Provisional text

JUDGMENT OF THE COURT (Grand Chamber)

6 October 2020 (*)

Table of Contents

(Reference for a preliminary ruling – Processing of personal data in the electronic communications

sector – Providers of electronic communications services – Hosting service providers and Internet access providers – General and indiscriminate retention of traffic and location data – Automated analysis of data – Real-time access to data – Safeguarding national security and combating terrorism – Combating crime – Directive 2002/58/EC – Scope – Article 1(3) and Article 3 – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Directive 2000/31/EC – Scope – Charter of Fundamental Rights of the European Union – Articles 4, 6, 7, 8 and 11 and Article 52(1) – Article 4(2) TEU)

In Joined Cases C-511/18, C-512/18 and C-520/18,

REQUESTS for a preliminary ruling under Article 267 TFEU from the Conseil d'État (Council of State, France), made by decisions of 26 July 2018, received at the Court on 3 August 2018 (C-511/18 and C-512/18), and from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 19 July 2018, received at the Court on 2 August 2018 (C-520/18), in the proceedings

La Quadrature du Net (C-511/18 and C-512/18),

French Data Network (C-511/18 and C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 and C-512/18),

Igwan.net (C-511/18)

v

Premier ministre (C-511/18 and C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 and C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18),

interveners:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

and

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

v

Conseil des ministres,

interveners:

Child Focus (C-520/18),

THE COURT (Grand Chamber),

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

Advocate General: M. Campos Sánchez-Bordona,

Registrar: C. Strömholm, Administrator,

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

after considering the observations submitted on behalf of:

– La Quadrature du Net, the Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net and the Center for Democracy and Technology, by A. Fitzjean Ò Cobhthaigh, avocat,

– French Data Network, by Y. Padova, avocat,

– Privacy International, by H. Roy, avocat,

– the Ordre des barreaux francophones et germanophone, by E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart and J.-F. Henrotte, avocats,

– the Académie Fiscale ASBL and UA, by J.-P. Riquet,

– the Liga voor Mensenrechten ASBL, by J. Vander Velpen, avocat,

– the Ligue des Droits de l'Homme ASBL, by R. Jespers and J. Fermon, avocats,

– VZ, WY and XX, by D. Pattyn, avocat,

– Child Focus, by N. Buisseret, K. De Meester and J. Van Cauter, avocats,

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

– the Belgian Government, by J.-C. Halleux, P. Cottin and C. Pochet, acting as Agents, and by J. Vanpraet, Y. Peeters, S. Depré and E. de Lophem, avocats,

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

– the Danish Government, initially by J. Nymann-Lindegren, M. Wolff and P. Ngo, then by J. Nymann-Lindegren and M. Wolff, acting as Agents,

– the German Government, initially by J. Möller, M. Hellmann, E. Lankenau, R. Kanitz and T. Henze, then by J. Möller, M. Hellmann, E. Lankenau and R. Kanitz, acting as Agents,

– the Estonian Government, by N. Grünberg and A. Kalbus, acting as Agents,

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

– the Spanish Government, initially by L. Aguilera Ruiz and A. Rubio González, then by L. Aguilera Ruiz, acting as Agent,

– the Cypriot Government, by E. Neofytou, acting as Agent,

– the Latvian Government, by V. Soņeca, acting as Agent,

– the Hungarian Government, initially by M.Z. Fehér and Z. Wagner, then by M.Z. Fehér, acting as Agent,

– the Netherlands Government, by M.K. Bulterman and M.A.M. de Ree, acting as Agents,

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

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

– the United Kingdom Government, by S. Brandon, acting as Agent, and by G. Facenna QC and C. Knight, Barrister,

– the Norwegian Government, by J. Vangsnes, acting as Agent,

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

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

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

gives the following

Judgment

1 These requests for a preliminary ruling concern the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’), and of Articles 12 to 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) (OJ 2000 L 178, p. 1), read in the light of Articles 4, 6, 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’) and Article 4(2) TEU.

2 The request in Case C-511/18 has been made in proceedings between La Quadrature du Net, French Data Network, the Fédération des fournisseurs d’accès à Internet associatifs and Igwan.net, on the one hand, and the Premier ministre (Prime Minister, France), the Garde des Sceaux, ministre de la Justice (Keeper of the Seals, Minister for Justice, France), the ministre de l’Intérieur (Minister for the Interior, France) and the ministre des Armées (Minister for the Armed Forces, France), on the other, concerning the lawfulness of: décret n° 2015-1185 du 28 septembre 2015 portant

désignation des services spécialisés de renseignement (Decree No 2015-1185 of 28 September 2015 designating specialised intelligence services) (*Journal Officiel de la République Française* (JORF) of 29 September 2015, text 1 of 97; 'Decree No 2015-1185'); décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decree No 2015-1211 of 1 October 2015 on litigation relating to the implementation of intelligence techniques subject to authorisation and files on matters of State security) (JORF of 2 October 2015, text 7 of 108; 'Decree No 2015-1211'), décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (Decree No 2015-1639 of 11 December 2015 on the designation of services other than the specialist intelligence services which are authorised to use the techniques referred to in Title V of Book VIII of the Internal Security Code, adopted pursuant to Article L. 811-4 thereof) (JORF of 12 December 2015, text 28 of 127; 'Decree No 2015-1639'), and décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Decree No 2016-67 of 29 January 2016 on intelligence gathering techniques) (JORF of 31 January 2016, text 2 of 113; 'Decree No 2016-67').

3 The request in Case C-512/18 has been made in proceedings between French Data Network, La Quadrature du Net and the Fédération des fournisseurs d'accès à Internet associatifs, on the one hand, and the Prime Minister (France) and the Keeper of the Seals, Minister for Justice (France), on the other, concerning the lawfulness of Article R. 10-13 of the code des postes et des communications électroniques (Post and Electronic Communications Code; 'the CPCE') and décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decree No 2011-219 of 25 February 2011 on the retention and communication of data that can be used to identify any person having assisted in the creation of content posted online) (JORF of 1 March 2011, text 32 of 170; 'Decree No 2011-219').

4 The request in Case C-520/18 has been made in proceedings between the Ordre des barreaux francophones et germanophone, the Académie Fiscale ASBL, UA, the Liga voor Mensenrechten ASBL, the Ligue des Droits de l'Homme ASBL, VZ, WY and XX, on the one hand, and the Conseil des ministres (Council of Ministers, Belgium), on the other, concerning the lawfulness of the loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (Law of 29 May 2016 on the collection and retention of data in the electronic telecommunications sector) (*Moniteur belge* of 18 July 2016, p. 44717; 'the Law of 29 May 2016').

Legislative framework

EU law

Directive 95/46

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed with effect from 25 May 2018 by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (OJ 2016 L 119, p 1). Article 3(2) of Directive 95/46 provided:

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

– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to

processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

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

6 Article 22 of Directive 95/46, which is in Chapter III of that directive, headed 'Judicial remedies, liability and sanctions', was worded as follows:

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

Directive 97/66

7 Under Article 5 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24, p. 1), headed 'Confidentiality of the communications':

'1. Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14(1).

2. Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.'

Directive 2000/31

8 Recitals 14 and 15 of Directive 2000/31 provide:

'(14) The protection of individuals with regard to the processing of personal data is solely governed by Directive [95/46] and Directive [97/66] which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

(15) The confidentiality of communications is guaranteed by Article 5 Directive [97/66]; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.'

9 Article 1 of Directive 2000/31 is worded as follows:

'1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary for the achievement of the objective set

out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

…

5. This Directive shall not apply to:

…

(b) questions relating to information society services covered by Directives [95/46] and [97/66];

…'

10 Article 2 of Directive 2000/31 is worded as follows:

'For the purpose of this Directive, the following terms shall bear the following meanings:

(a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC [of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ 1998 L 204, p. 37)] as amended by Directive 98/48/EC [of the European Parliament and of the Council of 20 July 1998 (OJ 1998 L 217, p. 18)];

…'

11 Article 15 of Directive 2000/31 provides:

'1. 'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'

Directive 2002/21

12 Recital 10 of 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) states:

'The definition of "information society service" in Article 1 of Directive [98/34, as amended by Directive 98/48,] spans a wide range of economic activities which take place on-line. Most of these activities are not covered by the scope of this Directive because they do not consist wholly or mainly in the conveyance of signals on electronic communications networks. Voice telephony and electronic mail conveyance services are covered by this Directive. The same undertaking, for example an Internet service provider, can offer both an electronic communications service, such as access to the Internet, and services not covered under this Directive, such as the provision of web-

based content.'

13 Article 2 of Directive 2002/21 provides:

'For the purposes of this Directive:

…

(c) "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive [98/34], which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

…'

Directive 2002/58

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

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

…

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

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

…

(11) Like Directive [95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [Union] law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950,] as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

…

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

…

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

…

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

15 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.'

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

'Save as otherwise provided, the definitions in Directive [95/46] and in Directive [2002/21] 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;

…'

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

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

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

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

…

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

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

'1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

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

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

…

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

…'

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

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

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

'1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [Union] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

…

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

…'

Regulation 2016/679

22 Recital 10 of Regulation 2016/679 states:

'In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and

freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …'

23 Article 2 of that regulation provides:

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

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

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

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

…

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

…

4. This Regulation shall be without prejudice to the application of Directive [2000/31], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.'

24 Article 4 of that regulation reads as follows:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

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

…'

25 Article 5 of Regulation 2016/679 provides:

'1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in

the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

…'

26 Article 6 of that regulation reads as follows:

'1. Processing shall be lawful only if and to the extent that at least one of the following applies:

…

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

…

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis … That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

…'

27 Article 23 of that regulation provides:

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

(a) national security;

(b) defence;

(c) public security;

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

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

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

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

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

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

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.’

28 Under Article 79(1) of that regulation:

‘Without prejudice to any available administrative or non-judicial remedy, including the right to

lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.'

29 Article 94 of Regulation 2016/679 provides:

'1. Directive [95/46] is repealed with effect from 25 May 2018.

