JUDGMENT OF THE COURT (Grand Chamber)

20 September 2022 (*)

[Text rectified by order of 27 October 2022]

(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Confidentiality of communications – Providers of electronic communications services – General and indiscriminate retention of traffic and location data – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 6, 7, 8 and 11 and Article 52(1) – Article 4(2) TEU)

In Joined Cases C-793/19 and C-794/19,

REQUESTS for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Germany), made by decisions of 25 September 2019, received at the Court on 29 October 2019, in the proceedings

Bundesrepublik Deutschland, represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

v

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and I. Ziemele, Presidents of Chambers, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (Rapporteur), N. Piçarra, L.S. Rossi and A. Kumin, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: D. Dittert, Head of Unit,

having regard to the written procedure and further to the hearing on 13 September 2021,

after considering the observations submitted on behalf of:

– the Bundesrepublik Deutschland, represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, by C. Mögelin, acting as Agent,

– [As rectified by order of 27 October 2022] SpaceNet AG, by M. Bäcker, Universitätsprofessor,

– Telekom Deutschland GmbH, by T. Mayen, Rechtsanwalt,

– the German Government, by J. Möller, F. Halibi, M. Hellmann, D. Klebs and E. Lankenau, acting as Agents,

– the Danish Government, by M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen and M. Søndahl Wolff, acting as Agents,

– the Estonian Government, by A. Kalbus and M. Kriisa, acting as Agents,

– Ireland, by A. Joyce and J. Quaney, acting as Agents, and by D. Fennelly, Barrister-at-Law, and P. Gallagher, Senior Counsel,

– the Spanish Government, by L. Aguilera Ruiz, acting as Agent,

– the French Government, by A. Daniel, D. Dubois, J. Illouz, E. de Moustier and T. Stéhelin, acting as Agents,

– the Cypriot Government, by I. Neophytou, acting as Agent,

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

– the Polish Government, by B. Majczyna, D. Lutostańska and J. Sawicka, acting as Agents,

– the Finnish Government, by A. Laine and M. Pere, acting as Agents,

– the Swedish Government, by H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson and H. Shev, acting as Agents,

– the European Commission, by G. Braun, S.L. Kalėda, H. Kranenborg, M. Wasmeier and F. Wilman, acting as Agents,

– the European Data Protection Supervisor, by A. Buchta, D. Nardi, N. Stolič and K. Ujazdowski, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 18 November 2021,

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 6 to 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’) and Article 4(2) TEU.

2 The requests have been made in proceedings between the Bundesrepublik Deutschland (Federal Republic of Germany), represented by the Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Agency for Electricity, Gas, Telecommunications, Post and Rail Networks, Germany), on the one hand, and SpaceNet AG (Case C-793/19) and Telekom Deutschland GmbH (Case C-794/19), on the other, concerning the obligation imposed on those companies to retain traffic and location data relating to their customers’ telecommunications.

Legal context

European Union law

Directive 95/46/EC

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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

4 Article 3(2) of Directive 95/46 provided:

‘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 of the Treaty on European Union 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

5 Recitals 2, 6, 7 and 11 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 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 [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 … Convention for the Protection of Human Rights and Fundamental Freedoms.’

6 Article 1 of that directive, 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 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 TFEU], such as those covered by Titles V and VI of the [TEU], and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

7 Under 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;

…'

8 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.'

9 Article 5 of the directive, 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.'

10 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.

…'

11 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. …'

12 Article 15 of Directive 2002/58, entitled 'Application of certain provisions of Directive [95/46]', provides, 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 Community law, including those referred to in Article 6(1) and (2) [TEU].'

German law

The TKG

13 Paragraph 113a(1), first sentence, of the Telekommunikationsgesetz (Law on Telecommunications) of 22 June 2004 (BGB1. 2004 I, p. 1190), in the version applicable to the dispute in the main proceedings ('the TKG'), is worded as follows:

'The obligations in respect of the retention, use and security of the traffic data defined in Paragraphs 113b to 113g apply to operators which provide publicly available telecommunications services to end users.'

14 Under Paragraph 113b of the TKG:

'(1) Operators to which Paragraph 113a(1) applies shall retain data in national territory as follows:

1. for 10 weeks in the case of the data referred to in subparagraphs 2 and 3;

2. for four weeks in the case of the location data referred to in subparagraph 4.

(2) Providers of publicly available telecommunications services shall retain:

1. the telephone number or other identifier of the calling and called parties as well as, in the case of call switching or forwarding, of every other line involved,

2. the date and time of the start and end of the communication, stating the time zone,

3. where different services can be used in the context of the telephone service, information on the service used;

4. and also, in the case of mobile telephony services,

   (a) the International Mobile Subscriber Identity of the calling and called parties,

   (b) the international identifier of the calling and called terminals,

   (c) in the case of pre-paid services, the date and time of the initial activation of the service, stating the time zone;

5. and, in the case of internet telephony services, the IP (internet protocol) addresses of the calling and called parties and the allocated identification numbers.

Subparagraph 1 above shall apply *mutatis mutandis*.

1. to SMS, multimedia messaging or similar services; in such cases, the information referred to in item 2 of subparagraph 1 shall be replaced by the time of despatch and receipt of the message;

2. to unanswered calls or calls that are unsuccessful due to intervention on the part of the network manager …

(3) Providers of publicly available internet access services shall retain:

1. the IP address allocated to the subscriber for the purposes of using the internet;

2. the clear identifier of the connection that provides access to the internet and the allocated network identification number;

3. the date and time of the start and end of internet use from the allocated IP address, stating the time zone.

