JUDGMENT OF THE COURT (Grand Chamber)

6 October 2020 (*)

(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Providers of electronic communications services – General and indiscriminate transmission of traffic data and location data – Safeguarding of national security – Directive 2002/58/EC – Scope – Article 1(3) and Article 3 – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Article 4(2) TEU)

In Case C-623/17,

REQUEST for a preliminary ruling under Article 267 TFEU from the Investigatory Powers Tribunal (United Kingdom), made by decision of 18 October 2017, received at the Court on 31 October 2017, in the proceedings

Privacy International

v

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb and L.S. Rossi, Presidents of Chambers, J. Malenovský, L. Bay Larsen, T. von Danwitz (Rapporteur), C. Toader, K. Jürimäe, C. Lycourgos and N. Piçarra, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 9 and 10 September 2019,

after considering the observations submitted on behalf of:

– Privacy International, by B. Jaffey QC and T. de la Mare QC, by D. Cashman, Solicitor, and by H. Roy, avocat,

– the United Kingdom Government, by Z. Lavery, D. Guðmundsdóttir and S. Brandon, acting as Agents, by G. Facenna QC and D. Beard QC, and by C. Knight and R. Palmer, Barristers,

– the Belgian Government, by P. Cottin and J.-C. Halleux, acting as Agents, and by J. Vanpraet, advocaat, and E. de Lophem, avocat,

– the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,

– the German Government, initially by M. Hellmann, R. Kanitz, D. Klebs and T. Henze, and subsequently by J. Möller, M. Hellmann, R. Kanitz and D. Klebs, acting as Agents,

– the Estonian Government, by A. Kalbus, acting as Agent,

– Ireland, by M. Browne, G. Hodge and A. Joyce, acting as Agents, and by D. Fennelly, Barrister,

– the Spanish Government, initially by L. Aguilera Ruiz and M.J. García-Valdecasas Dorrego, and subsequently by L. Aguilera Ruiz, acting as Agents,

– the French Government, initially by E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas and D. Dubois, and subsequently by E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune and D. Dubois, acting as Agents,

– the Cypriot Government, by E. Symeonidou and E. Neofytou, acting as Agents,

– the Latvian Government, initially by V. Soņeca and I. Kucina, and subsequently by V. Soņeca, acting as Agents,

– the Hungarian Government, initially by G. Koós, M.Z. Fehér, G. Tornyai and Z. Wagner, and subsequently by G. Koós and M.Z. Fehér, acting as Agents,

– the Netherlands Government, by C.S. Schillemans and M.K. Bulterman, acting as Agents,

– the Polish Government, by B. Majczyna, J. Sawicka and M. Pawlicka, acting as Agents,

– the Portuguese Government, by L. Inez Fernandes, M. Figueiredo and F. Aragão Homem, acting as Agents,

– the Swedish Government, initially by A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren and A. Alriksson, and subsequently by H. Shev, C. Meyer-Seitz, L. Zettergren and A. Alriksson, acting as Agents,

– the Norwegian Government, by T.B. Leming, M. Emberland and J. Vangsnes, acting as Agents,

– the European Commission, initially by H. Kranenborg, M. Wasmeier, D. Nardi and P. Costa de Oliveira, and subsequently by H. Kranenborg, M. Wasmeier, and D. Nardi, acting as Agents,

– the European Data Protection Supervisor, by T. Zerdick and A. Buchta, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 15 January 2020,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 1(3) and Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (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 Article 4(2) TEU and Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between Privacy International and the Secretary of State for Foreign and Commonwealth Affairs (United Kingdom), the Secretary of State for the Home Department (United Kingdom), Government Communications Headquarters (United Kingdom) ('GCHQ'), the Security Service (United Kingdom) ('MI5') and the Secret Intelligence Service (United Kingdom) ('MI6') concerning the legality of legislation authorising the acquisition and use of bulk communications data by the security and intelligence agencies.

Legal context

European Union law

Directive 95/46

3 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), was repealed, with effect from 25 May 2018, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1). Article 3 of that directive, entitled 'Scope', was worded as follows:

'1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI [TEU] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

– by a natural person in the course of a purely personal or household activity.'

