JUDGMENT OF THE COURT (Grand Chamber)

5 April 2022 (*)

(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Confidentiality of the communications – Providers of electronic communications services – General and indiscriminate retention of traffic and location data – Access to retained data – Subsequent court supervision – Directive 2002/58/EC – Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Possibility for a national court to restrict the temporal effect of a declaration of the invalidity of national legislation that is incompatible with EU law – Excluded)

In Case C 140/20,

REQUEST for a preliminary ruling under Article 267 TFEU from the Supreme Court (Ireland), made by decision of 25 March 2020, received at the Court on 4 August 2016, in the proceedings

G.D.

v

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and N. Jääskinen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, F. Biltgen, P.G. Xuereb, 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:

– G.D., by J. Dunphy, Solicitor, R. Kennedy, Senior Counsel, and R. Farrell, Senior Counsel, and K. McCormack, Barrister-at-Law,

– the Commissioner of An Garda Síochána, the Minister for Communications, Energy and Natural Resources and the Attorney General, by M. Browne, S. Purcell, C. Stone and J. Quaney and by A. Joyce, acting as Agents, and by S. Guerin, Senior Counsel, and P. Gallagher, Senior Counsel, D. Fennelly and L. Dwyer, Barristers-at-Law,

– the Belgian Government, by P. Cottin and J. C. Halleux, acting as Agents, and by J. Vanpraet, advocaat,

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

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

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

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

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

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

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

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

– the Portuguese Government, by L. Inez Fernandes and by P. Barros da Costa and I. Oliveira, acting as Agents,

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

– the Swedish Government, by O. Simonsson and J. Lundberg and by H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson and H. Eklinder, acting as Agents,

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

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

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

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’).

2 The request has been made in proceedings between G.D. and the Commissioner of An Garda Síochána (Commissioner of the national police force, Ireland), the Minister for Communications, Energy and Natural Resources (Ireland) and the Attorney General, concerning the validity of the Communications (Retention of Data) Act 2011 (‘the 2011 Act’).

Legal context

European Union law

3 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/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.’

4 Article 1 of Directive 2002/58, headed ‘Scope and aim’, provides:

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

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

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

5 Article 2 of Directive 2002/58, headed ‘Definitions’, provides:

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

The following definitions shall also apply:

(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;

…’

6 Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:

‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the [European Union], including public communications networks supporting data collection and identification devices.’

7 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.’

8 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.

…'

9 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. …'

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

Irish law

11 As stated in the order for reference, the 2011 Act was adopted in order to transpose into the Irish legal order Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

12 Section 1 of the 2011 Act defines ‘data’ as ‘traffic data or location data and the related data necessary to identify the subscriber or user’ and a ‘serious offence’ as one which is punishable by imprisonment for a term of five years or more and also those other offences listed in Schedule 1 to that act.

13 Section 3(1) of the 2011 Act requires all providers of electronic communications services to retain the data referred to in Schedule 2, Part 1, for a period of two years and the data referred to in Schedule 2, Part 2, for a period of one year.

14 Schedule 2, Part 1, to the 2011 Act applies, inter alia, to fixed network telephony data and mobile telephony data that permit the identification of the source, the destination, and the date and time of the start and end of a communication, the type of communication involved, the type of location and the geographic location of the communications equipment used. In particular, point 6 of Part 1 of Schedule 2 provides for the retention of data necessary to identify the location of mobile communication equipment, those data being, first, the identity of the cell (‘cell ID’) and, second, data identifying the geographical location of cells by reference to their cell ID during the period for which communication data are retained.

15 Schedule 2, Part 2, to the 2011 Act covers data relating to internet access, internet email and internet telephony and includes, inter alia, the user identification number (‘user ID’) and telephone number, the Internet Protocol (IP) address and the date, time and duration of a communication. The content of communications does not fall within this type of data.

16 Under sections 4 and 5 of the 2011 Act, service providers must take specified measures to ensure that data are protected against unauthorised access.

17 Section 6 of the 2011 Act, which lays down the conditions under which a disclosure request may be made, provides in paragraph 1:

‘A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for—

(a) the prevention, detection, investigation or prosecution of a serious offence,

(b) the safeguarding of the security of the State,

(c) the saving of human life.’

18 Section 7 of the 2011 Act requires service providers to comply with disclosure requests referred to in section 6 thereof.