(4) Where mobile telephony services are used, the designation of the cell sites used at the start of the communication by the caller and the recipient must be retained. In the case of mobile usage of publicly

available internet access services, the designation of the cell sites used at the start of the internet connection must be retained. Any data that enable identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question should also be retained.

(5) The content of the communication, data on internet sites visited and data from email services may not be retained pursuant to this provision.

(6) Data underlying the communications referred to in Paragraph 99(2) may not be retained pursuant to this provision. This applies, *mutatis mutandis*, to telephone communications originating from the entities referred to in Paragraph 99(2). The second to seventh sentences of Paragraph 99(2) apply *mutatis mutandis*.

…'

15 The communications mentioned in Paragraph 99(2) of the TKG, to which Paragraph 113b(6) of the TKG refers, are communications with persons, authorities and organisations of a social or religious nature which offer solely or essentially telephone assistance in psychological or social emergencies to callers who in principle remain anonymous and which are, along with their staff, subject to specific confidentiality obligations in that respect. The exemption laid down in the second and fourth sentences of Paragraph 99(2) of the TKG is conditional on the inclusion, upon request, of those call lines on a register drawn up by the Federal Agency for Electricity, Gas, Telecommunications, Post and Rail Networks, after the operators of those call lines have established the nature of the services provided by producing a certificate issued by an authority, entity, body or foundation governed by public law.

16 Under Paragraph 113c(1) and (2) of the TKG:

'(1) Data retained pursuant to Paragraph 113b may be:

1. disclosed to a law enforcement authority, where the authority so requests under a statutory provision which authorises it to collect the data referred to in Paragraph 113b for the purposes of prosecuting particularly serious criminal offences;

2. disclosed to a security authority of the *Länder*, where the authority so requests under a statutory provision which authorises it to collect the data referred to in Paragraph 113b for the purposes of preventing a specific risk to a person's physical integrity, life or freedom or to the continued existence of the Federal State or a *Land*;

…

(2) Data retained pursuant to Paragraph 113b may not be used by persons who are subject to the obligations established in Paragraph 113a(1) for purposes other than those provided for in subparagraph 1.'

17 Article 113d of the TKG states:

'A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that the data retained pursuant to the retention obligation in Paragraph 113b(1) are protected by state-of-the-art technical and organisational measures against unauthorised access and use. These measures shall include, in particular:

1. use of a particularly secure encryption method;

2. storage in separate storage facilities that are separate from those designated for normal operational tasks;

3. storage that provides a high level of protection against cyber-attacks, in isolated data processing computer systems;

4. measures to ensure that access to the data processing facilities is restricted to persons who have been specially authorised by the party subject to the obligation; and

5. a requirement for at least two persons who have been specially authorised by the party subject to the obligation to be involved when the data are accessed.'

18 Paragraph 113e of the TKG reads as follows:

'(1) A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that all access, in particular the reading, copying, alteration, deletion and blocking of data retained pursuant to the retention obligation under Paragraph 113b(1), is logged for data protection control purposes. The following data must be logged:

1. the time of access;

2. the persons accessing the data;

3. the purpose and nature of the access.

(2) The log data may not be used for purposes other than data protection control.

(3) A party that is subject to an obligation pursuant to Paragraph 113a(1) must ensure that the log data are deleted after one year.'

19 In order to ensure a particularly high level of security and quality of data, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways establishes, in accordance with Paragraph 113f(1) of the TKG, a set of requirements which, pursuant to Paragraph 113f(2) thereof, must be continuously assessed and adapted where appropriate. Paragraph 113g of the TKG requires that specific security measures be integrated into the security policy statement which must be presented by the party subject to the obligation.

The StPO

20 The first sentence of Paragraph 100g(2) of the Strafprozessordnung (Code of Criminal Procedure; 'the StPO') is worded as follows:

'Where there is prima facie evidence that someone has been the perpetrator of or an accessory to one of the particularly serious criminal offences referred to in the second sentence or, in those cases where an attempted offence is punishable, that someone has attempted to commit the offence in question and it is a particularly serious instance of the offence, the traffic data retained pursuant to Paragraph 113b of the [TKG] may be collected if the investigation of the facts or the determination of the whereabouts of the person under investigation would otherwise be significantly impeded or impracticable and the collection of the data is proportionate to the importance of the matter.'

21 Paragraph 101a(1) of the StPO establishes that judicial authorisation is required for the collection of traffic data pursuant to Paragraph 100g thereof. Under Paragraph 101a(2) of the StPO, the grounds of the judicial decision must include essential considerations relating to the necessity and appropriateness of the measure in the particular case in question. Paragraph 101a(6) of the StPO lays down an obligation to inform the participants in the telecommunications concerned.

The disputes in the main proceedings and the question referred for a preliminary ruling

22 SpaceNet and Telekom Deutschland provide publicly available internet access services in Germany. The latter also provides publicly available telephone services in Germany.

23 Those service providers brought proceedings before the Verwaltungsgericht Köln (Administrative Court, Cologne, Germany), challenging the obligation imposed on them by the combined provisions of Paragraph 113a(1) and Paragraph 113b of the TKG to retain traffic and location data relating to their customers' telecommunications as from 1 July 2017.