Directive 2002/58

4 Recitals 2, 6, 7, 11, 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 [the 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], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, 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, [signed in Rome on 4 November 1950], 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.

…

(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. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

…

(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. Traffic data used for marketing communications services … should also be erased or made anonymous ….

…

(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. …'

5 Article 1 of Directive 2002/58, entitled 'Scope and aim', provides:

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

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

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

6 According to Article 2 of that directive, entitled ‘Definitions’:

‘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:

(a) “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(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;

…’

7 Article 3 of that directive, entitled ‘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 European Union], including public communications networks supporting data collection and identification devices.’

8 Under Article 5 of Directive 2002/58, entitled ‘Confidentiality of the communications’:

‘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, entitled '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 of that directive, entitled 'Location data other than traffic data', provides, in paragraph 1 thereof:

'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, entitled 'Application of certain provisions of [Directive 95/46]', states,

in paragraph 1 thereof:

‘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 [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.’

Regulation 2016/679

12 Article 2 of Regulation 2016/679 provides:

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

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

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

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

…

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

…’

13 Article 4 of that regulation provides:

‘For the purposes of this Regulation:

…

(2) “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…’

14 Under Article 23(1) of that regulation:

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

safeguard:

(a) national security;

(b) defence;

(c) public security;

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

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

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

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

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

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

(j) the enforcement of civil law claims.'

15 Under Article 94(2) of Regulation 2016/679:

'References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of [Directive 95/46] shall be construed as references to the European Data Protection Board established by this Regulation.'

United Kingdom law

16 Section 94 of the Telecommunications Act 1984, in the version applicable to the facts in the main proceedings ('the 1984 Act'), entitled 'Directions in the interests of national security etc.', provides:

'(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.

(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.

(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under

Part 1 or Chapter 1 of Part 2 of the Communications Act 2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.

(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of [the] opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

…

(8) This section applies to [the Office of Communications (OFCOM)] and to providers of public electronic communications networks.'

17 Section 21(4) and (6) of the Regulation of Investigatory Powers Act 2000 ('the RIPA') provides:

'(4) … "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.

…

(6) … "traffic data", in relation to any communication, means—

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication.

…’

18 Sections 65 to 69 of the RIPA lay down the rules on the functioning and jurisdiction of the Investigatory Powers Tribunal (United Kingdom). Under section 65 of the RIPA, a complaint may be made to the Investigatory Powers Tribunal if there is reason to believe that data has been acquired inappropriately.

The dispute in the main proceedings and the questions referred for a preliminary ruling

19 At the beginning of 2015, the existence of practices for the acquisition and use of bulk communications data by the various security and intelligence agencies of the United Kingdom, namely GCHQ, MI5 and MI6, was made public, including in a report by the Intelligence and Security Committee of Parliament (United Kingdom). On 5 June 2015, Privacy International, a non-governmental organisation, brought an action before the Investigatory Powers Tribunal (United Kingdom) against the Secretary of State for Foreign and Commonwealth Affairs, the Secretary of State for the Home Department and those security and intelligence agencies, challenging the lawfulness of those practices.

20 The referring court examined the lawfulness of those practices in the light, first of all, of national law and the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (‘the ECHR’), and, subsequently, of EU law. In a judgment of 17 October 2016, that court held that the defendants in the main proceedings had acknowledged that those agencies acquired and used, in their activities, sets of bulk personal data, such as biographical data or travel data, financial or commercial information, communications data liable to include sensitive data covered by professional secrecy, or journalistic material. That data, obtained by various, possibly secret, means, would be analysed by cross-checking and by automated processing and could be disclosed to other persons and authorities and shared with foreign partners. In that context, the security and intelligence agencies would also use bulk communications data, acquired from providers of public electronic communications networks under, inter alia, directions issued by a Secretary of State on the basis of section 94 of the 1984 Act. GCHQ and MI5 have been doing this since 2001 and 2005 respectively.