19 For the purpose of reviewing the decision of the member of the Garda Síochána referred to in section 6 of the 2011 Act, a complaint procedure is provided for in section 10 thereof and a procedure before the designated judge, within the meaning of section 12 thereof, who is responsible for examining the application of the provisions of that act.

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

20 In March 2015, G.D. was sentenced to life imprisonment for the murder of a person who disappeared in August 2012 and whose remains were not discovered until September 2013. In the appeal against his conviction, G.D. criticised the first-instance court in particular for having incorrectly admitted as evidence traffic and location data relating to telephone calls, on the ground that the 2011 Act, which governed the retention of that data and on the basis of which the police carrying out the investigation had obtained access to those data, infringed rights conferred on him by EU law. That appeal is currently pending.

21 In order to be able to contest, as part of the criminal proceedings, the admissibility of that evidence, G.D. brought civil proceedings before the High Court (Ireland) seeking a declaration that some of the provisions of the 2011 Act are invalid. By decision of 6 December 2018, that court upheld G.D.'s submission and held that section 6(1)(a) of that act was incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Ireland appealed against that decision to the Supreme Court (Ireland), which is the referring court.

22 The criminal proceedings pending before the Court of Appeal (Ireland) were stayed until the delivery of the referring court's decision in the main civil proceedings.

23 Before the referring court, Ireland submitted that, in order to determine whether interference with the right to private life enshrined in Article 7 of the Charter as a result of the retention of traffic and location data under the 2011 Act is proportionate, it is necessary to examine the objectives of the regime established by that law as a whole. In addition, according to that Member State, that act established a detailed framework governing access to retained data by virtue of which the section responsible, within the national police force, for the prior examination of requests for access was functionally independent from the national police in the conduct of its duties and, therefore, satisfied the requirement for a prior review to be carried out by an independent administrative entity. That system of review is complemented by a complaints procedure and by judicial review. Finally, that Member State submits that, if the 2011 Act is ultimately held to be inconsistent with EU law, the temporal effect of any declaration which the referring court makes as a result should be prospective only.

24 For his part, G.D. submits that the system of general and indiscriminate retention of data established by the 2011 Act and the regime for access to those data provided for by that law are incompatible with EU law as interpreted, in particular, by the Court in paragraph 120 of the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C 203/15 and C 698/15, EU:C:2016:970).

25 The referring court states, as a preliminary matter, that it is for it to determine only whether the High Court was correct in law to hold that section 6(1)(a) of the 2011 Act was incompatible with EU law and that, by contrast, the question of the admissibility of the evidence submitted in the context of the criminal proceedings falls within jurisdiction of the Court of Appeal which is seised of the appeal brought against the conviction.

26 In that context, the referring court has doubts, first of all, as to the requirements of EU law as regards the retention of data for the purposes of combating serious crime. In that regard, it considers, in essence, that only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively, which the targeted and expedited retention (*quick freeze*) of data does not make possible. As regards targeted retention, the referring court wonders whether it is possible to target specific groups or geographic areas for the purposes of combating serious crimes, since some serious crimes rarely involve circumstances known to the competent national authorities enabling them to suspect the commission of an offence in advance. In addition, targeted retention could give rise to discrimination. As for expedited retention, the referring court considers that that is only useful in situations where it is possible to identify a suspect in the very early stages of an investigation.

27 As regards, next, access to data retained by providers of electronic communications services, the referring court explains that the national police force established, within its organisation, a system of self-certification of requests addressed to those service providers. Thus, it is clear from the evidence produced before the High Court that the Commissioner of the national police force decided, by an internal measure, that the requests for access made pursuant to the 2011 Act must be dealt with in a centralised manner, by a single national police officer of the rank of Chief Superintendent, namely the head of the security and intelligence section. If that official considers that the data concerned are necessary for the purposes, inter alia, of the prevention, detection, investigation or prosecution of a serious offence, he or she may address a request for access to the providers of electronic communications services. In addition, the Commissioner of the national police force established, within the police force, an independent unit entitled the Telecommunications Liaison Unit ('the TLU') in order to provide support to the head of the security and

intelligence section in the exercise of his or her duties and to serve as a single point of contact with those service providers.