24 By judgments of 20 April 2018, the Verwaltungsgericht Köln (Administrative Court, Cologne) held that SpaceNet and Telekom Deutschland were not required to retain the traffic data relating to the telecommunications, referred to in Paragraph 113b(3) of the TKG, of the customers to whom they provide internet access and that Telekom Deutschland was also not required to retain the traffic data relating to the telecommunications, referred to in the first and second sentences of Paragraph 113b(2) of the TKG, of customers to whom it provides publicly available telephone services. That court considered, in the light of the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), that that retention obligation was contrary to EU law.

25 The Federal Republic of Germany brought appeals on a point of law against those judgments before the Bundesverwaltungsgericht (Federal Administrative Court, Germany), the referring court.

26 The referring court considers that the question whether the retention obligation imposed by the combined provisions of Paragraph 113a(1) and Paragraph 113b of the TKG is contrary to EU law depends on the interpretation of Directive 2002/58.

27 In that respect, the referring court states that the Court has already established definitively, in the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), that rules governing the retention of traffic and location data and access to those data by national authorities fall, in principle, within the scope of Directive 2002/58.

28 It also states that the retention obligation at issue in the main proceedings, since it limits the rights deriving from Article 5(1), Article 6(1) and Article 9(1) of Directive 2002/58, could be justified only on the basis of Article 15(1) of that directive.

29 In that respect, it notes that it follows from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), 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.

30 According to the referring court, like the national legislation at issue in the cases which gave rise to that judgment, the national legislation at issue in the main proceedings does not require any reason for the retention of the data or any link between the data retained and a criminal offence or a risk to public security. That national legislation requires the general retention, without a reason, and without any distinction in terms of personal, temporal or geographical factors, of the majority of the traffic data relating to telecommunications.

31 The referring court considers, however, that it cannot be ruled out that the retention obligation at issue in the main proceedings may be justified under Article 15(1) of Directive 2002/58.

32 In the first place, it notes that, contrary to the national legislation at issue in the cases that gave rise to the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), the national legislation at issue in the main proceedings does not require the retention of all telecommunications traffic data of all subscribers and users in relation to all means of electronic communications. Not only is the content of communications excluded from the retention obligation, but data relating to websites visited, the data from electronic mail services and the data underlying social or religious communications to or from certain lines cannot be retained, as is apparent from Paragraph 113b(5) and (6) of the TKG.

33 In the second place, that court indicates that Paragraph 113b(1) of the TKG provides for a retention period of 4 weeks for location data and 10 weeks for traffic data, whereas 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 (OJ 2006 L 105, p. 54), on which the national legislation at issue in the cases that gave rise to the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), were based, provided for a retention period of between six months and two years.

34 According to the referring court, although the exclusion of certain means of communication or certain categories of data and the limitation of the retention period are not sufficient to eliminate all risk of establishing a comprehensive profile of the persons concerned, that risk would be at least considerably reduced in the context of the implementation of the national legislation at issue in the main proceedings.

35 In the third place, that legislation contains strict limitations as regards the protection of retained data and access thereto. Thus, first, it ensures the effective protection of retained data against the risks of abuse and against any unlawful access to those data. Secondly, the data retained can be used only for the purposes of fighting serious crime or for the prevention of a specific risk to a person's physical integrity, life or freedom or to the continued existence of the Federal Republic or a *Land*.

36 In the fourth place, the interpretation of Article 15(1) of Directive 2002/58 to the effect that any data retention without a reason is generally incompatible with EU law could conflict with the Member States' obligation to act, arising from the right to security enshrined in Article 6 of the Charter.

37 In the fifth place, the referring court considers that an interpretation of Article 15 of Directive 2002/58 as precluding the general retention of data would considerably restrict the discretion of the national legislature in an area concerning the prosecution of crimes and public security, which, in accordance with Article 4(2) TEU, remains the sole responsibility of each Member State.

38 In the sixth place, the referring court considers that it is necessary to take into account the case-law of the European Court of Human Rights and notes that that court has held that Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms ('the ECHR') does not preclude national provisions providing for the bulk interception of cross-border flows of data, in view of the threats currently facing many States and the technological tools which terrorists and criminals may now use in order to commit wrongdoings.

39 In those circumstances, the Bundesverwaltungsgericht (Federal Administrative Court) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

'In the light of Articles 7, 8 and 11 and Article 52(1) of the [Charter], on the one hand, and of Article 6 of the [Charter] and Article 4 [TEU], on the other hand, is Article 15 of Directive [2002/58] to be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services where:

(1) that obligation does not require a specific reason in terms of location, time or region,

(2) the following data are the subject of the retention obligation in the provision of publicly available telephone services – including the transmission of SMS, multimedia messages or similar messages and unanswered or unsuccessful calls:

(a) the telephone number or other identifier of the calling and called parties as well as, in the case of call switching or forwarding, of every other line involved,

(b) the date and time of the start and end of the call or – in the case of the transmission of a short message, multimedia message or similar message – the times of dispatch and receipt of the message, and an indication of the relevant time zone,

(c) information regarding the service used, if different services can be used in the context of the telephone service,

(d) and also, in the case of mobile telephone services

(i) the International Mobile Subscriber Identity of the calling and called parties,