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

30 Article 95 of that regulation provides:

'This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive [2002/58].'

French law

Code de la sécurité intérieure (Internal Security Code)

31 Book VIII of the legislative part of the code de la sécurité intérieure (Internal Security Code; 'the CSI') lays down rules relating to intelligence in Articles L. 801-1 to L. 898-1.

32 Article L. 811-3 of the CSI states:

'For the sole performance of their respective tasks, the specialised intelligence services may use the techniques referred to in Title V of this Book in order to gather intelligence relating to the protection and promotion of the following fundamental State interests:

1. National independence, territorial integrity and national defence;

2. Major foreign policy interests, the implementation of France's European and international commitments and the prevention of all forms of foreign interference;

3. France's major economic, industrial and scientific interests;

4. The prevention of terrorism;

5. The prevention of:

(a) attacks against the republican nature of the institutions;

(b) actions designed to maintain or rebuild groups that have been disbanded under Article L. 212-1;

(c) collective violence liable to cause serious disruption to the maintenance of law and order;

6. The prevention of organised crime;

7. The prevention of the proliferation of weapons of mass destruction.'

33 Article L. 811-4 of the CSI provides:

‘A decree adopted in the Conseil d’État (Council of State, France) following consultation of the Commission nationale de contrôle des techniques de renseignement (Commission for the Oversight of Intelligence Techniques, France) shall designate the services, other than the specialised intelligence services, within the purview of the Ministers for Defence, the Interior and Justice and the ministers responsible for economic affairs, the budget and customs, which may be authorised to use the techniques referred to in Title V of the present Book under the conditions laid down in this Book. It shall specify, for each service, the purposes mentioned in Article L. 811-3 and the techniques which may be authorised.’

34 The first paragraph of Article L. 821-1 of the CSI is worded as follows:

‘The implementation on national territory of the intelligence gathering techniques referred to in Chapters I to IV of Title V of this Book shall be subject to prior authorisation from the Prime Minister following consultation of the Commission for the Oversight of Intelligence Techniques.’

35 Article L. 821-2 of the CSI provides:

‘The authorisation mentioned in Article L. 821-1 shall be issued upon a written and reasoned application from the Minister for Defence, the Minister for the Interior, the Minister for Justice or the ministers responsible for economic affairs, the budget or customs. Each minister may delegate that power individually only to immediate staff with clearance to handle confidential material relating to national defence.

The application shall state:

1. the technique(s) to be implemented;

2. the service for which it is submitted;

3. the purpose(s) pursued;

4. the reason(s) for the measures;

5. the period of validity of the authorisation;

6. the person(s), place(s) or vehicle(s) concerned.

In respect of point 6, persons whose identity is not known may be designated by their identifiers or status and places or vehicles may be designated by reference to the persons who are the subject of the application.

…’

36 Under the first paragraph of Article L. 821-3 of the CSI:

‘The application shall be sent to the President or, failing that, to one of the members of the Commission for the Oversight of Intelligence Techniques mentioned in points 2 and 3 of Article L. 831-1, who shall provide the Prime Minister with an opinion within 24 hours. If the application is examined by the select panel or the full panel of the Commission, the Prime Minister shall be informed forthwith and the opinion shall be issued within 72 hours.’

37 Article L. 821-4 of the CSI provides:

‘Authorisation to implement the techniques referred to in Chapters I to IV of Title V of this Book shall be issued by the Prime Minister for a maximum period of four months. … The authorisation shall contain the grounds and statements set out in points 1 to 6 of Article L. 821-2. All authorisations shall be renewable under the same conditions as those laid down in this Chapter.

Where the authorisation is issued after obtaining an unfavourable opinion from the Commission for the Oversight of Intelligence Techniques, it shall state the reasons why that opinion was not followed.

…'

38 Article L. 833-4 of the CSI, which appears in Chapter III of Title III, provides:

'The Commission shall – on its own initiative or after receiving a complaint from any person wishing to verify that no intelligence techniques have been unlawfully implemented against him or her – conduct a review of the technique or techniques referred to with a view to determining whether they have been or are being implemented in accordance with this Book. It shall notify the complainant that the necessary investigations have been carried out, without confirming or denying their implementation.'

39 The first and second paragraphs of Article L. 841-1 of the CSI read as follows:

'Subject to the special provisions set out in Article L. 854-9 of this Code, the Conseil d'État (Council of State, France) shall have jurisdiction to hear, under the conditions laid down in Chapter III bis of Title VII of Book VII of the code de justice administrative (Code of Administrative Justice), actions concerning the implementation of the intelligence techniques referred to in Title V of this Book.

An action may be brought before it by:

1. any person wishing to verify that no intelligence techniques have been unlawfully implemented against him or her and who can demonstrate that the procedure provided for in Article L. 833-4 has been conducted beforehand;

2. the Commission for the Oversight of Intelligence Techniques, under the conditions laid down in Article L. 833-8.'

40 Title V of Book VIII of the legislative part of the CSI, concerning 'intelligence gathering techniques subject to authorisation', includes, inter alia, Chapter I, headed 'Access of the administrative authorities to connection data', containing Articles L. 851-1 to L. 851-7 of the CSI.

41 Article L. 851-1 of the CSI provides:

'Subject to the conditions laid down in Chapter I of Title II of this Book, the collection of information or documents processed or retained by their networks or electronic communications services, including technical data relating to the identification of the subscription or connection numbers to electronic communications services, the inventorying of the subscription and connection numbers of a specified person, the location of the terminal equipment used and the communications of a subscriber, namely the list of numbers called and calling and the duration and date of the communications, may be authorised from electronic communications operators and the persons referred to in Article L. 34-1 of the [CPCE] as well as from the persons referred to in Article 6(I)(1) and (2) of Loi n.° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy) [(JORF of 22 June 2004, p. 11168)].

By way of derogation from Article L. 821-2, written and reasoned applications for technical data relating to the identification of subscription or connection numbers to electronic communications services, or the inventorying of all the subscription or connection numbers of a specified person, shall be sent directly to the Commission for the Oversight of Intelligence Techniques by individually designated and authorised agents of the intelligence services referred to in Articles L. 811-2 and L. 811-4. The Commission shall issue its opinion under the conditions laid

down in Article L. 821-3.

A department reporting to the Prime Minister shall be responsible for gathering information or documents from the operators and persons referred to in the first paragraph of this article. The Commission for the Oversight of Intelligence Techniques shall have permanent, complete, direct and immediate access to the information or documents collected.

The detailed rules for the application of this article shall be laid down by decree adopted in the Conseil d'État (Council of State, France) following consultation of the Commission nationale de l'informatique et des libertés (Data Protection Authority, France) and the Commission for the Oversight of Intelligence Techniques.'

42 Article L. 851-2 of the CSI provides:

'I. Under the conditions laid down in Chapter I of Title II of this Book, and for the sole purpose of preventing terrorism, the collection in real time, on the networks of the operators and persons referred to in Article L. 851-1, of the information or documents referred to in that article relating to a person previously identified as potentially having links to a threat, may be individually authorised. Where there are substantial grounds for believing that one or more persons belonging to the circle of the person to whom the authorisation relates are capable of providing information in respect of the purpose for which the authorisation was granted, authorisation may also be granted individually for each of those persons.

I bis. The maximum number of authorisations issued under this article in force at the same time shall be determined by the Prime Minister following consultation of the Commission for the Oversight of Intelligence Techniques. The decision establishing that quota and how it is to be allocated between the ministers referred to in the first paragraph of Article L. 821-2, together with the number of interception authorisations issued, shall be forwarded to the Commission.

…'

43 Article L. 851-3 of the CSI provides:

'I. Under the conditions laid down in Chapter I of Title II of this Book, and for the sole purpose of preventing terrorism, the operators and persons referred to in Article L. 851-1 may be required to implement on their networks automated data processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat.

Such automated processing shall exclusively use the information or documents referred to in Article L. 851-1 and shall not collect any data other than data meeting the design parameters or allow the identification of the persons to whom the information or documents relate.

In accordance with the principle of proportionality, the authorisation of the Prime Minister shall specify the technical scope of the implementation of those processing practices.

II. The Commission for the Oversight of Intelligence Techniques shall issue an opinion on the application for authorisation for automated processing and the chosen detection parameters. It shall have permanent, complete and direct access to those processing practices and to the information and data collected. It shall be informed of any changes to the processing practices and parameters and may issue recommendations.

The first authorisation for the implementation of automated processing practices provided for in point I of this article shall be issued for a period of two months. The authorisation shall be renewable under the conditions on duration laid down in Chapter I of Title II of this Book. The application for renewal shall include a record of the number of identifiers flagged by the automated processing and an analysis of the relevance of that flagging.

III. The conditions laid down in Article L. 871-6 are applicable to the physical operations performed by the operators and persons referred to in Article L. 851-1 for the purpose of implementing such processing.

IV. Where the processing practices mentioned in point I of this article detect data likely to point to the existence of a terrorist threat, the Prime Minister or one of the persons delegated by him or her may – following consultation of the Commission for the Oversight of Intelligence Techniques under the conditions laid down in Chapter I of Title II of this Book – authorise the identification of the person or persons concerned and the collection of the related data. The data shall be used within 60 days of collection and shall be destroyed upon expiry of that period, unless there are substantial grounds confirming the existence of a terrorist threat associated with one or more of the persons concerned.

…'

44 Article L. 851-4 of the CSI reads as follows:

'Under the conditions laid down in Chapter I of Title II of this Book, technical data relating to the location of the terminal equipment used, as mentioned in Article L. 851-1, may be collected upon request from the network and transmitted in real time by the operators to a department reporting to the Prime Minister.'