28 The referring court adds that, during the period concerned by the criminal investigation brought against G.D., all the requests for access were required to be approved in the first place by a superintendent or inspector acting in that capacity, before they were sent to the TLU to be processed, and that the investigators were directed to include sufficient detail in their requests for access so that an informed decision could be taken. In addition, the TLU and the head of the security and intelligence section were required to examine the legality, necessity and proportionality of requests for access, taking into account the fact that that head could be called upon to answer for his or her decision before the judge designated by the High Court. Furthermore, the TLU is also subject to audit by the Data Protection Commissioner (Ireland).

29 Finally, the referring court is uncertain as to the scope and temporal effects of a possible declaration of incompatibility of the 2011 Act with EU law. In that regard, it states that such a declaration could only be applied prospectively on the ground the data used as evidence in the criminal proceedings against G.D. were the subject of retention and access at the end of 2013, namely in a period during which Ireland was required to apply the provisions of the 2011 Act transposing Directive 2006/24. According to Ireland, that solution would also be appropriate since, otherwise, the investigation and prosecution of serious offences in Ireland, and the situation of persons already tried and convicted could be seriously impacted.

30 It was in those circumstances that the Supreme Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Is a general/universal data retention regime – even subject to stringent restrictions on retention and access – *per se* contrary to the provisions of Article 15 of Directive [2002/58], interpreted in the light of the Charter?

(2) In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive [2006/24], and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive [2002/58]?

(3) In assessing, in the context of determining the compatibility with [EU] law and in particular with Charter Rights of a national measure for access to retained data, what criteria should a national court apply in considering whether any such access regime provides the required independent prior scrutiny as determined by the Court of Justice in its case-law? In that context, can a national court, in making such an assessment, have any regard to the existence of ex post judicial or independent scrutiny?

(4) In any event, is a national court obliged to declare the inconsistency of a national measure with the provisions of Article 15 of [Directive 2002/58], if the national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime?

(5) If a national court is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive [2002/58], as interpreted in the light of the Charter, is it entitled to limit the temporal effect of any such declaration, if satisfied that a failure to do so would lead to “resultant chaos and damage to the public interest” (in line with the approach taken, for example, in *R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, at paragraph 46)?

(6) May a national court invited to declare the inconsistency of national legislation with Article 15 of [Directive 2002/58], and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of [Directive 2006/24] issued by the [judgment of 8 April 2014, *Digital Rights Ireland and Others* (C 293/12 and C 594/12, EU:C:2014:238)]?'

Consideration of the questions referred

The first, second and fourth questions

31 By its first, second and fourth question, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that provides for the general and indiscriminate retention of traffic and location data for the purposes of combating serious crime.

32 It should be noted, as a preliminary point, that 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 105 and the case-law cited).

33 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.

34 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.

35 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 (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 107).

36 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 (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C 203/15 and C 698/15, EU:C:2016:970, paragraph 83, and 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 106).

37 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 (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 109).

38 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 payments pursued in order to obtain payment. 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.

39 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.

40 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 35 of this judgment, 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 that data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C 203/15 and C 698/15, EU:C:2016:970, paragraph 89, and 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 111).

41 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 112 and the case-law cited).

42 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, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (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 113 and the case-law cited).

43 Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (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 114 and the case-law cited).

44 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, second, 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 (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, paragraphs 115 and 116 and the case-law cited).

45 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 117 and the case-law cited).

46 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. Second, 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 (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, paragraphs 118 and 119 and the case-law cited).

47 In that regard, 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 44 of this judgment, 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.

48 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 34 to 37 of this judgment, 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraphs 120 to 122 and the case-law cited).

49 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 126 and the case-law cited).

50 It is against the backdrop of those different positive obligations that the Court must strike a balance between the various interests and rights at issue. The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, whose corresponding safeguards are set out in Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child's physical and moral well-being is at risk. However, the measures to be taken by the competent authorities must fully respect due process and the other safeguards limiting the scope of criminal investigation powers, as well as other freedoms and rights. In particular, according to that court, a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected (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 127 and 128 and the case-law cited).

51 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 35 of this judgment 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 (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 129).

52 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 130 and the case-law cited).

53 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 131 and the case-law cited).

54 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

55 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. In particular, as regards combating serious crime, the data whose retention is provided for must be capable of contributing to the prevention, detection or prosecution of serious offences (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C 293/12 and C 594/12, EU:C:2014:238, paragraph 59, and 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 133).

56 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.

57 In that regard, the Court held that the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (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, paragraphs 135 and 136).

58 It is for that reason that the Court held that Article 15(1) of Directive 2002/58, 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 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).