(ii) the international identifier of the calling and called terminal equipment,

(iii) in the case of pre-paid services, the date and time of the initial activation of the service, and an indication of the relevant time zone,

(iv) the designations of the cells that were used by the calling and called parties at the beginning of the call,

(e) in the case of internet telephone services, the Internet Protocol addresses of the calling and the called parties and allocated user IDs,

(3) the following data are the subject of the retention obligation in the provision of publicly available internet access services:

(a) the Internet Protocol address allocated to the subscriber for internet use,

(b) a unique identifier of the connection via which the internet use takes place, as well as an allocated user ID,

(c) the date and time of the start and end of the internet use at the allocated Internet Protocol address, and an indication of the relevant time zone,

(d) in the case of mobile use, the designation of the cell used at the start of the internet connection,

(4) the following data must not be retained:

(a) the content of the communication,

(b) data regarding the internet pages accessed,

(c) data from electronic mail services,

(d) data underlying links to or from specific connections of persons, authorities and organisations in social or ecclesiastical spheres,

(5) the retention period is 4 weeks for location data, that is to say, the designation of the cell used, and 10 weeks for the other data,

(6) effective protection of retained data against risks of abuse and against any unlawful access to those data is ensured, and

(7) the retained data may be used only to prosecute particularly serious criminal offences and to prevent a specific threat to a person's physical integrity, life or freedom or to the continued existence of the Federal Republic or of a *Land*, with the exception of the Internet Protocol address allocated to a subscriber for internet use, the use of which data is permissible in the context of the provision of inventory data information for the prosecution of any criminal offence, maintaining public order and security and carrying out the tasks of the intelligence services?'

Procedure before the Court

40 By decision of the President of the Court of 3 December 2019, Cases C-793/19 and C-794/19 were joined for the purposes of the written and oral parts of the procedure and the judgment.

41 By decision of the President of the Court of 14 July 2020, the proceedings in Joined Cases C-793/19 and C-794/19 were stayed pursuant to Article 55(1)(b) of the Rules of Procedure of the Court of Justice, pending delivery of the judgment in *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18).

42 On 6 October 2020, the Court delivered its judgment in *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and, on 8 October 2020, the President of the Court ordered

the resumption of the proceedings in Joined Cases C-793/19 and C-794/19.

43 The referring court, to which the Registry communicated that judgment, stated that it was maintaining its request for a preliminary ruling.

44 In that respect, the referring court first of all noted that the retention obligation provided for by the legislation at issue in the main proceedings concerns a smaller amount of data and a shorter retention period than that provided for by the national legislation at issue in the cases that gave rise to the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791*)*. Those particular features reduce the possibility that the data retained could allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained.

45 Next, it reiterated that the national legislation at issue in the main proceedings ensures the effective protection of retained data against the risks of abuse and unlawful access.

46 Lastly, it indicated that uncertainties remain as regards the question of the compatibility with EU law of the retention of IP addresses, provided for by the national legislation at issue in the main proceedings, due to an inconsistency between paragraphs 155 and 168 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791*)*. Thus, according to the referring court, uncertainty arises from that judgment as to whether the Court requires, for the retention of IP addresses, a ground for retention linked to the objective of safeguarding national security, combating serious crime or preventing serious threats to public security, as seems to follow from paragraph 168 of that judgment, or whether the retention of IP addresses is permitted even in the absence of a specific ground, since only the use of the retained data is limited by those objectives, as paragraph 155 of that judgment suggests.

Consideration of the question referred

47 By its question, the referring court seeks, in essence, to ascertain whether Article 15(1) of Directive 2002/58, read in the light of Articles 6 to 8 and 11 and Article 52(l) of the Charter and Article 4(2) TEU, must be interpreted as meaning that it precludes a national legislative measure which, with certain exceptions, requires providers of publicly available electronic communications services – for the purposes set out in Article 15(1) of that directive, and inter alia for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security – to retain, in a general and indiscriminate way, most of the traffic and location data of the end users of those services, laying down a retention period of several weeks and rules intended to ensure the effective protection of the retained data against the risks of abuse and against any unlawful access to those data.

Applicability of Directive 2002/58

48 As regards the argument of Ireland and the French, Netherlands, Polish and Swedish Governments that the national legislation at issue in the main proceedings does not fall within the scope of Directive 2002/58, since it was adopted, inter alia, in order to safeguard national security, it is sufficient to note that national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes, inter alia, of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58 (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 104).

Interpretation of Article 15(1) of Directive 2002/58

The principles drawn from the Court's case-law

49 It is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 32 and the case-law cited).

50 It is clear from the wording itself of Article 15(1) of Directive 2002/58 that the legislative measures that it authorises Member States to take, under the conditions that it lays down, may seek only 'to restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of Directive 2002/58 (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 33).

51 As regards the system established by that directive of which Article 15(1) forms part, it must be recalled that, pursuant to the first and second sentences of Article 5(1) of that directive, Member States are required to ensure, through their national legislation, the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as of the related traffic data. In particular, they are required to 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) of the same directive (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 34).

52 In that regard, the Court has already held that Article 5(1) of Directive 2002/58 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 data (judgments of 6 October 2020, *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, EU:C:2020:791*, paragraph 107,* and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 35).

53 That provision reflects the objective pursued by the EU legislature when adopting Directive 2002/58. 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'. As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of that directive 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, as stated in recital 2 of the directive, the EU legislature's intent is to ensure full respect for the rights set out in Articles 7 and 8 of the Charter, relating, respectively, to respect for private and family life and the protection of personal data (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 36 and the case-law cited).