45 Article R. 851-5 of the CSI, which appears in the regulatory part of that code, provides:

'I. The information or documents referred to in Article L. 851-1 are – excluding the content of the correspondence or the information consulted – as follows:

1. Those listed in Articles R. 10-13 and R. 10-14 of the [CPCE] and in Article 1 of Decree [No 2011-219];

2. Technical data other than the data mentioned in point 1:

(a) enabling terminal equipment to be located;

(b) relating to access by terminal equipment to online public communication networks or services;

(c) relating to the conveyance of electronic communications by networks;

(d) relating to the identification and authentication of a user, a connection, a network or an online public communication service;

(e) relating to the characteristics of terminal equipment and the configuration data of their software.

II. Only the information and documents referred to in point I(1) may be collected pursuant to Article L. 851-1. Such collection shall take place in non-real time.

The information listed in point I(2) may be collected only pursuant to Articles L. 851-2 and L. 851-3 under the conditions and within the limits laid down in those articles and subject to the application of Article R. 851-9.'

The CPCE

46 Article L. 34-1 of the CPCE states:

'I. This article shall apply to the processing of personal data in the course of the provision to the

public of electronic communications services; it shall apply in particular to networks that support data collection and identification devices.

II. Electronic communications operators, in particular persons whose business is to provide access to online public communication services, shall erase or render anonymous any data relating to traffic, subject to the provisions contained in points III, IV, V and VI.

Persons who provide electronic communications services to the public shall, with due regard for the provisions contained in the preceding paragraph, establish internal procedures for responding to requests from the competent authorities.

Persons who, as a principal or ancillary business activity, provide to the public a connection allowing online communication via access to the network shall, including where this is offered free of charge, be subject to compliance with the provisions applicable to electronic communications operators under this article.

III. For the purposes of investigating, detecting and prosecuting criminal offences or a failure to fulfil an obligation laid down in Article L. 336-3 of the code de la propriété intellectuelle (Intellectual Property Code) or for the purposes of preventing breaches of automated data processing systems as provided for and punishable under Articles 323-1 to 323-3-1 of the Code pénal (Criminal Code), and for the sole purpose of making information available, as necessary, to the judicial authority or high authority mentioned in Article L. 331-12 of the Intellectual Property Code or to the national authority for the security of information systems mentioned in Article L. 2321-1 of the code de la défense (Defence Code), operations designed to erase or render anonymous certain categories of technical data may be deferred for a maximum period of one year. A decree adopted in the Conseil d'État (Council of State, France) following consultation of the Data Protection Authority shall, within the limits laid down in point VI, determine the categories of data involved and the period for which they are to be retained, depending on the business of the operators, the nature of the communications and the methods of offsetting any identifiable and specific additional costs associated with the services provided for these purposes by operators at the request of the State.

…

VI. Data retained and processed under the conditions set out in points III, IV and V shall relate exclusively to the identification of persons using the services provided by operators, the technical characteristics of the communications provided by the latter and the location of terminal equipment.

Under no circumstance may such data relate to the content of the correspondence or the information consulted, in any form whatsoever, as part of those communications.

The retention and processing of such data shall be effected with due regard for the provisions of loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Law No 78-17 of 6 January 1978 on information technology, files and freedoms).

Operators shall take any measures necessary to prevent such data from being used for purposes other than those provided for in this article.'

47 Article R. 10-13 of the CPCE reads as follows:

'I. Pursuant to point III of Article L. 34-1, electronic communications operators shall retain the following data for the purposes of investigating, detecting and prosecuting criminal offences:

(a) Information identifying the user;

(b) Data relating to the communications terminal equipment used;

(c) The technical characteristics and date, time and duration of each communication;

(d) Data relating to the additional services requested or used and the providers of those services;

(e) Data identifying the addressee or addressees of the communication.

II. In the case of telephony activities, the operator shall retain the data referred to in point II and, additionally, data enabling the origin and location of the communication to be identified.

III. The data referred to in this article shall be retained for one year from the date of registration.

IV. Identifiable and specific additional costs borne by operators which have been ordered by judicial authorities to provide data falling within the categories mentioned in this article shall be offset in accordance with the methods laid down in Article R. 213-1 of the code de procédure pénale (Code of Criminal Procedure).'

48 Article R. 10-14 of the CPCE provides:

'I. Pursuant to point IV of Article L. 34-1, electronic communications operators are authorised to retain technical data identifying the user and the data mentioned in Article R. 10-13(I)(b), (c) and (d) for the purposes of their billing and payment operations.

II. In the case of telephony activities, operators may retain, in addition to the data mentioned in point I, technical data relating to the location of the communication and the identification of the addressee or addressees of the communication and data for billing purposes.

III. The data mentioned in points I and II of this article may be retained only if it is necessary for billing purposes and for the payment of services rendered. Its retention shall be limited to the time strictly necessary for that purpose and shall not exceed one year.

IV. Operators may retain the following data for a period not exceeding three months to ensure the security of networks and facilities:

(a) Data identifying the origin of the communication;

(b) The technical characteristics and date, time and duration of each communication;

(c) Technical data identifying the addressee or addressees of the communication;

(d) Data relating to the additional services requested or used and the providers of those services.'

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy)

49 Article 6 of Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law No 2004-575 of 21 June 2004 to promote trust in the digital economy) (JORF of 22 June 2004, p. 11168; 'the LCEN') provides:

'I. 1. Persons whose business is to provide access to online public communication services shall inform their subscribers of the existence of technical tools enabling access to some services to be restricted or for a selection of those services to be made and shall offer them at least one of those tools.

…

2. Natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind

provided by recipients of those services, may not incur any civil liability for the activities or information stored at the request of a recipient of those services if they had no actual knowledge of either the unlawful nature of the activities or information in question or of the facts and circumstances pointing to their unlawful nature, or if, as soon as they became aware of that unlawful nature, they acted expeditiously to remove the data at issue or block access to them.

…

II. The persons referred to in point I(1) and (2) shall keep and retain the data in such a way as to make it possible to identify anyone who has assisted in the creation of all or part of the content of the services of which they are the providers.

They shall provide persons who publish an online public communication service with technical tools enabling them to satisfy the identification conditions laid down in point III.

A judicial authority may require the service providers mentioned in point I(1) and (2) to communicate the data referred to in the first paragraph.

The provisions of Articles 226-17, 226-21 and 226-22 of the Criminal Code shall apply to the processing of that data.

A decree adopted in the Conseil d'État (Council of State, France) following consultation of the Data Protection Authority shall define the data referred to in the first paragraph and determine the period for which, and the methods by which, that data is to be retained.

…'

Decree No 2011-219

50 Chapter I of Decree No 2011-219, adopted on the basis of the last paragraph of Article 6(II) of the LCEN, contains Articles 1 to 4 of that decree.

51 Article 1 of Decree No 2011-219 provides:

'The following data is the data referred to in Article 6(II) of the [LCEN], which persons are required to retain under that provision:

1. For the persons referred to in point I(1) of that article and for each connection of their subscribers:

(a) The connection identifier;

(b) The identifier assigned by those persons to the subscriber;

(c) The identifier of the terminal used for the connection when they have access to it;

(d) The date and time of the start and end of the connection;

(e) The characteristics of the subscriber's line.

2. For the persons referred to in point I(2) of that article and for each creation operation:

(a) The identifier of the connection giving rise to the communication;

(b) The identifier assigned by the information system to the content forming the subject of the operation;

(c) The types of protocols used to connect to the service and transfer the content;

(d) The nature of the operation;

(e) The date and time of the operation;

(f) The identifier used by the author of the operation where provided by the author.

3. For the persons referred to in point I(1) and (2) of that article, the information provided by a user when signing up to a contract or creating an account:

(a) The identifier of the connection at the time when the account was created;

(b) The first name and surname or business name;

(c) The associated postal addresses;

(d) The pseudonyms used;

(e) The associated email or account addresses;

(f) The telephone numbers;

(g) The updated password and the data for verifying or changing it.

4. For the persons referred to in point I(1) and (2) of that article, where the signing up to the contract or the account is subject to payment, the following information relating to the payment, for each payment operation:

(a) The type of payment used;

(b) The payment reference;

(c) The amount;

(d) The date and time of the transaction.

The data mentioned in points 3 and 4 shall be retained only to the extent that the persons ordinarily collect such data.'

52 Article 2 of that decree reads as follows:

'Contributing to the creation of content involves the following operations:

(a) Initial content creation;

(b) Changes to content and content-related data;

(c) Content erasure.'

53 Article 3 of that decree provides:

'The data referred to in Article 1 shall be retained for one year from the date of:

(a) creation of the content, for each operation contributing to the creation of content as defined in Article 2, as regards the data mentioned in points 1 and 2;

(b) termination of the contract or closure of the account, as regards the data mentioned in

point 3;

(c) issue of the bill or the payment operation, for each bill or payment operation, as regards the data mentioned in point 4.'

Belgian law

54 The Law of 29 May 2016 amended, in particular, the loi du 13 juin 2005 relative aux communications électroniques (Law of 13 June 2005 on electronic communications) (*Moniteur belge* of 20 June 2005, p. 28070; 'the Law of 13 June 2005'), the code d'instruction criminelle (Code of Criminal Procedure) and the loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Basic Law of 30 November 1998 on the intelligence and security services) (*Moniteur belge* of 18 December 1998, p. 40312; 'the Law of 30 November 1998').

55 Article 126 of the Law of 13 June 2005, as amended by the Law of 29 May 2016, provides:

'1. Without prejudice to the Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Law of 8 December 1992 on the protection of privacy with respect to the processing of personal data), providers to the public of telephony services, including via the Internet, Internet access and Internet-based email, operators providing public electronic communications networks and operators providing any of those services shall retain the data referred to in paragraph 3 where that data is generated or processed by them in the course of providing the communications services concerned.

This article shall not concern the content of communications.

The obligation to retain the data referred to in paragraph 3 shall also apply to unsuccessful call attempts, provided that that data is, in the course of providing the communications services concerned:

(1) generated or processed by operators of publicly available electronic communications services or of a public electronic communications network, so far as concerns telephony data, or

(2) logged by those providers, so far as concerns Internet data.