59 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 6 October 2020, *La Quadrature du Net and Others*, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraph 140 and the case-law cited).

60 At the hearing, the European Commission submitted that particularly serious crime could be treated in the same way as a threat to national security.

61 However, 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 (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 135).

62 It should also be observed that, 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 (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, paragraphs 136 and 137).

63 Thus, criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. As the Advocate General observed in points 49 to 50 of his Opinion, 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.

64 It also follows that the fact, recalled in the second question referred for a preliminary ruling, that traffic and location data were legally the object of retention for the purpose of safeguarding national security does not have any bearing on the legality of their retention for the purpose of combating serious crime.

65 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 respect for private life. 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 46 of this judgment, which is liable to result from the retention of those data, and, second, 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 (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, paragraphs 141 and 142 and the case-law cited).

66 In addition, the Court has emphasised that national legislation providing for the general and indiscriminate retention of traffic and location data covers the electronic communications of practically the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. Such legislation is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and a threat to public security. In particular, as the Court has already held, such legislation is not restricted to retention in relation to (i) data pertaining to a time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to combating serious crime (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 143 and 144 and the case-law cited).

67 However, in paragraph 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), the Court stated that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that 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;

– 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.

68 In the present order for reference, which was lodged with the Court before the 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), and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C 746/18, EU:C:2021:152), were delivered, the referring court considered however that only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively. At the hearing on 13 September 2021, it was submitted, inter alia by Ireland and the French Government, that that conclusion was not invalidated by the fact that it was possible for the Member States to have recourse to the measures referred to in the preceding paragraph.

69 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.

70 In the second place, it must be noted 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, as interpreted by the case-law recalled in paragraph 67 of this

judgment, 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, second, of IP addresses assigned to the source of a connection.

71 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.

72 As is clear from the case-law summarised in paragraph 67 of this judgment, Directive 2002/58 does not preclude, for the purposes of combating crime in general, the general 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.

73 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 50 to 53 of this judgment, 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), 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 (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, paragraphs 153 and 154).

74 Hence, the Court held that such general and indiscriminate retention solely of 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 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, as referred to in paragraphs 155 and 156 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).

75 In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, the indications provided in the order for reference show a narrower understanding of the scope of those measures than that upheld in the case-law recalled in paragraph 67 of this judgment. While, as is recalled in paragraph 40 of this judgment, 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.

76 As regards, first, targeted retention, the Court 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 (judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C 203/15 and C 698/15, EU:C:2016:970, paragraph 111, and 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 148).

77 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 (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C 203/15 and C 698/15, EU:C:2016:970, paragraph 110, and 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 149).

78 Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of 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.

79 Second, 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 (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, paragraphs 150 and the case-law cited).

80 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 entirely unconnected with any potentially discriminatory factors.

81 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.

82 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 76 to 81 of this judgment 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 (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 151).

83 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.

84 In any event, as Advocate General Campos Sánchez-Bordona observed in point 50 of his Opinion in Joined Cases *SpaceNet and Telekom Deutschland* (C 793/19 and C 794/19, EU:C:2021:939), 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 retention of traffic and location data.

85 As regards, second, 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 (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, paragraphs 160 and 161).

86 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 50 to 53 of this judgment, 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 (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 163).

87 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).

88 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 findings in paragraph 55 of this judgment, 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 (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 165).

89 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.

90 Such expedited retention may, according to the Court's case-law recalled in paragraph 88 of this judgment 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 or a person, possibly the victim of a serious crime, who 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).

91 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 for public security or a possible serious crime, namely from the time when the authorities may, in accordance with the provisions of national law, commence such an investigation.

92 As regards the variety of measures for the retention of traffic and location data referred to in paragraph 67 of this judgment, 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.

93 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.

94 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.

95 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 49 of this judgment, 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 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.

96 At the hearing, the Danish Government submitted that the competent national authorities should be able to access, for the purpose of fighting serious crime, traffic and location data which have been retained in a general and indiscriminate way, in accordance with the line of 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, paragraphs 135 to 139), in order to address a serious threat to national security that is genuine and present, or foreseeable.

97 It should be observed, first of all, that the fact of 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 facts that fall outside 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.

98 As the Court has already held, access to traffic and location data retained by providers 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 Directive 2002/58, 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 (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, paragraphs 165 and 166).

99 The Danish Government's submission 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 also to paragraphs 53, 56, 57 and 59 of this judgment.