21 The referring court found that those measures for the acquisition and use of data were consistent with national law and, since 2015, subject to issues that remained under consideration concerning the proportionality of those measures and the transfer of data to third parties, with Article 8 ECHR. In that regard, it stated that evidence had been submitted to it concerning the applicable safeguards, in particular as regards the procedures for accessing and disclosing data outside the security and intelligence agencies, the arrangements for retaining data, and independent oversight arrangements.

22 As regards the lawfulness of the acquisition and use measures at issue in the main proceedings in the light of EU law, the referring court examined, in a judgment of 8 September 2017, whether those measures fell within the scope of EU law and, if so, whether they were compatible with EU law. That court found, as regards bulk communications data, that the providers of electronic communications networks were required, under section 94 of the 1984 Act, should a Secretary of State issue directions to that effect, to provide the security and intelligence agencies with data collected in the course of their economic activity falling within the scope of EU law. However, that was not the case for the acquisition of other data obtained by those agencies without the use of such binding powers. On the basis of that finding, the referring court considered it necessary to refer questions to the Court in order to determine whether a regime such as that resulting from section 94 of the 1984 Act falls within the scope of EU law and, if so, whether and in what way the requirements laid down by the case-law resulting from the judgment of 21 December 2016, *Tele2 Sverige* and *Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970; ‘*Tele2*’) apply to that regime.

23 In that regard, in its request for a preliminary ruling, the referring court states that, pursuant to

section 94 of the 1984 Act, the Secretary of State may give providers of electronic communications services such general or specific directions as appear to him to be necessary in the interests of national security or relations with a foreign government. Referring to the definitions set out in section 21(4) and (6) of the RIPA, that court states that the data concerned includes traffic data and service use information, within the meaning of that provision, with only the content of communications being excluded. Such data and information make it possible, in particular, to know the 'who, where, when and how' of a communication. That data is transmitted to the security and intelligence agencies and retained by them for the purposes of their activities.

24 According to the referring court, the regime at issue in the main proceedings differs from that resulting from the Data Retention and Investigatory Powers Act 2014, at issue in the case which gave rise to the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970), since the latter regime provided for the retention of data by providers of electronic communications services and the making available of that data not only to security and intelligence agencies, in the interests of national security, but also to other public authorities, depending on their needs. Furthermore, that judgment concerned a criminal investigation, not national security.

25 The referring court adds that the databases compiled by the security and intelligence agencies are subject to bulk, unspecific, automated processing, with the aim of discovering unknown threats. To that end, the referring court states that the sets of metadata thus compiled should be as comprehensive as possible, so as to have a 'haystack' in order to find the 'needle' hidden therein. As regards the usefulness of bulk data acquisition by those agencies and the techniques for consulting that data, that court refers in particular to the findings of the report drawn up on 19 August 2016 by David Anderson QC, then United Kingdom Independent Reviewer of Terrorism Legislation, who relied, when drawing up that report, on a review conducted by a team of intelligence specialists and on the testimony of security and intelligence agency officers.

26 The referring court also states that, according to Privacy International, the regime at issue in the main proceedings is unlawful in the light of EU law, while the defendants in the main proceedings consider that the obligation to transfer data provided for by that regime, access to that data and its use do not fall within the competences of the European Union, in accordance, in particular, with Article 4(2) TEU, according to which national security remains the sole responsibility of each Member State.

27 In that regard, the Investigatory Powers Tribunal considers, on the basis of the judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346, paragraphs 56 to 59), concerning the transfer of passenger name record data for the purpose of protecting public security, that the activities of commercial undertakings in processing and transferring data for the purpose of protecting national security do not appear to fall within the scope of EU law. For the referring court, it is necessary to examine not whether the activity in question constitutes data processing, but only whether, in substance and effect, the purpose of such activity is to advance an essential State function, within the meaning of Article 4(2) TEU, through a framework established by the public authorities that relates to public security.

28 Should the measures at issue in the main proceedings nevertheless fall within the scope of EU law, the referring court considers that the requirements set out in paragraphs 119 to 125 of the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970) appear inappropriate in the context of national security and would undermine the ability of the security and intelligence agencies to tackle some threats to national security.