54 In adopting Directive 2002/58, the EU legislature gave concrete expression to those rights, 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 (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 109, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 37).

55 As regards the processing and storage by electronic communications service providers of subscribers' and users' traffic data, Article 6 of Directive 2002/58 provides, in paragraph 1, that those data must be erased or made anonymous, when they are no longer needed for the purpose of the transmission of a communication, and states, in paragraph 2, that the traffic data necessary for the purposes of subscriber billing and interconnection fees may only be processed up to the end of the period during which the bill may lawfully be challenged or payment pursued. As regards location data other than traffic data, Article 9(1) of that directive provides that those data may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained.

56 Therefore, Directive 2002/58 does not merely create a framework for access to such data through safeguards to prevent abuse, but also enshrines, in particular, the principle of the prohibition of their

storage by third parties (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 39).

57 In so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that 'restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of that directive, such as those arising from the principles of confidentiality of communications and the prohibition on storing related data recalled in paragraph 52 above, that provision provides for an exception to the general rule provided for inter alia in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. That provision, therefore, 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 those data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 40 and the case-law cited).

58 As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 41 and the case-law cited).

59 Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States must comply with the general principles of EU law, which include the principle of proportionality, and ensure respect for the fundamental rights guaranteed by 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 them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, but also with Article 11 of the Charter, relating to the freedom of expression, which constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the European Union is founded (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraphs 42 and 43 and the case-law cited).

60 It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing those data, and, secondly, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private life is sensitive, whether the persons concerned have been inconvenienced in any way on account of that interference, or, furthermore, whether the data retained will or will not be used subsequently (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 44 and the case-law cited).

61 That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoy special protection under EU law. Taken as a whole, those data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, 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. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 45 and the case-law cited).

62 Therefore, first, the retention of traffic and location data for policing 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 electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter, effects that are all the more serious given the quantity and breadth of data retained. Secondly, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from those data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 46 and the case-law cited).

63 That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce the derogations referred to in paragraph 51 to 54 above, that provision reflects the fact that 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. 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 European Union or the need to protect the rights and freedoms of others. Thus, in order to interpret Article 15(1) of Directive 2002/58 in the light of the Charter, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 48 and the case-law cited).

64 Thus as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual's home and communications, and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 49 and the case-law cited).

65 In view of those different positive obligations, it is therefore necessary to strike a balance between the various interests and rights at issue and to establish a legal framework which enables such a balance to be struck (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 50 and the case-law cited).

66 In that context, it is clear from the wording itself of the first sentence of Article 15(1) of Directive 2002/58 that the Member States may adopt a measure derogating from the principle of confidentiality referred to in paragraph 52 above where such a measure is 'necessary, appropriate and proportionate within a democratic society', and recital 11 of the directive specifies, in that respect, 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 (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 52 and the case-law cited).

68 More specifically, it follows from the Court's case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that

limitation is proportionate to that seriousness (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).

69 In order to satisfy the requirement of proportionality, the national 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 are affected have sufficient guarantees that those 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 are subjected to automated processing, in particular where there is a significant risk of unlawful access to those data. Those considerations apply especially where the protection of the particular category of personal data that are sensitive data is at stake (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 54 and the case-law cited).

70 Thus, national legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 55 and the case-law cited).

71 As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court's case-law, in particular the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that, in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 56).

72 Thus, as regards safeguarding national security, the importance of which exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, the Court held that that provision, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 58 and the case-law cited).

73 As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited).

74 As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to privacy. Thus, and also taking into account, first, the dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the

Charter, referred to in paragraph 62 above, which is liable to result from the retention of those data, and, secondly, the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that those data should not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance that must be attached to them (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 65 and the case-law cited).

75 However, the Court specified 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, does not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for:

– the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;

– the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;

– the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and

– recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 67).

A measure providing for general and indiscriminate retention of the majority of traffic and location data for a period of several weeks

76 It is in the light of those governing considerations that the characteristics of the national legislation at issue in the main proceedings, highlighted by the referring court, must be examined.

77 In the first place, as regards the extent of the data retained, it is apparent from the order for reference that, in the context of the provision of telephone services, the retention obligation laid down by that legislation covers, inter alia, the data necessary to identify the source of a communication and its destination, the date and time of the start and end of the communication or – in the case of communication by SMS, multimedia message or similar message – the time of dispatch and receipt of the message and, in the case of mobile use, the designation of the cell sites used by the caller and the recipient at the start of the communication. In the context of the provision of internet access services, the retention obligation covers, inter alia, the IP address assigned to the subscriber, the date and time of the start and end of internet use from the assigned IP address and, in the case of mobile use, the designation of the cell sites used at the beginning of the internet connection. The data enabling the identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question are also retained.

78 Although the national legislation at issue in the main proceedings excludes the content of the communication and the data concerning the websites visited from the retention obligation and requires the retention of the cell site designation only at the beginning of the communication, that was also true, in essence, of the national legislation transposing Directive 2006/24 at issue in the cases that gave rise

to the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791). Despite those limitations, the Court held in that judgment that the categories of data retained under that directive and those national rules could allow very precise conclusions to be drawn concerning the private life of the persons concerned, such as the habits of everyday life, 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 and, in particular, provide the means of establishing a profile of those persons.