100 In addition and moreover, in accordance with the case-law recalled in paragraph 65 of this judgment, 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 the safeguarding of national security against a genuine and present or foreseeable threat, in the circumstances referred to in paragraph 58 of this judgment, 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 65.

101 In the light of all of the foregoing considerations, the answer to the first, second and fourth questions 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 legislative measures which provide, as a preventive measure, for the purposes of combating serious crime and for the prevention of serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, Article 15(1), 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 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.

The third question

102 By its third question, the referring court asks, in essence, whether, 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 pursuant to which the centralised processing of requests for access to retained data, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, assisted by a unit established within the police service which enjoys a degree of autonomy in the exercise of its duties and whose decisions may subsequently by subject to judicial review.

103 As a preliminary matter, it should be borne in mind that, while it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to data in their possession, the national legislation must, in order to satisfy the requirement of proportionality, as recalled in paragraph 54 of this judgment, 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 (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 48 and the case-law cited).

104 In particular, national legislation governing the access by the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C 746/18, EU:C:2021:152, paragraph 49 and the case-law cited).

105 Accordingly, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or

of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that those data might, in a specific case, make an effective contribution to combating such activities (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C 746/18, EU:C:2021:152, paragraph 50 and the case-law cited).

106 In order to ensure, in practice, that those conditions are fully observed, it is essential that access by the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C 746/18, EU:C:2021:152, paragraph 51 and the case-law cited).

107 One of the requirements for the prior review is that the court or independent administrative body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C 746/18, EU:C:2021:152, paragraph 52).

108 Where that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. Accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the body entrusted with the prior review, first, should not be involved in the conduct of the criminal investigation in question and, second, must have a neutral stance vis-à-vis the parties to the criminal proceedings (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, paragraphs 53 and 54).

109 Thus, the Court has, inter alia, found that a public prosecutor's office, which directs the investigation procedure and, where appropriate, brings the public prosecution cannot be considered to have third party status in relation to the interests at issue, since it has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of bringing it, where appropriate, before the court that has jurisdiction. Consequently, a public prosecutor's office is not in a position to carry out the prior review of requests for access to retained data (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, paragraphs 55 and 57).

110 Finally, the independent review required in accordance with Article 15(1) of Directive 2002/58 must take place before any access to the data concerned, except in the event of duly justified urgency, in which case the review must take place within a short time. A subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, 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 189, and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C 746/18, EU:C:2021:152, paragraph 58).

111 In the present case, it is apparent from the order for reference that the 2011 Act assigns to a police officer, whose rank is not below that of chief superintendent, the power to carry out the prior review of requests for access to data issued by the police investigation services and to request the providers of electronic communications services to transmit the data that they retain to those services. To the extent that that officer does not have the status of a third party in relation to those services, he or she does not fulfil the requirements for independence and impartiality recalled in paragraph 108 of this judgment, notwithstanding the fact that he or she is assisted in that duty by a police unit, in this case the TLU, which benefits from a certain degree of autonomy in the exercise of its duties.

112 Next, while it is true that the 2011 Act provides for mechanisms of review subsequent to the decision of the competent police officer in the form of a complaint procedure and a procedure before a judge responsible for examining the application of the provisions of that act, it is clear from the case-law recalled in paragraph 110 of this judgment that a review carried out subsequently cannot be substituted for the requirement, recalled in paragraph 106 of this judgment, for a review that is independent and, except in duly justified urgent cases, undertaken beforehand.

113 Finally, the 2011 Act does not lay down any objective criteria which define precisely the conditions and circumstances in which national authorities must be granted access to data and the police officer responsible for processing the requests for access to retained data is solely competent, as Ireland confirmed at the hearing, to assess the suspicions that exist with respect to the persons concerned and the need for access to data that relate to them.

114 Consequently, the answer to the third question is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.

The fifth and sixth questions

115 By its fifth and sixth questions, which it is appropriate to examine together, the referring courts asks, in essence, whether EU law must be interpreted as meaning that a national court may limit the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter.

116 It is apparent from the information provided by the referring court that the national legislation at issue in the main proceedings, namely the 2011 Act, was adopted in order to transpose into national law Directive 2006/24, which was later declared invalid by the Court in its judgment of 8 April 2014, *Digital Rights Ireland and Others* (C 293/12 and C 594/12, EU:C:2014:238).