29 In those circumstances, the Investigatory Powers Tribunal decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'In circumstances where:

(a) the [security and intelligence agencies'] capabilities to use [bulk communications data]

supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;

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

(c) the provider of an electronic communications network is not thereafter required to retain [the bulk communications data] (beyond the period of their ordinary business requirements), which [are] retained by the State (the [security and intelligence agencies]) alone;

(d) the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of [bulk communications data] by the [security and intelligence agencies] are consistent with the requirements of the ECHR; and

(e) the national court has found that the imposition of the requirements specified in [paragraphs 119 to 125 of the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970)], if applicable, would frustrate the measures taken to safeguard national security by the [security and intelligence agencies], and thereby put the national security of the United Kingdom at risk;

(1) Having regard to Article 4 TEU and Article 1(3) of [Directive 2002/58], does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the [security and intelligence agencies] of a Member State fall within the scope of Union law and of [Directive 2002/58]?

(2) If the answer to Question (1) is "yes", do any of the [requirements applicable to retained communications data, set out in paragraphs 119 to 125 of the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970)] or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the [security and intelligence agencies] to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?'

Consideration of the questions referred

Question 1

30 By its first question, the referring court asks, in essence, whether Article 1(3) of Directive 2002/58, read in the light of Article 4(2) TEU, is to be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.

31 In that regard, Privacy International argues, in essence, that, having regard to the guidance derived from the case-law of the Court of Justice as regards the scope of Directive 2002/58, both the acquisition of data by the security and intelligence agencies from those providers under section 94 of the 1984 Act and the use of that data by those agencies fall within the scope of that directive, whether that data is acquired by means of a transmission carried out in real-time or subsequently. In

particular, it argues that the fact that the objective of protecting national security is explicitly listed in Article 15(1) of that directive does not mean that the directive does not apply to such situations, and that assessment is not affected by Article 4(2) TEU.

32 By contrast, the United Kingdom, Czech and Estonian Governments, Ireland, and the French, Cypriot, Hungarian, Polish and Swedish Governments contend, in essence, that Directive 2002/58 does not apply to the national legislation at issue in the main proceedings, as the purpose of that legislation is to safeguard national security. They argue that the activities of the security and intelligence agencies are essential State functions relating to the maintenance of law and order and the safeguarding of national security and territorial integrity, and, accordingly, are the sole responsibility of the Member States, as attested to by, in particular, the third sentence of Article 4(2) TEU.

33 According to those governments, Directive 2002/58 cannot therefore be interpreted as meaning that national measures concerning the safeguarding of national security fall within its scope. Article 1(3) of that directive defines the scope of that directive and excludes from that scope, as was previously provided in the first indent of Article 3(2) of Directive 95/46, activities concerning public security, defence, and State security. Those provisions reflect the allocation of competences laid down in Article 4(2) TEU and would be deprived of any practical effect if it were necessary for measures in the field of national security to meet the requirements of Directive 2002/58. Furthermore, the case-law of the Court derived from the judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346), concerning the first indent of Article 3(2) of Directive 95/46 can be transposed to Article 1(3) of Directive 2002/58.

34 In that regard, it should be stated that, under Article 1(1) thereof, Directive 2002/58 provides, inter alia, 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 communications sector.

35 Article 1(3) of that directive excludes from its scope ‘activities of the State’ in specified fields, including activities 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. The activities thus mentioned by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 32 and the case-law cited).

36 In addition, 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 (judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788*,* paragraph 33 and the case-law cited).

37 In that context, 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]’ (judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 71).

38 Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, such measures regulate, for the purposes mentioned in that provision, the activity of providers of electronic communications services (judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16,

EU:C:2018:788, paragraph 34 and the case-law cited).

39 It is in the light of, inter alia, those considerations that the Court has held that Article 15(1) of Directive 2002/58, read in conjunction with Article 3 thereof, must be interpreted as meaning that the scope of that directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic data and location data, but also to a legislative measure requiring them to grant the competent national authorities access to that data. Such legislative measures necessarily involve the processing, by those providers, of the data and cannot, to the extent that they regulate the activities of those providers, be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58 (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 35 and 37 and the case-law cited).