2. Data retained under this article may be obtained, by simple request, from the providers and operators referred to in the first subparagraph of paragraph 1, for the purposes and under the conditions listed below, only by the following authorities:

(1) judicial authorities, with a view to the investigation, detection and prosecution of offences, in order to execute the measures referred to in Articles 46bis and 88bis of the Code of Criminal Procedure and under the conditions laid down in those articles;

(2) under the conditions laid down in this law, intelligence and security services, in order to carry out intelligence missions employing the data-gathering methods referred to in Articles 16/2, 18/7 and 18/8 of the Basic Law of 30 November 1998 on the intelligence and security services;

(3) any judicial police officer attached to the [Institut belge des services postaux et des télécommunications (Belgian Institute for Postal Services and Telecommunications)], with a view to the investigation, detection and prosecution of offences contrary to Articles 114 and 124 and this article;

(4) emergency services providing on-site assistance, in the case where, after having received an emergency call, they cannot obtain from the provider or operator concerned the data identifying the person having made the emergency call using the database referred to in the third subparagraph of Article 107(2), or obtain incomplete or incorrect data. Only the data identifying the caller may be

requested and the request must be made no later than 24 hours after the call;

(5) any judicial police officer attached to the Missing Persons Unit of the Federal Police, in the course of his or her task of providing assistance to persons in danger, searching for persons whose disappearance is a cause for concern and in cases where there are serious presumptions or indications that the physical well-being of the missing person is in imminent danger. Only the data referred to in the first and second subparagraphs of paragraph 3, relating to the missing person, and retained during the 48 hours prior to the data request, may be requested from the operator or provider concerned via a police service designated by the King;

(6) the Telecommunications Ombudsman, with a view to identifying a person who has misused an electronic communications network or service, in accordance with the conditions laid down in Article 43bis(3)(7) of the loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (Law of 21 March 1991 on the reform of certain public commercial undertakings). Only the identification data may be requested.

The providers and operators referred to in the first subparagraph of paragraph 1 shall ensure that the data referred to in paragraph 3 are accessible without restriction from Belgium and that that data and any other necessary information concerning that data may be transmitted without delay and only to the authorities referred to in this paragraph.

Without prejudice to other legal provisions, the providers and operators referred to in the first subparagraph of paragraph 1 may not use the data retained under paragraph 3 for any other purposes.

3. Data that can be used to identify the user or subscriber and the means of communication, other than the data specifically provided for in the second and third subparagraphs, shall be retained for 12 months as from the date on which communication was last able to be made using the service employed.

Data relating to the terminal devices' access and connection to the network and the service, and to the location of those devices, including the network termination point, shall be retained for 12 months as from the date of the communication.

Communication data other than content, including the origin and destination thereof, shall be retained for 12 months as from the date of the communication.

The King shall, by decree deliberated in the Council of Ministers and on a proposal from the Minister for Justice and the Minister [with responsibility for matters relating to electronic communications], and after obtaining the opinion of the Committee for the Protection of Privacy and the Institute, determine the data to be retained by category type as referred to in the first to third subparagraphs and the requirements which that data must satisfy.

…'

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

Case C-511/18

56 By applications lodged on 30 November 2015 and 16 March 2016, joined in the main proceedings, La Quadrature du Net, French Data Network, the Fédération des fournisseurs d'accès à Internet associatifs and Igwan.net brought actions before the Conseil d'État (Council of State, France) for the annulment of Decrees No 2015-1185, No 2015-1211, No 2015-1639 and No 2016-67, on the ground, inter alia, that they infringe the French Constitution, the European Convention for the Protection of Human Rights and Fundamental Freedoms ('the ECHR') and Directives 2000/31 and

2002/58, read in the light of Articles 7, 8 and 47 of the Charter.

57 As regards, in particular, the pleas alleging infringement of Directive 2000/31, the referring court states that the provisions of Article L. 851-3 of the CSI require electronic communications operators and technical service providers to 'implement on their networks automated data processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat'. That technique is intended only to facilitate the collection, for a limited period and from all of the connection data processed by those operators and service providers, of such data as might be related to a serious offence of this kind. In those circumstances, those provisions, which do not impose a general obligation of active surveillance, do not, in the view of the referring court, infringe Article 15 of Directive 2000/31.

58 As regards the pleas alleging infringement of Directive 2002/58, the referring court considers that it follows, inter alia, from the provisions of that directive and from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970; '*Tele2*'), that national provisions imposing obligations on providers of electronic communications services, such as the general and indiscriminate retention of the traffic and location data of their users and subscribers, for the purposes stated in Article 15(1) of that directive, which include safeguarding national security, defence and public security, fall within the scope of that directive since those rules govern the activity of those providers. That also applies to rules governing access to and use of data by national authorities.

59 The referring court concludes from this that both the obligation to retain data resulting from Article L. 851-1 of the CSI and the access of the administrative authorities to that data, including real-time access, provided for in Articles L. 851-1, L. 851-2 and L. 851-4 of that code, fall within the scope of Directive 2002/58. The same is true, according to that court, of the provisions of Article L. 851-3 of the CSI, which, although they do not impose a general retention obligation on the operators concerned, do however require them to implement automated processing on their networks that is intended to detect links that might constitute a terrorist threat.

60 On the other hand, the referring court takes the view that the scope of Directive 2002/58 does not extend to the provisions of the CSI referred to in the applications for annulment which relate to intelligence gathering techniques applied directly by the State, but do not regulate the activities of providers of electronic communications services by imposing specific obligations on them. Accordingly, those provisions cannot be regarded as implementing EU law, with the result that the pleas alleging that they infringe Directive 2002/58 cannot validly be relied on.

61 Thus, with a view to settling the disputes concerning the lawfulness of Decrees No 2015-1185, No 2015-1211, No 2015-1639 and No 2016-67 in the light of Directive 2002/58, in so far as they were adopted to implement Articles L. 851-1 to L. 851-4 of the CSI, three questions on the interpretation of EU law arise.

62 As regards the interpretation of Article 15(1) of Directive 2002/58, the referring court is uncertain, in the first place, whether a general and indiscriminate retention obligation, imposed on providers of electronic communications services on the basis of Articles L. 851-1 and R. 851-5 of the CSI, is to be regarded in the light, inter alia, of the safeguards and checks to which the access of the administrative authorities to and the use of connection data are subject, as interference justified by the right to security guaranteed in Article 6 of the Charter and by the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 TEU.

63 As regards, in the second place, the other obligations which may be imposed on providers of electronic communications services, the referring court states that the provisions of Article L. 851-2 of the CSI permit, for the sole purpose of preventing terrorism, the collection of the information or documents referred to in Article L. 851-1 of that code from the same persons. Such collection, in relation solely to one or more individuals previously identified as potentially having links to a

terrorist threat, is to be carried out in real time. The same is true of the provisions of Article L. 851-4, which authorise the real-time transmission by operators exclusively of technical data relating to the location of terminal equipment. Those techniques regulate the real-time access of the administrative authorities to data retained under the CPCE and the LCEN for various purposes and by various means, without, however, imposing on the providers concerned any additional retention requirement over and above what is necessary for the billing and provision of their services. In the same vein, nor do the provisions of Article L. 851-3 of the CSI, which require service providers to implement on their networks an automated system for the analysis of connections, entail general and indiscriminate retention.

64 The referring court considers that both general and indiscriminate retention and real-time access to connection data are of unparalleled operational usefulness, against a background of serious and persistent threats to national security, in particular the terrorist threat. General and indiscriminate retention allows the intelligence services to obtain access to communications data before the reasons for believing that the person concerned poses a threat to public security, defence or State security are identified. In addition, real-time access to connection data makes it possible to monitor, with a high level of responsiveness, the conduct of individuals who may pose an immediate threat to public order.

65 Furthermore, the technique provided for in Article L. 851-3 of the CSI makes it possible to detect, on the basis of criteria specifically defined for that purpose, those individuals whose conduct may, in view of their methods of communication, constitute a terrorist threat.

66 In the third place, as regards access by the competent authorities to retained data, the referring court is unsure whether Directive 2002/58, read in the light of the Charter, is to be interpreted as meaning that it is a prerequisite for the lawfulness of the procedures for the collection of connection data that the data subjects are informed whenever their being so informed is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or whether such procedures may be regarded as lawful taking into account all the other procedural safeguards provided for in national law where those safeguards ensure that the right to a remedy is effective.

67 As regards those other procedural safeguards, the referring court states in particular that any person wishing to verify that no intelligence techniques have been unlawfully implemented against him or her may bring the matter before a specialist panel of the Conseil d'État (Council of State, France), which is responsible for determining – in the light of the information communicated to it outside *inter partes* proceedings – whether the applicant has been the subject of an intelligence technique and whether that technique was implemented in accordance with Book VIII of the CSI. The powers conferred on that panel to investigate applications ensure that the judicial review conducted by it is effective. Thus, it has jurisdiction to investigate applications, to raise of its own motion any illegalities it may find and to order the authorities to take all appropriate measures to remedy the illegalities found. In addition, it is for the Commission for the Oversight of Intelligence Techniques to check that intelligence gathering techniques are implemented, on national territory, in accordance with the requirements flowing from the CSI. Thus, the fact that the legislative provisions at issue in the main proceedings do not provide for the notification to the persons concerned of the surveillance measures applied to them does not, in itself, constitute excessive interference with the right to respect for private life.

68 It is on that basis that the Conseil d'État (Council of State, France) decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'(1) Is the general and indiscriminate retention obligation imposed on providers on the basis of the implementing provisions of Article 15(1) of [Directive 2002/58] to be regarded, against a background of serious and persistent threats to national security, and in particular the terrorist threat, as interference justified by the right to security guaranteed in Article 6 of the [Charter] and the requirements of national security, responsibility for which falls to the Member States

alone pursuant to Article 4 [TEU]?

(2) Is [Directive 2002/58], read in the light of the [Charter], to be interpreted as authorising legislative measures, such as the measures for the real-time collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?

