance with the law’), Article 9(2) ECHR (freedom of thought, conscience and religion) (‘prescribed by law’), Article 10(2) ECHR (freedom of expression) and Article 11(2) ECHR (freedom of assembly and association) (‘prescribed by law’). In the Charter, Article 52(1) applies to any limitation on the exercise of the rights enshrined in the Charter, where such limitations are in fact permitted.

41 – See, to that effect, Peers, S., ‘Article 52 — Scope of guaranteed rights’ in Peers, S., et al., *The EU Charter of Fundamental Rights: a Commentary*, Oxford, OUP, 2014, No 52.39.

42 – See, inter alia, judgments of 30 May 2013 in Asbeek Brusse and de Man Garabito (C-488/11, EU:C:2013:341, paragraph 26); 24 June 2015 in Hotel Sava Rogaška (C-207/14, EU:C:2015:414, paragraph 26); and 26 February 2015 in Christie’s France (C-41/14, EU:C:2015:119, paragraph 26).

43 – See, in particular, ECtHR, 14 September 2010, Sanoma Uitgevers B.V. v. The Netherlands, EC:ECHR:2010:0914JUD003822403, § 83: ‘the [word “law”] which [appears] in Articles 8 to 11 of the [ECHR includes] both “written law”, encompassing enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under

independent rule-making powers delegated to them by Parliament, and unwritten law. “Law” must be understood to include both statutory law and judge-made “law”.

44 – That requirement does not emerge from the wording of Article 15(1) of Directive 2002/58 or from the general structure of Directive 2002/58, for the reasons which I set out in points 99 to 116 of this Opinion.

45 – See the description of the national regimes at issue in the main proceedings given above, especially points 13 and 36.

46 – Digital Rights Ireland, paragraph 54. See the description of the national regimes at issue in the main proceedings, at points 29 to 33 and 45 and 46 above.

47 – Digital Rights Ireland, paragraph 42 and the case-law cited.

48 – Judgment of 29 January 2008 (C-275/06, EU:C:2008:54, paragraphs 50 to 54).

49 – Judgment of 29 January 2008 (C-275/06, EU:C:2008:54).

50 – See points 252 to 261 of this Opinion.

51 – As regards necessity, see points 185 to 245 of this Opinion.

52 – As regards proportionality, *stricto sensu*, see points 246 to 262 of this Opinion.

53 – The Commission too has emphasised that the additional value of general data retention obligations over and above that of targeted data preservation lies in this limited ability to examine the past: see the Commission’s Staff Working Document annexed to the proposal for a directive which led to the adoption of Directive 2006/24, SEC(2005) 1131, 21 September 2005, Section 3.6, ‘Data Preservation versus Data Retention’: ‘with only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified — data retention is indispensable in many cases to actually identify those suspects’.

54 – The French Government has referred in this connection to the report of its Conseil d’État entitled *Le numérique et les droits fondamentaux*, 2014, pp. 209 and 210. The Conseil d’État states that a system of targeted surveillance measures ‘would be significantly less effective than systematic data retention from the point of view of national security and identifying criminals. Such a system affords no retrospective access to exchanges that took place before the authorities identified a threat or discovered a crime: its operational character would thus depend on the authorities’ ability to anticipate whose connection data might be useful, something which it would be impossible for the judicial police to do. In the case of a crime, for example, a court would have no access to communications effected prior to the crime, even though that information could be valuable or even indispensable in identifying the offender and his accomplices, as has been shown by certain recent cases involving terrorist attacks. In the sphere of the prevention of acts endangering national security, new

technical programmes rely on an ability to detect weak signals, something which is incompatible with the concept of the advance targeting of dangerous persons’.

55 – The Commission’s Staff Working Document annexed to the proposal for a directive which led to the adoption of Directive 2006/24, SEC(2005) 1131, 21 September 2005, Section 1.2, ‘The importance of traffic data for law enforcement’.

56 – See, *inter alia*, judgments of 22 January 2013 in *Sky Österreich* (C-283/11, EU:C:2013:28, paragraphs 54 to 57); 13 November 2014 in *Reindl* (C-443/13, EU:C:2014:2370, paragraph 39); and 16 July 2015 in *CHEZ Razpredelenie Bulgaria* (C-83/14, EU:C:2015:480, paragraphs 120 to 122). In legal theory, see, in particular, Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 29: ‘Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value.’