79 It must also be noted that, although the legislation at issue in the main proceedings does not cover the data concerning the websites visited, it nevertheless provides for the retention of IP addresses. Since IP addresses may be used, among other things, to track an internet user's complete clickstream and, therefore, his or her entire online activity, those data enable a detailed profile of the user to be established. Thus, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the internet user enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 153).

80 In addition, and as SpaceNet observed in its written observations, the data relating to electronic mail services, although not covered by the retention obligation laid down by the legislation at issue in the main proceedings, represent only a very small part of the data in question.

81 Thus, as the Advocate General observed, in essence, in point 60 of his Opinion, the retention obligation laid down by the national legislation at issue in the main proceedings applies to a very broad set of traffic and location data which corresponds, in essence, to those which led to the settled case-law referred to in paragraph 78 above.

82 In addition, in response to a question put to it at the hearing, the German Government stated that only 1 300 entities were listed on the register of persons, authorities or organisations of a social or religious nature whose electronic communications data are not retained under Paragraph 99(2) and Paragraph 113b(6) of the TKG, which clearly represents a small proportion of all users of telecommunications services in Germany whose data fall within the scope of the retention obligation laid down by the national legislation at issue in the main proceedings. The data of users who are subject to a duty of professional secrecy, such as lawyers, doctors and journalists, are thus retained.

83 It is therefore apparent from the order for reference that the retention of traffic and location data provided for by that national legislation concerns practically the entire population without those persons being, even indirectly, in a situation liable to give rise to criminal prosecutions. Similarly, that legislation requires the general retention, without a reason, and without any distinction in terms of personal, temporal or geographical factors, of most traffic and location data, the scope of which corresponds, in essence, to that of the data retained in the cases which led to the case-law referred to in paragraph 78 above.

84 Accordingly, in the light of the case-law cited in paragraph 75 above, a data retention obligation such as that at issue in the main proceedings cannot be regarded as a targeted retention of data, contrary to the submissions of the German Government.

85 In the second place, as regards the data retention period, it follows from the second sentence of Article 15(1) of Directive 2002/58 that the length of the retention period provided for by a national measure imposing a general and indiscriminate retention obligation is indeed a relevant factor, amongst others, in determining whether EU law precludes such a measure, since that sentence requires that that period be 'limited'.

86 In the present case, it is true that those periods – which amount, according to Paragraph 113b(1) of the TKG, to 4 weeks for location data and to 10 weeks for other data – are significantly shorter that those provided for by the national legislation imposing a general and indiscriminate retention obligation examined by the Court in its judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258).

87 However, as is apparent from the case-law cited in paragraph 61 above, the seriousness of the interference stems from the risk, particularly in view of their number and variety, that the data retained, taken as a whole, may enable very precise conclusions to be drawn concerning the private life of the person or persons whose data have been retained and, in particular, provide the means of establishing a profile of the person or persons concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

88 Accordingly, the retention of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious regardless of the length of the retention period and the quantity or nature of the data retained, when that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned (see, as regards access to such data, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 39).

89 Even the retention of a limited quantity of traffic or location data or the retention of those data for a short period are liable to provide very precise information on the private life of a user of a means of electronic communication. Furthermore, the quantity of the data available and the very specific information on the private life of the person concerned that results from the data can be assessed only after the data have been consulted. However, the interference resulting from the retention of those data necessarily occurs before the data and the information resulting therefrom can be consulted. Thus, the assessment of the seriousness of the interference that the retention constitutes is necessarily carried out on the basis of the risk generally pertaining to the category of data retained for the private lives of the persons concerned, without it indeed mattering whether or not the resulting information relating to the person's private life is in actual fact sensitive (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications),* C-746/18, EU:C:2021:152, paragraph 40).

90 In the present case, as is apparent from paragraph 77 above and as was confirmed at the hearing, a set of traffic and location data retained for 10 weeks and 4 weeks respectively may allow very precise conclusions to be drawn concerning the private lives of the persons whose data are retained, such as habits of everyday life, 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 and, in particular, enable a profile of those persons to be established.

91 In the third place, as regards the safeguards provided for by the national legislation at issue in the main proceedings, which are intended to protect the retained data against the risks of abuse and against any unlawful access, it must be emphasised that the retention of and access to those data each constitute, as is clear from the case-law recalled in paragraph 60 above, separate interferences with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, requiring a separate justification pursuant to Article 52(1) of the Charter. It follows that national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 47).

92 In the fourth and last place, as regards the European Commission's argument that particularly serious crime could be treated in the same way as a threat to national security, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through 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 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 61 and the case-law cited).

93 Unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 62 and the case-law cited).

94 Thus, crime, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. To treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 63).

The measures providing for targeted retention, expedited retention or retention of IP addresses

95 Several governments, including the French Government, submit that only general and indiscriminate retention enables the efficient achievement of the objectives pursued by the retention measures and the German Government has argued, in essence, that that conclusion is not undermined by the fact that the Member States may have recourse to the targeted retention and expedited retention measures referred to in paragraph 75 above.

96 In that regard, it must be observed, in the first place, that the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 69).

97 In the second place, 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 interpreted by the case-law recalled in paragraph 75 above, allows Member States to adopt, for the purposes of combating serious crime and preventing serious threats to public security, not only measures for targeted retention and expedited retention, but also measures providing for the general and indiscriminate retention, first, of data relating to the civil identity of users of electronic communications systems and, secondly, of IP addresses assigned to the source of a connection (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 70).