(3) Is [Directive 2002/58], read in the light of the [Charter], to be interpreted as meaning that it is a prerequisite for the lawfulness of the procedures for the collection of connection data that the data subjects are informed whenever their being so informed is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural safeguards where those safeguards ensure that the right to a remedy is effective?'

Case C-512/18

69 By application lodged on 1 September 2015, French Data Network, La Quadrature du Net and the Fédération des fournisseurs d'accès à Internet associatifs brought an action before the Conseil d'État (Council of State, France) for the annulment of the implied rejection decision arising from the Prime Minister's failure to reply to their application for the repeal of Article R. 10-13 of the CPCE and Decree No 2011-219, on the ground, inter alia, that those legislative texts infringe Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter. Privacy International and the Center for Democracy and Technology were granted leave to intervene in the main proceedings.

70 As regards Article R. 10-13 of the CPCE and the obligation of general and indiscriminate retention of communications data laid down therein, the referring court, which raises similar considerations to those in Case C-511/18, observes that such retention allows a judicial authority to access data relating to communications made by an individual before being suspected of having committed a criminal offence, with the result that such retention is of unparalleled usefulness for the investigation, detection and prosecution of criminal offences.

71 As regards Decree No 2011-219, the referring court considers that Article 6(II) of the LCEN, which imposes an obligation to hold and retain only data relating to the creation of content, does not fall within the scope of Directive 2002/58 since that directive's scope is limited, in accordance with Article 3(1) thereof, to the provision of publicly available electronic communications services in public communications networks in the European Union. On the other hand, that national provision does fall within the scope of Directive 2000/31.

72 The referring court considers, however, that it follows from Article 15(1) and (2) of Directive 2000/31 that the directive does not establish a prohibition in principle on retaining data relating to the creation of content, from which derogation would be possible only by way of exception. Thus, the question arises whether Articles 12, 14 and 15 of Directive 2000/31, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter, are to be interpreted as allowing a Member State to introduce national legislation, such as Article 6(II) of the LCEN, which requires the persons concerned to retain data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that a judicial authority may, where appropriate, require the communication of that data with a view to ensuring compliance with the rules on civil and criminal liability.

73 It is on that basis that the Conseil d'État (Council of State, France) decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'(1) Is the general and indiscriminate retention obligation imposed on providers on the basis of the implementing provisions of Article 15(1) of [Directive 2002/58] to be regarded, inter alia

in the light of the safeguards and checks to which the collection and use of such connection data are then subject, as interference justified by the right to security guaranteed in Article 6 of the [Charter] and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 [TEU]?

(2) Are the provisions of [Directive 2000/31], read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the [Charter], to be interpreted as allowing a State to introduce national legislation requiring the persons, whose activity consists in offering access to online public communications services and the natural or legal persons who, even free of charge, and for provision to the public via online public communications services, store signals, writing, images, sounds or messages of any kind provided by recipients of those services, to retain the data capable of enabling the identification of anyone who has contributed to the creation of the content or some of the content of the services which they provide, so that a judicial authority may, where appropriate, require the communication of that data with a view to ensuring compliance with the rules on civil and criminal liability?'

Case C-520/18

74 By applications lodged on 10, 16, 17 and 18 January 2017, joined in the main proceedings, the Ordre des barreaux francophones et germanophone, the Académie Fiscale ASBL and UA, the Liga voor Mensenrechten ASBL, the Ligue des Droits de l'Homme ASBL, and VZ, WY and XX brought actions before the Cour constitutionnelle (Constitutional Court, Belgium) for the annulment of the Law of 29 May 2016, on the ground that it infringes Articles 10 and 11 of the Belgian Constitution, read in conjunction with Articles 5, 6 to 11, 14, 15, 17 and 18 of the ECHR, Articles 7, 8, 11 and 47 and Article 52(1) of the Charter, Article 17 of the International Covenant on Civil and Political Rights, which was adopted by the United Nations General Assembly on 16 December 1966 and entered into force on 23 March 1976, the general principles of legal certainty, proportionality and self-determination in relation to information and Article 5(4) TEU.

75 In support of their actions, the applicants in the main proceedings submit, in essence, that the Law of 29 May 2016 is unlawful because, among other things, it goes beyond what is strictly necessary and does not lay down adequate guarantees of protection. In particular, neither its provisions relating to the retention of data nor those governing access by the authorities to retained data satisfy the requirements deriving from the judgments of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238; '*Digital Rights*') and of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970). They contend that those provisions entail a risk that personality profiles will be compiled, which may be misused by the competent authorities, and that they do not establish an appropriate level of security and protection for the retained data. Lastly, that law covers persons who are bound by professional secrecy and persons who are under a duty of confidentiality, and applies to personal communication data that is sensitive, without including specific safeguards to protect such data.

76 The referring court observes that the data which must be retained by providers of telephony services, including via the Internet, Internet access and Internet-based email and by operators providing public electronic communications networks, under the Law of 29 May 2016, is identical to that listed in 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), without any distinction being made as regards the persons concerned or on the basis of the objective pursued. As regards the latter point, the referring court states that the objective pursued by the legislature by means of that law is not only to combat terrorism and child pornography, but also to enable the use of the retained data in a wide variety of situations in the context of criminal investigations. The referring court also notes that it is apparent from the explanatory memorandum for that law that the national legislature considered it impossible, in the light of the objective pursued, to impose a targeted and selective obligation to

retain data, and that it chose to apply strict guarantees to the general and indiscriminate retention obligation, both as regards the data retained and access to that data, in order to keep interference with the right to respect for private life to a minimum.

77 The referring court also states that subparagraphs 1 and 2 of Article 126(2) of the Law of 13 June 2005, as amended by the Law of 29 May 2016, lay down the conditions under which, respectively, judicial authorities and the intelligence and security services may obtain access to retained data, and consequently the review of the lawfulness of that law in the light of the requirements of EU law should be deferred until the Court has adjudicated on two preliminary ruling procedures pending before it concerning such access.

78 Lastly, the referring court states that the Law of 29 May 2016 seeks to ensure an effective criminal investigation and effective penalties in cases involving the sexual abuse of minors and to make it possible to identify the perpetrator of such an offence, even where electronic communications systems are used. In the proceedings before it, attention was drawn in that respect to the positive obligations under Articles 3 and 8 of the ECHR. Those obligations may also arise under the corresponding provisions of the Charter, which may have consequences for the interpretation of Article 15(1) of Directive 2002/58.

79 It is on that basis that the Cour constitutionnelle (Constitutional Court, Belgium) decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

‘(1) Must Article 15(1) of [Directive 2002/58], read in conjunction with the right to security, guaranteed by Article 6 of the [Charter], and the right to respect for personal data, as guaranteed by Articles 7, 8 and 52(1) of the [Charter], be interpreted as precluding national legislation such as that at issue, which lays down a general obligation for operators and providers of electronic communications services to retain the traffic and location data within the meaning of [Directive 2002/58], generated or processed by them in the context of the supply of those services, national legislation whose objective is not only the investigation, detection and prosecution of serious criminal offences but also the safeguarding of national security, the defence of the territory and of public security, the investigation, detection and prosecution of offences other than serious crime or the prevention of the prohibited use of electronic communication systems, or the attainment of another objective identified by Article 23(1) of [Regulation 2016/679] and which, furthermore, is subject to specific safeguards in that legislation in terms of data retention and access to that data?

(2) Must Article 15(1) of [Directive 2002/58], in conjunction with Articles 4, 7, 8, 11 and 52(1) of the [Charter], be interpreted as precluding national legislation such as that at issue, which lays down a general obligation for operators and providers of electronic communications services to retain the traffic and location data within the meaning of [Directive 2002/58], generated or processed by them in the context of the supply of those services, if the object of that legislation is, in particular, to comply with the positive obligations borne by the authority under Articles 4 and [7] of the Charter, consisting in the provision of a legal framework which allows the effective criminal investigation and the effective punishment of sexual abuse of minors and which permits the effective identification of the perpetrator of the offence, even where electronic communications systems are used?

(3) If, on the basis of the answer to the first or the second question, the Cour constitutionnelle (Constitutional Court, Belgium) should conclude that the contested law fails to fulfil one or more obligations arising under the provisions referred to in these questions, might it maintain on a temporary basis the effects of [the Law of 29 May 2016] in order to avoid legal uncertainty and to enable the data previously collected and retained to continue to be used for the objectives pursued by the law?’

Procedure before the Court

80 By decision of the President of the Court of 25 September 2018, Cases C-511/18 and C-512/18 were joined for the purposes of the written and oral parts of the procedure and the judgment. Case C-520/18 was joined to those cases by decision of the President of the Court of 9 July 2020 for the purposes of the judgment.

Consideration of the questions referred

Question 1 in Cases C-511/18 and C-512/18 and questions 1 and 2 in Case C-520/18

81 By question 1 in Cases C-511/18 and C-512/18 and questions 1 and 2 in Case C-520/18, which should be considered together, the referring courts essentially ask whether Article 15(1) of Directive 2002/58 must be interpreted as precluding national legislation which imposes on providers of electronic communications services, for the purposes set out in Article 15(1), an obligation requiring the general and indiscriminate retention of traffic and location data.

Preliminary remarks

82 It is apparent from the documents available to the Court that the legislation at issue in the main proceedings covers all electronic communications systems and applies to all users of such systems, without distinction or exception. Furthermore, the data which must be retained by providers of electronic communications services under that legislation is, in particular, the data necessary for locating the source of a communication and its destination, for determining the date, time, duration and type of communication, for identifying the communications equipment used, and for locating the terminal equipment and communications, data which comprises, inter alia, the name and address of the user, the telephone numbers of the caller and the person called, and the IP address for Internet services. By contrast, that data does not cover the content of the communications concerned.

83 Thus, the data which must, under the national legislation at issue in the main proceedings, be retained for a period of one year makes it possible, inter alia, to identify the person with whom the user of an electronic communications system has communicated and by what means, to determine the date, time and duration of the communications and Internet connections and the place from which those communications and connections took place, and to ascertain the location of the terminal equipment without any communication necessarily having been transmitted. In addition, that data enables the frequency of a user's communications with certain persons over a given period of time to be established. Last, as regards the national legislation at issue in Cases C-511/18 and C-512/18, it appears that that legislation, in so far as it also covers data relating to the conveyance of electronic communications by networks, also enables the nature of the information consulted online to be identified.