40 Concerning a legislative measure such as section 94 of the 1984 Act, on the basis of which the competent authority may give the providers of electronic communications services a direction to disclose bulk data to the security and intelligence agencies by transmission, it should be noted that, pursuant to the definition provided in Article 4(2) of Regulation 2016/679, which, according to Article 2 of Directive 2002/58, read in conjunction with Article 94(2) of that regulation, is applicable, the concept of 'the processing of personal data' designates 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, … storage, … consultation, use, disclosure by transmission, dissemination or otherwise making available …'.

41 It follows that the disclosure of personal data by transmission, like the storage or otherwise making available of data, constitutes processing for the purposes of Article 3 of Directive 2002/58 and, accordingly, falls within the scope of that directive (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 45).

42 In addition, having regard to the considerations set out in paragraph 38 above and the general scheme of Directive 2002/58, an interpretation of that directive under which the legislative measures referred to in Article 15(1) thereof were excluded from the scope of that directive because the objectives which such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that same directive would deprive Article 15(1) thereof of any practical effect (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 72 and 73).

43 The concept of 'activities' referred to in Article 1(3) of Directive 2002/58 cannot therefore, as was noted, in essence, by the Advocate General in point 75 of his Opinion in Joined Cases *La Quadrature du Net and Others* (C-511/18 and C-512/18, EU:C:2020:6), to which he makes reference in point 24 of his Opinion in the present case, be interpreted as covering the legislative measures referred to in Article 15(1) of that directive.

44 Article 4(2) TEU, to which the governments listed in paragraph 32 above have made reference, cannot invalidate that conclusion. Indeed, according to the settled case-law of the Court, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law (see, to that effect, judgments of 4 June 2013, *ZZ*, C-300/11, EU:C:2013:363, paragraph 38 and the case-law cited; of 20 March 2018, *Commission* v *Austria (State printing office)*, C-187/16, EU:C:2018:194, paragraphs 75 and 76; and of 2 April 2020, *Commission* v *Poland, Hungary and Czech Republic (Temporary mechanism for the relocation of applicants for international protection)*, C-715/17, C-718/17 and C-719/17, EU:C:2020:257, paragraphs 143 and 170).

45 It is true that, in the judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04

and C-318/04, EU:C:2006:346, paragraphs 56 to 59), the Court held that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes did not, pursuant to the first indent of Article 3(2) of Directive 95/46, fall within the scope of that directive, because such a transfer fell within a framework established by the public authorities relating to public security.

46 However, having regard to the findings set out in paragraphs 36, 38 and 39 above, that case-law cannot be transposed to the interpretation of Article 1(3) of Directive 2002/58. Indeed, as the Advocate General noted, in essence, in points 70 to 72 of his Opinion in Joined Cases *La Quadrature du Net and Others* (C-511/18 and C-512/18, EU:C:2020:6), the first indent of Article 3(2) of Directive 95/46, to which that case-law relates, excluded, in a general way, from the scope of that directive 'processing operations concerning public security, defence, [and] State security', without drawing any distinction according to who was carrying out the data processing operation concerned. By contrast, in the context of interpreting Article 1(3) of Directive 2002/58, it is necessary to draw such a distinction. As is apparent from paragraphs 37 to 39 and 42 above, all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive, including processing operations resulting from obligations imposed on those providers by the public authorities, whereas those processing operations could, where appropriate, on the contrary, fall within the scope of the exception laid down in the first indent of Article 3(2) of Directive 95/46, given the broader wording of that provision, which covers all processing operations concerning public security, defence, or State security, regardless of the person carrying out those operations.