98 In that respect, it is common ground that retention of data relating to the civil identity of users of electronic communications systems may contribute to the fight against serious crime to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 71).

99 Directive 2002/58 does not preclude, for the purposes of combating crime in general, the generalised retention of data relating to civil identity. In those circumstances, it must be stated that neither the directive nor any other EU law act precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 72).

100 In addition, it should be recalled that the generalised retention of IP addresses of the source of connection constitutes a serious interference in the fundamental rights enshrined in Articles 7 and 8 of the Charter as those IP addresses may allow precise conclusions to be drawn concerning the private life of the user of the means of electronic communication concerned and may be a deterrent to the exercise of freedom of expression guaranteed in Article 11 of the Charter. However, as regards such retention, the Court has held that in order to strike the necessary balance between the rights and interests at issue as required by the case-law referred to in paragraphs 65 to 68 above, it is necessary to take into account,

in a case of an offence committed online and, in particular, in cases of the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1, and corrigendum OJ 2012 L 18, p. 7), the fact that the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 73).

101 In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the internet would catch persons who at first sight have no connection, within the meaning of the case-law cited in paragraph 70 above, with the objectives pursued, and it is also true, in accordance with what has been stated in paragraph 54 above, that internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of those data (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 155).

102 In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of those data, particularly via tracking, with regard to communications made and activities carried out online by the persons concerned (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 156).

103 Thus, contrary to the observations of the referring court, there is no tension between paragraphs 155 and 168 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791). As the Advocate General observed, in essence, in points 81 and 82 of his Opinion, it is clear from that paragraph 155, read in conjunction with paragraph 156 and paragraph 168 of that judgment, that only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying the general retention of IP addresses assigned to the source of a connection, irrespective of whether the persons concerned are liable to have at least an indirect link to the objectives pursued.

104 In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, some of the arguments put forward by the Member States against such measures show a narrower understanding of the scope of those measures than that set out in the case-law referred to in paragraph 75 above. While, as is recalled in paragraph 57 above, those retention measures are a derogation within the system established by Directive 2002/58, that directive, read in the light of the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter, does not make the possibility of issuing an order requiring a targeted retention subject to the condition either that the places likely to be the location of a serious crime or the persons suspected of being involved in such an act must be known in advance. Likewise, that directive does not require that the order requiring an expedited retention be limited to suspects identified in advance of that order (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 75).

105 As regards, first, targeted retention, the Court has held that Article 15(1) of Directive 2002/58 does not preclude national legislation based on objective evidence which makes it possible to target persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 76 and the case-law cited).

106 The Court stated, in that regard, that, while the objective evidence may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective and non-discriminatory factors, as posing a threat to public or national security in the Member State concerned (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 77).

107 Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of such an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of persons thus identified is justified (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 78).

108 Secondly, a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 79 and the case-law cited).

109 It should be borne in mind that, according to that case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern, depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is, in itself, entirely unconnected with any potentially discriminatory factors (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 80).

110 In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 81).

111 It should also be noted that the geographic areas covered by such a targeted retention measure may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime. The Court has held that the duration of those targeted retention measures described in paragraphs 105 to 110 above must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary (judgments of 6 October 2020, *La Quadrature du Net and*

Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 151, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 82).

112 As regards the possibility of providing distinctive criteria other than a personal or geographic criterion for the targeted retention of traffic and location data, it is possible that other objective and non-discriminatory criteria may be considered in order to ensure that the scope of a targeted retention measure is as limited as is strictly necessary and to establish a connection, at least indirectly, between serious criminal acts and the persons whose data are retained. However, since Article 15(1) of Directive 2002/58 refers to legislative measures of the Member States, it is for the latter and not for the Court to identify those criteria, it being understood that there can be no question of reinstating, by that means, the general and indiscriminate retention of traffic and location data (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 83).

113 In any event, as the Advocate General observed in point 50 of his Opinion, the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general and indiscriminate retention of traffic and location data (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 84).

114 As regards, secondly, the expedited retention of traffic and location data processed and stored by providers of electronic communications services on the basis of Articles 5, 6 and 9 of Directive 2002/58 or on the basis of legislative measures taken under Article 15(1) of that directive, it should be noted that those data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which those data must be processed and stored in accordance with the national provisions transposing that directive. Nevertheless, the Court has held that during that processing and storage, situations may arise in which it becomes necessary to retain those data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 85).

115 In such a situation, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraphs 65 to 68 above, it is permissible for Member States to provide, in legislation adopted pursuant to Article 15(1) of Directive 2002/58, for the possibility of instructing, by means of a decision of the competent authority subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 163, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 86).

116 To the extent that the purpose of that expedited retention no longer corresponds to the purpose for which those data were initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only actions to combat serious crime and, a fortiori, to safeguard national security are such as to justify such interference, on the condition that the measure and access to the retained data comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791) (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 87).

117 The Court has stated that a measure of retention of that nature need not be limited to the data of persons who have been identified previously as being a threat to public security or national security of the Member State concerned or of persons specifically suspected of having committed a serious criminal offence or acts adversely affecting national security. According to the Court, while it must

comply with the framework established 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, and taking into account the considerations set out in paragraph 70 above, such a measure may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle (judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 165, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 88).