84 As for the aims pursued, it should be noted that the legislation at issue in Cases C-511/18 and C-512/18 pursues, among other aims, the investigation, detection and prosecution of criminal offences in general; national independence, territorial integrity and national defence; major foreign policy interests; the implementation of France's European and international commitments; France's major economic, industrial and scientific interests; and the prevention of terrorism, attacks against the republican nature of the institutions and collective violence liable to cause serious disruption to the maintenance of law and order. The objectives of the legislation at issue in Case C-520/18 are, inter alia, the investigation, detection and prosecution of criminal offences and the safeguarding of national security, the defence of the territory and public security.

85 The referring courts are uncertain, in particular, as to the possible impact of the right to security enshrined in Article 6 of the Charter on the interpretation of Article 15(1) of Directive 2002/58. Similarly, they ask whether the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter entailed by the retention of data provided for in the legislation at issue in the main proceedings may, in the light of the existence of rules restricting national authorities' access to retained data, be regarded as justified. In addition, according to the Conseil d'État (Council of State,

France), since that question arises in a context characterised by serious and persistent threats to national security, it should also be assessed in the light of Article 4(2) TEU. The Cour constitutionnelle (Constitutional Court, Belgium), for its part, points out that the national legislation at issue in Case C-520/18 also implements positive obligations flowing from Articles 4 and 7 of the Charter, consisting in the establishment of a legal framework for the effective prevention and punishment of the sexual abuse of minors.

86 While both the Conseil d'État (Council of State, France) and the Cour constitutionnelle (Constitutional Court, Belgium) start from the premiss that the respective national legislation at issue in the main proceedings, which governs the retention of traffic and location data and access to that data by national authorities for the purposes set out in Article 15(1) of Directive 2002/58, such as safeguarding national security, falls within the scope of that directive, a number of parties to the main proceedings and some of the Member States which submitted written observations to the Court disagree on that point, particularly concerning the interpretation of Article 1(3) of that directive. It is therefore necessary to examine, first of all, whether the legislation at issue falls within the scope of that directive.

Scope of Directive 2002/58

87 La Quadrature du Net, the Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International and the Center for Democracy and Technology rely on the Court's case-law on the scope of Directive 2002/58 to argue, in essence, that both the retention of data and access to retained data fall within that scope, whether that access takes place in non-real time or in real time. Indeed, they contend that since the objective of safeguarding national security is expressly mentioned in Article 15(1) of that directive, the pursuit of that objective does not render that directive inapplicable. In their view, Article 4(2) TEU, mentioned by the referring courts, does not affect that assessment.

88 As regards the intelligence measures implemented directly by the competent French authorities, without regulating the activities of providers of electronic communications services by imposing specific obligations on them, the Center for Democracy and Technology observes that those measures necessarily fall within the scope of Directive 2002/58 and of the Charter, since they are exceptions to the principle of confidentiality guaranteed in Article 5 of that directive. Those measures must therefore comply with the requirements stemming from Article 15(1) of the directive.

89 On the other hand, the Czech and Estonian Governments, Ireland, and the French, Cypriot, Hungarian, Polish, Swedish and United Kingdom Governments submit, in essence, that Directive 2002/58 does not apply to national legislation such as that at issue in the main proceedings, since the purpose of that legislation is to safeguard national security. The intelligence services' activities, in so far as they relate to the maintenance of public order and to the safeguarding of internal security and territorial integrity, are part of the essential functions of the Member States and, consequently, are within their exclusive competence, as evidenced, in particular, by the third sentence of Article 4(2) TEU.

90 Those governments and Ireland also refer to Article 1(3) of Directive 2002/58, which excludes from the scope of that directive, as the first indent of Article 3(2) of Directive 95/46 did in the past, activities concerning public security, defence and State security. They rely in that regard on the interpretation of the latter provision set out in the judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346).

91 In that regard, it should be stated that, under Article 1(1) thereof, Directive 2002/58 provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications

sector.

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

93 In addition, Article 3 of Directive 2002/58 states that that directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices (‘electronic communications services’). Consequently, that directive must be regarded as regulating the activities of the providers of such services (judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 33 and the case-law cited).

94 In that context, Article 15(1) of Directive 2002/58 states that Member States may adopt, subject to the conditions laid down, ‘legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of [that directive]’ (judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 71).

95 Article 15(1) of Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, such measures regulate, for the purposes mentioned in that provision, the activity of providers of electronic communications services (judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 34 and the case-law cited).

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

97 In addition, having regard to the considerations set out in paragraph 95 above and the general scheme of Directive 2002/58, an interpretation of that directive under which the legislative measures referred to in Article 15(1) thereof were excluded from the scope of that directive because the objectives which such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of that same directive would deprive Article 15(1) thereof of any practical effect (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 72 and 73).

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

99 Article 4(2) TEU, to which the governments listed in paragraph 89 of the present judgment have made reference, cannot invalidate that conclusion. Indeed, according to the Court’s settled case-law,

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

100 It is true that, in the judgment of 30 May 2006, *Parliament* v *Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346, paragraphs 56 to 59), the Court held that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes did not, pursuant to the first indent of Article 3(2) of Directive 95/46, fall within the scope of that directive, because that transfer fell within a framework established by the public authorities relating to public security.

101 However, having regard to the considerations set out in paragraphs 93, 95 and 96 of the present judgment, that case-law cannot be transposed to the interpretation of Article 1(3) of Directive 2002/58. Indeed, as the Advocate General noted, in essence, in points 70 to 72 of his Opinion in Joined Cases *La Quadrature du Net and Others* (C-511/18 and C-512/18, EU:C:2020:6), the first indent of Article 3(2) of Directive 95/46, to which that case-law relates, excluded, in a general way, from the scope of that directive 'processing operations concerning public security, defence, [and] State security', without drawing any distinction according to who was carrying out the data processing operation concerned. By contrast, in the context of interpreting Article 1(3) of Directive 2002/58, it is necessary to draw such a distinction. As is apparent from paragraphs 94 to 97 of the present judgment, all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive, including processing operations resulting from obligations imposed on those providers by the public authorities, although those processing operations could, where appropriate, on the contrary, fall within the scope of the exception laid down in the first indent of Article 3(2) of Directive 95/46, given the broader wording of that provision, which covers all processing operations concerning public security, defence, or State security, regardless of the person carrying out those operations.

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

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

question must comply with, inter alia, national constitutional law and the requirements of the ECHR.

104 It follows from the foregoing considerations that national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, such as the legislation at issue in the main proceedings, falls within the scope of Directive 2002/58.

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

105 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 (see, to that effect, judgment of 17 April 2018, *Egenberger*, C-414/16, EU:C:2018:257, paragraph 44).

106 As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of Directive 2002/58 is to protect users of electronic communications services from risks for their personal data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, that directive seeks, as is stated in recital 2 thereof, to ensure that the rights set out in Articles 7 and 8 of the Charter are fully respected. In that regard, it is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM (2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to 'ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'.

107 To that end, 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 that data.

108 As regards, in particular, the processing and storage of traffic data by providers of electronic communications services, it is apparent from Article 6 and recitals 22 and 26 of Directive 2002/58 that such processing is permitted only to the extent necessary and for the time necessary for the marketing and billing of services and the provision of value added services. Once that period has elapsed, the data that has been processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers has been obtained (judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 86 and the case-law cited).

109 Thus, in adopting that directive, the EU legislature gave concrete expression to the rights enshrined in Articles 7 and 8 of the Charter, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise.

110 However, Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to, inter alia, in Articles 6 and 9 of that directive, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those

grounds.

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

112 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 (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 52 and the case-law cited).

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

114 Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 6 March 2001, *Connolly* v *Commission*, C-274/99 P, EU:C:2001:127, paragraph 39, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 93 and the case-law cited).

115 It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, on the one hand, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing that data, and, on the other, an interference with the fundamental rights to 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 or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited; see, by analogy, as regards Article 8 of the ECHR, ECtHR, 30 January 2020, *Breyer v. Germany*, CE:ECHR:2020:0130JUD005000112, § 81).

116 Whether or not the retained data has been used subsequently is also irrelevant (see, by analogy, as regards Article 8 of the ECHR, ECtHR, 16 February 2000, *Amann v. Switzerland*, CE:ECHR:2000:0216JUD002779895, § 69, and 13 February 2020, *Trajkovski and Chipovski v. North Macedonia*, CE:ECHR:2020:0213JUD005320513, § 51), since access to such data is a

separate interference with the fundamental rights referred to in the preceding paragraph, irrespective of the subsequent use made of it (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126).

117 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 enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has 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, that data provides 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 (see, to that effect, judgments of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 27, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 99).

118 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 (see, to that effect, judgments of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 28, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 101). Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistleblowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ 2019 L 305, p. 17). Moreover, that deterrent effect is all the more serious given the quantity and breadth of data retained.

119 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 that data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access.

120 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 110 above, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited).

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

122 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.

123 In that regard, Article 6 of the Charter, to which the Conseil d'État (Council of State, France) and the Cour constitutionnelle (Constitutional Court, Belgium) refer, lays down the right of every individual not only to liberty but also to security and guarantees rights corresponding to those

guaranteed in Article 5 of the ECHR (see, to that effect, judgments of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 47; of 28 July 2016, *JZ*, C-294/16 PPU, EU:C:2016:610, paragraph 48; and of 19 September 2019, *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, paragraph 42 and the case-law cited).

124 In addition, it should be recalled that Article 52(3) of the Charter is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union. Account must therefore be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection (see, to that effect, judgments of 12 February 2019, *TC*, C-492/18 PPU, EU:C:2019:108, paragraph 57, and of 21 May 2019, *Commission* v *Hungary (Rights of usufruct over agricultural land)*, C-235/17, EU:C:2019:432, paragraph 72 and the case-law cited).