47 Furthermore, it should be noted that Directive 95/46, which was at issue in the case that gave rise to the judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346), has been, pursuant to Article 94(1) of Regulation 2016/679, repealed and replaced by that regulation with effect from 25 May 2018. Although that regulation states, in Article 2(2)(d) thereof, that it does not apply to processing operations carried out 'by competent authorities' for the purposes of, inter alia, the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security, it is apparent from Article 23(1)(d) and (h) of that regulation that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation. It follows that the above interpretation of Article 1(3), Article 3 and Article 15(1) of Directive 2002/58 is consistent with the definition of the scope of Regulation 2016/679, which is supplemented and specified by that directive.

48 By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by Directive 2002/58, but by national law only, subject to the application of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89), with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.

49 Having regard to the foregoing considerations, the answer to the first question is that Article 1(3), Article 3 and Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.

Question 2

50 By its second question, the referring court seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, is to be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.

51 As a preliminary point, it should be borne in mind that, according to the information set out in the request for a preliminary ruling, section 94 of the 1984 Act permits the Secretary of State to require providers of electronic communications services, by way of directions, if he considers it necessary in the interests of national security or relations with a foreign government, to forward bulk communications data to the security and intelligence agencies. That data includes traffic data and location data, as well as information relating to the services used, pursuant to section 21(4) and (6) of the RIPA. That provision covers, inter alia, the data necessary to (i) identify the source and destination of a communication, (ii) determine the date, time, length and type of communication, (iii) identify the hardware used, and (iv) locate the terminal equipment and the communications. That data includes, inter alia, the name and address of the user, the telephone number of the person making the call and the number called by that person, the IP addresses of the source and addressee of the communication and the addresses of the websites visited.

52 Such a disclosure of data by transmission concerns all users of means of electronic communication, without its being specified whether that transmission must take place in real-time or subsequently. Once transmitted, that data is, according to the information set out in the request for a preliminary ruling, retained by the security and intelligence agencies and remains available to those agencies for the purposes of their activities, as with the other databases maintained by those agencies. In particular, the data thus acquired, which is subject to bulk automated processing and analysis, may be cross-checked with other databases containing different categories of bulk personal data or be disclosed outside those agencies and to third countries. Lastly, those operations do not require prior authorisation from a court or independent administrative authority and do not involve notifying the persons concerned in any way.

53 As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of Directive 2002/58 is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, that directive seeks, as is stated in recital 2 thereof, to ensure that the rights set out in Articles 7 and 8 of the Charter are fully respected. In that regard, it is apparent 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 gave rise 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’.

54 To that end, Article 5(1) of Directive 2002/58 provides that ‘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’. That provision also emphasises that, ‘in particular, [Member States] 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)’, and specifies that ‘this paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’

55 Thus, Article 5(1) of that directive enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires, inter alia, that, in principle, persons other

than users be prohibited from storing, without those users' consent, those communications and that data. Having regard to the general nature of its wording, that provision necessarily covers any operation enabling third parties to become aware of communications and data relating thereto for purposes other than the conveyance of a communication.

56 The prohibition on the interception of communications and data relating thereto laid down in Article 5(1) of Directive 2002/58 therefore encompasses any instance of providers of electronic communications services making traffic data and location data available to public authorities, such as the security and intelligence agencies, as well as the retention of that data by those authorities, regardless of how that data is subsequently used.

57 Thus, in adopting that directive, the EU legislature gave concrete expression to the rights enshrined in Articles 7 and 8 of the Charter, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraph 109).

58 However, Article 15(1) of Directive 2002/58 enables the Member States to introduce an exception 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, inter alia, in Articles 6 and 9 of that directive, where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds.

59 That being said, the option to derogate from the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58 cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, explicitly laid down in Article 5 of that directive, to become the rule (see judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 89 and 104, and judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraph 111).

60 In addition, it is apparent from the third sentence of Article 15(1) of Directive 2002/58 that the Member States are not permitted to adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5, 6 and 9 of that directive unless they do so in accordance with the general principles of EU law, including the principle of proportionality, and with the fundamental rights guaranteed in the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making it available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 25 and 70, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 91 and 92 and the case-law cited).

61 Those same issues also arise for other types of data processing, such as the transmission of that data to persons other than users or access to that data with a view to its use (see, by analogy, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraphs 122 and 123 and the case-law cited).