118 Thus, a legislative measure may authorise the issuing of an instruction to providers of electronic communications services to carry out the expedited retention of traffic and location data, inter alia, of persons with whom, prior to the serious threat to public security arising or a serious crime being committed, a victim was in contact via those electronic means of communications (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 89).

119 Such expedited retention may, according to the Court's case-law recalled in paragraph 117 above and under the same conditions as those referred to in that paragraph, also be extended to specific geographic areas, such as the places of the commission of or preparation for the offence or attack on national security in question. It should be stated that the subject matter of such a measure may also be the traffic and location data relating to a place where a person, possibly the victim of a serious crime, has disappeared, on condition that that measure and access to the data so retained comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791) (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 90).

120 Furthermore, it must be stated that Article 15(1) of Directive 2002/58 does not preclude the competent national authorities from ordering a measure of expedited retention at the first stage of an investigation into a serious threat to public security or a possible serious crime, namely from the time when those authorities may, in accordance with the relevant provisions of national law, commence such an investigation (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 91).

121 Again as regards the variety of measures for the retention of traffic and location data referred to in paragraph 75 above, it must be stated that those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently. Accordingly, 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 interpreted by case-law resulting from the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), does not preclude a combination of those measures (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 92).

122 In the fourth and final place, it must be emphasised that the proportionality of the measures adopted pursuant to Article 15(1) of Directive 2002/58 requires, according to the Court's settled case-law, as recalled in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 93).

123 In that context, it should be recalled that, in paragraph 51 of its judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238), the Court held that while the fight against serious crime is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques, that objective of general interest, however fundamental it may be, does not, in itself, justify that a measure providing

for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 94).

124 In the same vein, the Court stated, in paragraph 145 of the judgment of 6 October 2020, *La Quadrature du Net and Others (*C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate, as pointed out in paragraph 64 above, to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by national legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 95).

125 Furthermore, the judgments of the European Court of Human Rights of 25 May 2021, *Big Brother Watch and Others v. the United Kingdom* (CE:ECHR:2021:0525JUD005817013), and of 25 May 2021, *Centrum för Rättvisa v. Sweden* (CE:ECHR:2021:0525JUD003525208), relied on by certain governments at the hearing to argue that the ECHR does not preclude national legislation providing, in essence, for a general and indiscriminate retention of traffic and location data, cannot call into question the interpretation of Article 15(1) of Directive 2002/58 resulting from the foregoing considerations. Those judgments concerned the bulk interception of data relating to international communications. Thus, as the Commission observed at the hearing, the European Court of Human Rights did not rule, in those judgments, on the compatibility with the ECHR of a general and indiscriminate retention of traffic and location data on national territory or even a large-scale interception of those data for the purposes of the prevention, detection and investigation of serious criminal offences. In any event, it should be borne in mind that Article 52(3) of the Charter is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union, with the result that, for the purpose of interpreting the Charter, account must be taken of the corresponding rights of the ECHR only as the minimum threshold of protection (judgment of 17 December 2020, *Centraal Israëlitisch Consistorie van België and Others*, C-336/19, EU:C:2020:1031, paragraph 56).

Access to data that have been retained in a general and indiscriminate way

126 At the hearing, the Danish Government argued that the competent national authorities should be able to access, for the purpose of combating serious crime, traffic and location data that have been retained in a general and indiscriminate way, in accordance with the case-law arising from the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 to 139), in order to confront a serious threat to national security which is shown to be genuine and present or foreseeable.

127 It should be observed, first of all, that authorising access, for the purpose of combating serious crime, to traffic and location data which have been retained in a general and indiscriminate way would make that access depend upon circumstances unrelated to that objective, according to whether or not, in the Member State concerned, there was a serious threat to national security as referred to in the preceding paragraph, whereas, in view of the sole objective of the fight against serious crime which must justify the retention of those data and access thereto, there is nothing to justify a difference in treatment, in particular as between the Member States (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 97).

128 As the Court has already held, access to traffic and location data retained by providers of electronic communications services in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting that directive, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective

pursued by access is greater than that of the objective which justified retention (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 98).

129 The Danish Government's argument refers to a situation in which the objective pursued by the access request proposed, namely the fight against serious crime, is of lesser importance in the hierarchy of objectives of public interest than that which justified the retention, namely the safeguarding of national security. To authorise, in that situation, access to retained data would be contrary to that hierarchy of public interest objectives recalled in the preceding paragraph and in paragraphs 68, 71, 72 and 73 above (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 99).

130 In addition and moreover, in accordance with the case-law recalled in paragraph 74 above, traffic and location data cannot be the object of general and indiscriminate retention for the purpose of combating serious crime and, therefore, access to those data cannot be justified for that same purpose. Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of safeguarding national security against a genuine and present or foreseeable threat, in the circumstances referred to in paragraph 71 above, the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime, recalled in paragraph 74 above (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 100).

131 In the light of all of the foregoing considerations, the answer to the question referred for a preliminary ruling 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 legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, that Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding national legislative measures that:

– allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;

– provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;

– allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for

a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

Costs

132 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:

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 meaning that:

it precludes national legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data;

it does not preclude legislative measures that:

– **allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;**

– **provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;**

– **provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;**

– **provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;**

– **allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,**

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

[Signatures]

---

* Language of the case: German.