125 Article 5 of the ECHR, which enshrines the 'right to liberty' and the 'right to security', is intended, according to the case-law of the European Court of Human Rights, to ensure that individuals are protected from arbitrary or unjustified deprivations of liberty (see, to that effect, ECtHR, 18 March 2008, *Ladent v. Poland*, CE:ECHR:2008:0318JUD001103603, §§ 45 and 46; 29 March 2010, *Medvedyev and Others v. France*, CE:ECHR:2010:0329JUD000339403, §§ 76 and 77; and 13 December 2012, *El-Masri v. 'The former Yugoslav Republic of Macedonia'*, CE:ECHR:2012:1213JUD003963009, § 239). However, since that provision applies to deprivations of liberty by a public authority, Article 6 of the Charter cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences.

126 On the other hand, as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, mentioned by the Cour constitutionnelle (Constitutional Court, Belgium), it should be pointed out 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 (see, to that effect, judgment of 18 June 2020, *Commission* v *Hungary (Transparency of associations)*, C-78/18, EU:C:2020:476, paragraph 123 and the case-law cited of the European Court of Human Rights). 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.

127 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.

128 The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the ECHR, 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 (ECtHR, 28 October 1998, *Osman v. United Kingdom*, CE:ECHR:1998:1028JUD002345294, §§ 115 and 116; 4 March 2004, *M.C. v. Bulgaria*, CE:ECHR:2003:1204JUD003927298, § 151; 24 June 2004, *Von Hannover v. Germany*, CE:ECHR:2004:0624JUD005932000, §§ 57 and 58; and 2 December 2008, *K.U. v. Finland*, CE:ECHR:2008:1202JUD000287202, §§ 46, 48 and 49).

129 Concerning observance of the principle of proportionality, the first sentence of Article 15(1) of

Directive 2002/58 provides that the Member States may adopt a measure derogating from the principle that communications and the related traffic data are to be confidential where such a measure is 'necessary, appropriate and proportionate … within a democratic society', in view of the objectives set out in that provision. Recital 11 of that directive specifies that a measure of that nature must be 'strictly' proportionate to the intended purpose.

130 In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (see, to that effect, judgments of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paragraph 56; of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 76, 77 and 86; and of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52; Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 140).

131 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 (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited).

132 In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 117; Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 141).

133 Thus, 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 (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 191 and the case-law cited, and judgment of 3 October 2019, *A and Others*, C-70/18, EU:C:2019:823, paragraph 63).

– *Legislative measures providing for the preventive retention of traffic and location data for the purpose of safeguarding national security*

134 It should be observed that the objective of safeguarding national security, mentioned by the referring courts and the governments which submitted observations, has not yet been specifically examined by the Court in its judgments interpreting Directive 2002/58.

135 In that regard, it should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the

primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.

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

137 Thus, in situations such as those described in paragraphs 135 and 136 of the present judgment, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, as referred to in paragraphs 135 and 136 of the present judgment, to national security which is shown to be genuine and present or foreseeable. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.

138 The instruction for the preventive retention of data of all users of electronic communications systems must, however, be limited in time to what is strictly necessary. Although it is conceivable that an instruction requiring providers of electronic communications services to retain data may, owing to the ongoing nature of such a threat, be renewed, the duration of each instruction cannot exceed a foreseeable period of time. Moreover, such data retention must be subject to limitations and must be circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons concerned against the risk of abuse. Thus, that retention cannot be systematic in nature.

139 In view of the seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter resulting from a measure involving the general and indiscriminate retention of data, it must be ensured that recourse to such a measure is in fact limited to situations in which there is a serious threat to national security as referred to in paragraphs 135 and 136 of the present judgment. For that purpose, it is essential that decisions giving an instruction to providers of electronic communications services to carry out such data retention be 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.

– *Legislative measures providing for the preventive retention of traffic and location data for the purposes of combating crime and safeguarding public security*

140 As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, 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, investigating, detecting and prosecuting criminal offences in general (see, to that effect, judgments of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 102, and of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 56 and 57; Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 149).

141 National legislation providing for the general and indiscriminate retention of traffic and location data for the purpose of combating serious crime exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 107).

142 In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of that data is essential for the right to respect for private life. Thus, having regard, first, to the deterrent effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 118 above, which is liable to result from the retention of that data, and, second, to 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 the data 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 to be attached to them.

143 In addition, the Court has emphasised that 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, in contrast to the requirement mentioned in paragraph 133 above, is comprehensive in that it affects all persons using electronic communications 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 (see, to that effect, judgments of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 and 58, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 105).

144 In particular, as the Court has previously 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 (see, to that effect, judgments of 8 April 2014, *Digital Rights*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 59, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 106).

145 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 relating, as pointed out in paragraphs 126 and 128 of the present 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, without there being a link, at least an indirect one, between the data of the persons concerned and the objective pursued.

146 By contrast, in accordance with what has been stated in paragraphs 142 to 144 of the present judgment, and having regard to the balance that must be struck between the rights and interests at issue, the objectives of combating serious crime, preventing serious attacks on public security and, a

fortiori, safeguarding national security are capable of justifying – given their importance, in the light of the positive obligations mentioned in the preceding paragraph to which the Cour constitutionnelle (Constitutional Court, Belgium), referred, inter alia – the particularly serious interference entailed by the targeted retention of traffic and location data.

147 Thus, as the Court has previously held, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data for the purposes of combating serious crime, preventing serious threats to public security and equally of safeguarding national security, provided that such retention is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 108).

148 As regards the limits to which such a data retention measure must be subject, these may, in particular, be determined according to the categories of persons concerned, since Article 15(1) of Directive 2002/58 does not preclude legislation based on objective evidence which makes it possible to target persons whose traffic and location data is 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 (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111).

149 In that regard, it must be made clear that 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 evidence, as posing a threat to public or national security in the Member State concerned.

150 The limits on a measure providing for the retention of traffic and location data may 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 (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111). Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.

151 In order to ensure that the interference entailed by the targeted retention measures described in paragraphs 147 to 150 of the present judgment complies with the principle of proportionality, their duration 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.

– *Legislative measures providing for the preventive retention of IP addresses and data relating to civil identity for the purposes of combating crime and safeguarding public security*

152 It should be noted that although IP addresses are part of traffic data, they are generated independently of any particular communication and mainly serve to identify, through providers of electronic communications services, the natural person who owns the terminal equipment from which an Internet communication is made. Thus, in relation to email and Internet telephony, provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient of the communication, those addresses do not, as such, disclose any information about third parties who were in contact with the person who made the communication. That category of data is therefore less sensitive than other traffic data.

153 However, since IP addresses may be used, among other things, to track an Internet user's complete clickstream and, therefore, his or her entire online activity, that data enables a detailed profile of the user to be produced. Thus, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the Internet user enshrined in Articles 7 and 8 of the Charter, which may have a deterrent effect as mentioned in paragraph 118 of the present judgment.

154 In order to strike a balance between the rights and interests at issue as required by the case-law cited in paragraph 130 of the present judgment, account must be taken of the fact that, where an offence is committed online, 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. To that consideration must be added the fact that the retention of IP addresses by providers of electronic communications services beyond the period for which that data is assigned does not, in principle, appear to be necessary for the purpose of billing the services at issue, with the result that the detection of offences committed online may therefore prove impossible without recourse to a legislative measure under Article 15(1) of Directive 2002/58, something which several governments mentioned in their observations to the Court. As those governments argued, that may occur, inter alia, in cases involving particularly serious child pornography offences, such as 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).

155 In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the Internet would catch persons who at first sight have no connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with the objectives pursued, and it is also true, in accordance with what has been stated in paragraph 109 of the present judgment, that Internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of that data.

156 In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of that data, particularly via tracking, with regard to communications made and activities carried out online by the persons concerned.

157 Concerning, last, data relating to the civil identity of users of electronic communications systems, that data does not, in itself, make it possible to ascertain the date, time, duration and recipients of the communications made, or the locations where those communications took place or their frequency with specific people during a given period, with the result that it does not provide, apart from the contact details of those users, such as their addresses, any information on the communications sent and, consequently, on the users' private lives. Thus, the interference entailed by the retention of that data cannot, in principle, be classified as serious (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 59 and 60).

158 It follows that, in accordance with what has been stated in paragraph 140 of the present judgment, legislative measures concerning the processing of that data as such, including the retention of and access to that data solely for the purpose of identifying the user concerned, and without it being

possible for that data to be associated with information on the communications made, are capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 62).

159 In those circumstances, having regard to the balance that must be struck between the rights and interests at issue, and for the reasons set out in paragraphs 131 and 158 of the present judgment, it must be held that, even in the absence of a connection between all users of electronic communications systems and the objectives pursued, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude a legislative measure which requires providers of electronic communications services, without imposing a specific time limit, to retain data relating to the civil identity of all users of electronic communications systems for the purposes of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security, there being no need for the criminal offences or the threats to or acts having adverse effects on public security to be serious.

– *Legislative measures providing for the expedited retention of traffic and location data for the purpose of combating serious crime*

160 With regard to 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, as described in paragraphs 134 to 159 of the present judgment, it should be noted that that data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which that data must be processed and stored in accordance with the national provisions transposing that directive.

161 However, during that processing and storage, situations may arise in which it becomes necessary to retain that 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.

162 In that regard, the Council of Europe's Convention on Cybercrime of 23 November 2001 (European Treaty Series – No. 185), which was signed by the 27 Member States and ratified by 25 of them and has as its objective to facilitate the fight against criminal offences committed using computer networks, provides, in Article 14, that the parties to the convention are to adopt, for the purpose of specific criminal investigations or proceedings, certain measures concerning traffic data already stored, such as the expedited preservation of that data. In particular, Article 16(1) of that convention stipulates that the parties to that convention are to adopt such legislative measures as may be necessary to enable their competent authorities to order or similarly obtain the expedited preservation of traffic data that has been stored by means of a computer system, in particular where there are grounds to believe that that data is particularly vulnerable to loss or modification.