62 Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of 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 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that 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 6 March 2001, *Connolly* v *Commission*, C-274/99 P, EU:C:2001:127, paragraph 39, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 93 and the case-law cited).

63 However, the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited).

64 Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

65 It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).

66 Concerning observance of the principle of proportionality, the first sentence of Article 15(1) of Directive 2002/58 provides that the Member States may adopt a measure derogating from the principle that communications and the related traffic data are to be confidential where such a measure is ‘necessary, appropriate and proportionate … within a democratic society’, in view of the objectives set out in that provision. Recital 11 of that directive specifies that a measure of that nature must be ‘strictly’ proportionate to the intended purpose.

67 In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (see, to that effect, 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, paragraphs 76, 77 and 86; and of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52; Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 140).

68 In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, in particular where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12,

EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 117; Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 141).

69 As regards the question whether national legislation, such as that at issue in the main proceedings, meets the requirements of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, it should be noted that the transmission of traffic data and location data to persons other than users, such as security and intelligence agencies, derogates from the principle of confidentiality. Where that operation is carried out, as in the present case, in a general and indiscriminate way, it has the effect of making the exception to the obligation of principle to ensure the confidentiality of data the rule, whereas the system established by Directive 2002/58 requires that that exception remain an exception.

70 In addition, in accordance with the settled case-law of the Court, the transmission of traffic data and location data to a third party constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, regardless of how that data is subsequently used. In that regard, it does not matter whether the information in question relating to persons' private lives is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited, and judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraphs 115 and 116).

71 The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (see, by analogy, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 27 and 37, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 99 and 100).

72 It should also be noted that the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter. Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistle-blowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ 2019 L 305, p. 17). Moreover, that deterrent effect is all the more serious given the quantity and breadth of the data retained (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 28; of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 101; and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraph 118).

73 Lastly, given the significant amount of traffic data and location data that can be retained continuously by a general retention measure and the sensitive nature of the information which that data may provide, the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access.

74 As regards the objectives that may justify such interferences, and in particular the objective of safeguarding national security, at issue in the main proceedings, it should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member

State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraph 135).

75 The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in paragraph 74 above can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraph 136).

76 However, in order to satisfy the requirement of proportionality referred to in paragraph 67 above, according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, national legislation entailing interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter must meet the requirements stemming from the case-law cited in paragraphs 65, 67 and 68 above.

77 In particular, as regards an authority's access to personal data, legislation cannot confine itself to requiring that authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 192 and the case-law cited).

78 Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary, national legislation governing access to traffic data and location data must rely 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 at issue (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119 and the case-law cited).

79 Those requirements apply, a fortiori, to a legislative measure, such as that at issue in the main proceedings, on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission. Such transmission has the effect of making that data available to the public authorities (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 212).

80 Given that the transmission of traffic data and location data is carried out in a general and indiscriminate way, it is comprehensive in that it affects all persons using electronic communications services. It therefore applies even to persons for whom there is no evidence to suggest that their conduct might have a link, even an indirect or remote one, with the objective of safeguarding national security and, in particular, without any relationship being established between the data which is to be transmitted and a threat to national security (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 and 58, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 105). Having regard to the fact that the transmission of such data to public authorities is equivalent, in accordance with the finding in paragraph 79 above, to access, it must be held that

legislation which permits the general and indiscriminate transmission of data to public authorities entails general access.

81 It follows that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission 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 Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter.

82 In the light of all the foregoing considerations, the answer to the second question is that Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.

Costs

83 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. 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 1(3), Article 3 and Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (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 Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.**

2. **Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Article 4(2) TEU and 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 enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.**

Lenaerts Silva de Lapuerta Bonichot

Arabadjiev Prechal Safjan

Xuereb Rossi Malenovský

Bay Larsen	von Danwitz	Toader
Jürimäe	Lycourgos	Piçarra

Delivered in open court in Luxembourg on 6 October 2020.

A. Calot Escobar	K. Lenaerts
Registrar	President

* Language of the case: English.