57 – See Rivers, J., ‘Proportionality and variable intensity of review’, *The Cambridge Law Journal*, vol. 65, issue 1 (2006) 174, p. 198: ‘The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise, an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest.’

58 – On the two elements of the test of necessity, see Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, pp. 323 to 331.

59 – See, *inter alia*, the judgments of 9 November 2010 in *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraphs 77 and 86), and 7 November 2013 in *IPI* (C-473/12, EU:C:2013:715, paragraph 39).

60 – See points 117 to 125 of this Opinion.

61 – See points 216 to 245 of this Opinion.

62 – See paragraph 65 of *Digital Rights Ireland*: ‘It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary’ (my italics).

63 – Judgment of 6 October 2015 (C-362/14, EU:C:2015:650).

64 – See points 178 to 183 of this Opinion.

65 – See the ‘Issue Paper on the rule of law on the Internet and in the wider digital world’, published by the Council of Europe Commissioner for Human Rights, December 2014, CommDH/IssuePaper(2014)1, p. 115, the report of the United Nations High Commissioner for Human Rights (Human Rights Council) on the right to privacy in the digital age of 30



June 2014, A/HRC/27/37, paragraph 26, and the report of the Special Rapporteur (United Nations, General Assembly) on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 23 September 2014, A/69/397, paragraphs 18 and 19.

66 – That observation relates solely to general data retention obligations (which are liable to cover all persons whether or not they have any connection with a serious crime), not to targeted surveillance measures (which are focused on persons who have already been identified as being connected with a serious crime). On this distinction, see points 178 to 183 of this Opinion.

67 – The German Government in particular stated at the hearing that the German Parliament had excluded emails from the retention obligation imposed under German law, but that its regime covered all users and all of the national territory.

68 – See Barak, A., *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, p. 344: ‘The first three components of proportionality deal mainly with the relation between the limiting law’s purpose and the means to fulfil that purpose. ... Accordingly, those tests are referred to as means-end analysis. They are not based on balancing. The test of proportionality *stricto sensu* is different. ... It focuses on the relation between the benefit in fulfilling the law’s purpose and the harm caused by limiting the constitutional right. It is based on balancing’ (my italics).

69 – ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, EC:ECHR:2016:0112JUD003713814, § 68: ‘Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens’ trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens’ private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities’ enhanced technical possibilities to intercept private information.’

70 – See points 170 to 173 of this Opinion.

71 – I would nevertheless clarify that this requirement for a prior, independent review cannot, in my view, arise from Article 8(3) of the Charter, since the Charter does not apply, as such, to national provisions governing access to retained data: see points 123 to 125 of this Opinion.

72 – See points 252 to 261 of this Opinion.

73 – United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 28 December 2009, A/HRC/13/37, paragraph 62: ‘there must be no secret surveillance system that is not under the review of an effective oversight body and all interferences must be

authorised through an independent body’ (see also paragraph 51). See also the Report of the Special Rapporteur (United Nations, General Assembly) on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 23 September 2014, A/69/397, paragraph 61.

74 – See point 212 of this Opinion. As regards journalists’ sources, the ECtHR has emphasised the need for prior authorisation by an independent body, inasmuch as an *ex post facto* review cannot re-establish the confidentiality of such sources: see ECtHR, 22 November 2012, Telegraaf Media Nederland Landelijke Media B.V. and Others v. The Netherlands, EC:ECHR:2012:1122JUD003931506, § 101, and ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, EC:ECHR:2016:0112JUD003713814, § 77. In its judgment in *Kopp v. Switzerland*, which concerned the surveillance of a lawyer’s telephone lines, the ECtHR criticised the fact that an official within the authority was instructed to filter out information covered by professional privilege, without any oversight on the part of an independent court: see ECtHR, 25 March 1998, *Kopp v. Switzerland*, EC:ECHR:1998:0325JUD002322494, § 74.

75 – See, in this connection, the mechanism described in point 22 of this Opinion. I would emphasise that this issue was not addressed by the Court in *Digital Rights Ireland*.

