СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

JUDGMENT OF THE COURT (Grand Chamber)

EN

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:

* * Languages of the case: English and Swedish.

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, Rechtsanwalte,

– 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. Bréchot 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

...’

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.

...

1b. 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 integritetsskyddsnämnden (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 additions, 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 Kammarrätten 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 Kammarrätten 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 then 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, *Pohotovosť*, 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.**

Lenaerts Tizzano Silva de Lapuerta

von Danwitz Da Cruz Vilaça Juhász

Vilaras Borg Barthet Malenovský

Levits Bonichot Arabadjiev

Rodin Biltgen Lycourgos

Delivered in open court in Luxembourg on 21 December 2016.

A. Calot Escobar K. Lenaerts

Registrar President