117 In addition, the referring court states that, while the assessment of the admissibility of the evidence based on data retained pursuant to the 2011 Act and relied on as regards G.D. in the context of the criminal proceedings is a matter for the criminal court, it is nevertheless, in the context of the civil proceedings, its responsibility to rule on the validity of the provisions at issue of that act and on the temporal effects of a declaration of invalidity of those provisions. Thus, while the sole issue raised before the referring court is that of the validity of the provisions of the 2011 Act, that court considers however that it is necessary to inquire of the Court as to the effect of a possible finding of invalidity on the admissibility of the evidence obtained by means of the general and indiscriminate retention of data that that act permitted.

118 In the first place, it should be recalled that the principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State

bodies to give full effect to the various provisions of EU law, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (see, to that effect, judgments of 15 July 1964, *Costa*, 6/64, EU:C:1964:66, p. 594; of 19 November 2019, *A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)*, C 585/18, C 624/18 and C 625/18, EU:C:2019:982, paragraphs 157, 158 and 160; and 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 214 and 215).

119 Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (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 216 and 217 and the case-law cited).

120 It is true that the Court has held, in a case concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned, which cannot be remedied by any other means or alternatives, particularly in the context of the internal market, and continues only for as long as is strictly necessary to remedy the breach (see, to that effect, judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen*, C 411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181).

121 However, unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph (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 219).

122 Maintaining the effects of national legislation such as the 2011 Act would mean that the legislation would continue to impose on providers of electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been retained (see, by analogy, 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 219).

123 Therefore, the referring court cannot limit the temporal effects of a declaration of invalidity which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, 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 220).

124 In that regard, as the Advocate General observed in essence in point 75 of his Opinion, the fact that that legislation was adopted in order to transpose Directive 2006/24 into national law is irrelevant since, due to the Court's decision that that directive was invalid, the invalidity has effect as from the date of its entry into force (see, to that effect, judgment of 8 February 1996, *FMC and Others*, C 212/94, EU:C:1996:40,

paragraph 55), the validity of that national legislation must be assessed by the referring court in the light of Directive 2002/58 and the Charter, as interpreted by the Court.

125 As regards, more specifically, the interpretation of Directive 2002/58 and the Charter upheld 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), and of 6 October 2020, *La Quadrature du Net and Others* (C 511/18, C 512/18 and C 520/18, EU:C:2020:791), it should be recalled that, according to settled case-law, the interpretation that the Court gives to a rule of EU law, in the exercise of the jurisdiction conferred upon it by Article 267 TFEU, clarifies and defines the meaning and scope of that rule as it must be, or ought to have been, understood and applied from the time of its coming into force. It follows that the rule as thus interpreted may and must be applied by the courts to legal relationships arising and established before the judgment ruling on the request for interpretation, provided that in other respects the conditions for bringing an action relating to the application of that rule before the courts having jurisdiction are satisfied (judgment of 16 September 2020, *Romenergo and Aris Capital*, C 339/19, EU:C:2020:709, paragraph 47 and the case-law cited).

126 In that regard, it should also be stated that a temporal limitation of the effects of the interpretation given was not imposed in the judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C 203/15 and C 698/15, EU:C:2016:970), and of 6 October 2020, *La Quadrature du Net and Others* (C 511/18, C 512/18 and C 520/18, EU:C:2020:791), with the result that, in accordance with the case-law recalled in paragraph 119 of this judgment, it should not be imposed in a judgment of the Court subsequent to those judgments.

127 Finally, as regards the effect of a declaration of the potential incompatibility of the 2011 Act with Directive 2002/58, read in the light of the Charter, on the admissibility of evidence relied on against G.D. in the context of the criminal proceedings, it suffices to refer to the Court's case-law on that subject, in particular the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C 746/18, EU:C:2021:152), from which it follows that that admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

128 Having regard to the foregoing considerations, the answer to the fifth and sixth questions is that EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member State, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

Costs

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

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

1. **Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009,**

read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data. However, that Article 15(1), read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that 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;**

– **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 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.

2. **Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data, which have been retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.**

3. **EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of the Charter of Fundamental Rights. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.**

Lenaerts Arabadjiev Prechal

Rodin Jarukaitis Jääskinen

von Danwitz	Safjan	Biltgen
Xuereb	Piçarra	Rossi
	Kumin	

Delivered in open court in Luxembourg on 5 April 2022.

A. Calot Escobar	K. Lenaerts
Registrar	President

---

* Language of the case: English.