76 – See, on this point, judgment of 6 October 2015 in *Schrems* (C-362/14, EU:C:2015:650).

77 – See ECtHR, 4 December 2015, *Roman Zakharov v. Russia*, EC:ECHR:2015:1204JUD004714306, § 254 and 255. Under Russian law, intercept material must be destroyed after six months of storage if the person concerned has not been charged with a criminal offence. The ECtHR considered the six-month storage time limit set out in Russian law for such data reasonable. At the same time, it deplored the lack of any requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained and stated that the automatic storage for six months of clearly irrelevant data could not be considered justified under Article 8 of the ECHR.

78 – See, in particular, judgments of 15 February 2016 in *N.* (C-601/15 PPU, EU:C:2016:84, paragraph 54; the necessity of the measure was examined in paragraphs 56 to 67, its proportionality in paragraphs 68 and 69); 16 July 2015 in *CHEZ Razpredelenie Bulgaria* (C-83/14, EU:C:2015:480, paragraph 123; the necessity was addressed in paragraphs 120 to 122, its proportionality in paragraphs 123 to 127); and 22 January 2013 in *Sky Österreich* (C-283/11, EU:C:2013:28, paragraph 50; the necessity of the measure was examined in paragraphs 54 to 57, its proportionality in paragraphs 58 to 67).

79 – See Rivers, J., ‘Proportionality and variable intensity of review’ in *The Cambridge Law Journal*, vol. 65, issue 1 (2006) p. 174, at p. 198: ‘It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters

out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable.’

80 – See Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 30: ‘In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail.’

81 – The particular nature of the requirement of proportionality *stricto sensu* by comparison with the requirements of appropriateness and necessity may be illustrated by the following example. Let us suppose that a Member State were to require every person residing within its territory to have a geolocation electronic chip injected into their body, one that enabled the authorities to retrace the comings and goings of the wearer over the past year. Such a measure might be considered ‘necessary’ if no other measure were capable of achieving the same degree of effectiveness in the fight against serious crime. However, to my mind, it would be disproportionate within a democratic society, since the disadvantages resulting from the interference with the rights to physical integrity, privacy and the protection of personal data would be disproportionate to the advantages offered in terms of the fight against serious crime.

82 – C-293/12 and C-594/12, EU:C:2013:845. See also *Digital Rights Ireland*, paragraphs 27 and 37.

83 – The data retained include the identity of the sender and the recipient of every communication, and it would merely be necessary to cross-reference that data with a list of telephone numbers of psychologists practising in the country.

84 – See, in this connection, United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism of 28 December 2009, A/HRC/13/37, paragraph 42: ‘in Germany, research showed a chilling effect of data retention policies: 52 percent of persons interviewed said they probably would not use telecommunication for contact with drug counsellors, psychotherapists or marriage counsellors because of data retention laws’.

85 – Since the data retained include the location of the source and destination of every communication, any person initiating or receiving a communication during a demonstration could easily be identified using that data. Marc Goodman, an FBI and Interpol expert on the risks posed by new technologies, relates that, recently, the Ukrainian Government proceeded to identify, during an opposition demonstration, all mobile telephones located in the vicinity of street battles between law enforcers and government opponents. All those telephones then received a message which Mr Goodman describes as maybe the most Orwellian text message a government’s ever sent: ‘Dear subscriber, you are

registered as a participant in a mass disturbance’ (Goodman, M., *Future Crimes*, Anchor Books, New York, 2016, p. 153). See also United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, paragraph 75, and the report of the United Nations High Commissioner for Human Rights (Human Rights Council) on the right to privacy in the digital age, 30 June 2014, A/HRC/27/37, paragraph 3.

86 – See the report of the United Nations High Commissioner for Human Rights (Human Rights Council) on the right to privacy in the digital age, 30 June 2014, A/HRC/27/37, paragraph 19: ‘in a similar vein, it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as “metadata” may give an insight into an individual’s behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication’ (my italics). See also the report of the Special Rapporteur (United Nations, General Assembly) on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 23 September 2014, A/69/397, paragraph 53.

87 – See, in particular, United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, paragraph 67: ‘Databases of communications data become vulnerable to theft, fraud and accidental disclosure.’

88 – See points 178 to 183 of this Opinion.