163 In a situation such as the one described in paragraph 161 of the present judgment, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraph 130 of the present 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 which is 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.

164 To the extent that the purpose of such expedited retention no longer corresponds to the purpose for

which that data was 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 action to combat serious crime and, a fortiori, the safeguarding of national security are such as to justify such interference. Moreover, in order to ensure that the interference entailed by a measure of that kind is limited to what is strictly necessary, first, the retention obligation must relate only to traffic and location data that may shed light on the serious criminal offences or the acts adversely affecting national security concerned. Second, the duration for which such data is retained must be limited to what is strictly necessary, although that duration can be extended where the circumstances and the objective pursued by that measure justify doing so.

165 In that regard, such expedited retention need not be limited to the data of persons specifically suspected of having committed a criminal offence or acts adversely affecting national security. 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 133 above, such a measure may, at the choice of the 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 that 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, his or her social or professional circle, or even specified geographical areas, such as the place where the offence or act adversely affecting national security at issue was committed or prepared. Additionally, the competent authorities must be given access to the data thus retained in observance of the conditions that emerge from the case-law on how Directive 2002/58 is to be interpreted (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 118 to 121 and the case-law cited).

166 It should also be added that, as is clear, in particular, from paragraphs 115 and 133 above, access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58 may, in principle, be justified only by the public interest objective for which those providers were ordered to retain that data. It follows, in particular, that access to such data for the purpose of prosecuting and punishing an ordinary criminal offence may in no event be granted where the retention of such data has been justified by the objective of combating serious crime or, a fortiori, by the objective of safeguarding national security. However, in accordance with the principle of proportionality, as mentioned in paragraph 131 above, access to data retained for the purpose of combating serious crime may, provided that the substantive and procedural conditions associated with such access referred to in the previous paragraph are observed, be justified by the objective of safeguarding national security.

167 In that regard, it is permissible for Member States to specify in their legislation that access to traffic and location data may, subject to those same substantive and procedural conditions, be permitted for the purpose of combating serious crime or safeguarding national security where that data is retained by a provider in a manner that is consistent with Articles 5, 6 and 9 or Article 15(1) of Directive 2002/58.

168 In the light of all of the above considerations, the answer to question 1 in Cases C-511/18 and C-512/18 and questions 1 and 2 in Case C-520/18 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, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, 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:

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

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

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

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

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

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

Questions 2 and 3 in Case C-511/18

169 By questions 2 and 3 in Case C-511/18, 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 which requires providers of electronic communications services to implement, on their networks, measures allowing, first, the automated analysis and real-time collection of traffic and location data and, second, real-time collection of technical data concerning the location of the terminal equipment used, but which makes no provision for the persons concerned by that processing and that collection to be notified thereof.

170 The referring court notes that the intelligence gathering techniques provided for in Articles L. 851-2 to L. 851-4 of the CSI do not impose on providers of electronic communications services a specific obligation to retain traffic and location data. With regard, in particular, to the automated analysis referred to in Article L. 851-3 of the CSI, the referring court observes that the aim of that processing is to detect, according to criteria established for that purpose, links that might constitute a terrorist threat. As for the real-time collection referred to in Article L. 851-2 of the CSI, that court notes that such collection concerns exclusively one or more persons who have been identified in advance as potentially having a link to a terrorist threat. According to that same court, those two techniques may be implemented only with a view to preventing terrorism and cover the data referred to in Articles L. 851-1 and R. 851-5 of the CSI.

171 As a preliminary point, it should be noted that the fact that, according to Article L. 851-3 of the CSI, the automated analysis that it provides for does not, as such, allow the users whose data is being analysed to be identified, does not prevent such data from being classified as 'personal data'. Since the procedure provided for in point IV of that provision allows the person or persons concerned by the data, the automated analysis of which has shown that there may be a terrorist threat, to be identified at a later stage, all persons whose data has been the subject of automated analysis can still be identified from that data. According to the definition of personal data in Article 4(1) of Regulation 2016/679, information relating, inter alia, to an identifiable person constitutes personal data.

Automated analysis of traffic and location data

172 It is clear from Article L. 851-3 of the CSI that the automated analysis for which it provides corresponds, in essence, to a screening of all the traffic and location data retained by providers of electronic communications services, which is carried out by those providers at the request of the competent national authorities applying the parameters set by the latter. It follows that all data of users of electronic communications systems is verified if it corresponds to those parameters. Therefore, such automated analysis must be considered as involving, for the providers of electronic communications services concerned, the undertaking on behalf of the competent authority of general and indiscriminate processing, in the form of the use of that data with the assistance of an automated operation, within the meaning of Article 4(2) of Regulation 2016/679, covering all traffic and location data of all users of electronic communications systems. That processing is independent of the subsequent collection of data relating to the persons identified following that automated analysis, such collection being authorised on the basis of Article L. 851-3, IV, of the CSI.

173 National legislation authorising such automated analysis of traffic and location data derogates from the obligation of principle, established in Article 5 of Directive 2002/58, to ensure the confidentiality of electronic communications and related data. Such legislation also constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, regardless of how that data is used subsequently. Finally, as was stated in the case-law cited in paragraph 118 of the present judgment, such legislation is likely to have a deterrent effect on the exercise of freedom of expression, which is enshrined in Article 11 of the Charter.

174 Moreover, the interference resulting from the automated analysis of traffic and location data, such as that at issue in the main proceedings, is particularly serious since it covers, generally and indiscriminately, the data of persons using electronic communication systems. That finding is all the more justified given that, as is clear from the national legislation at issue in the main proceedings, the data that is the subject of the automated analysis is likely to reveal the nature of the information consulted online. In addition, such automated analysis is applied generally to all persons who use electronic communication systems and, consequently, applies also 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 terrorist activities.

175 With regard to the justification for such interference, the requirement, established in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits that interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).

176 In addition, in order to meet the requirement of proportionality recalled in paragraphs 130 and 131 of the present judgment, according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, national legislation governing the access of the competent authorities to retained traffic and location data must comply with the requirements that emerge from the case-law cited in paragraph 132 of the present judgment. In

particular, such legislation cannot be limited to requiring that the authorities' access to such data should correspond to the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (see, by analogy, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 192 and the case-law cited).

177 In that regard, it should be noted that the particularly serious interference that is constituted by the general and indiscriminate retention of traffic and location data, as referred to in the findings in paragraphs 134 to 139 of the present judgment, and the particularly serious interference constituted by the automated analysis of that data can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary.

178 In situations such as those referred to in the previous paragraph, the implementation of automated analysis of the traffic and location data of all users of electronic communications systems, for a strictly limited period, may be considered to be justified in the light of the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

179 That being said, in order to guarantee that such a measure is actually limited to what is strictly necessary in order to protect national security and, more particularly, to prevent terrorism, in accordance with what was held in paragraph 139 of the present judgment, it is essential that the decision authorising automated analysis be 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 a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed.

180 In that regard, it should be noted that the pre-established models and criteria on which that type of data processing are based should be, first, specific and reliable, making it possible to achieve results identifying individuals who might be under a reasonable suspicion of participation in terrorist offences and, second, should be non-discriminatory (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 172).

181 In addition, it must be noted that any automated analysis carried out on the basis of models and criteria founded on the premiss that racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person's health or sex life could, in themselves and regardless of the individual conduct of that person, be relevant in order to prevent terrorism would infringe the rights guaranteed in Articles 7 and 8 of the Charter, read in conjunction with Article 21 thereof. Therefore, pre-established models and criteria for the purposes of an automated analysis that has as its objective the prevention of terrorist activities that constitute a serious threat to national security cannot be based on that sensitive data in isolation (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 165).

182 Furthermore, since the automated analyses of traffic and location data necessarily involve some margin of error, any positive result obtained following automated processing must be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the persons concerned is adopted, such as the subsequent real-time collection of traffic and location data, since such a measure cannot be based solely and decisively on the result of automated processing. Similarly, in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary in the light of the objective of preventing terrorist activities that constitute a serious threat to national security, a regular re-examination should be undertaken to ensure that those pre-established models and criteria and the databases used are reliable and up to date (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592,

paragraphs 173 and 174).

Real-time collection of traffic and location data

183 The real-time collection of traffic and location data referred to in Article L. 851-2 of the CSI may be individually authorised in respect of a 'person previously identified as potentially having links to a [terrorist] threat'. Moreover, according to that description, and 'where there are substantial grounds for believing that one or more persons belonging to the circle of the person to whom the authorisation relates are capable of providing information in respect of the purpose for which the authorisation was granted, authorisation may also be granted individually for each of those persons'.

184 The data that is the subject of such a measure allows the national competent authorities to monitor, for the duration of the authorisation, continuously and in real time, the persons with whom those persons are communicating, the means that they use, the duration of their communications and their places of residence and movements. It may also reveal the type of information consulted online. Taken as a whole, as is clear from paragraph 117 of the present judgment, that data makes it possible to draw very precise conclusions concerning the private lives of the persons concerned and provides the means to establish a profile of the individuals concerned, information that is no less sensitive, from the perspective of the right to privacy, than the actual content of communications.

185 With regard to the real-time collection of data referred to in Article L. 851-4 of the CSI, that provision authorises technical data concerning the location of terminal equipment to be collected and transmitted in real time to a department reporting to the Prime Minister. It appears that such data allows the department responsible, at any moment throughout the duration of that authorisation, to locate, continuously and in real time, the terminal equipment used, such as mobile telephones.

186 Like national legislation authorising the automated analysis of data, national legislation authorising such real-time collection derogates from the obligation of principle, established in Article 5 of Directive 2002/58, to ensure the confidentiality of electronic communications and related data. It therefore also constitutes interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter and is likely to have a deterrent effect on the exercise of freedom of expression, which is guaranteed in Article 11 of the Charter.

187 It must be emphasised that the interference constituted by the real-time collection of data that allows terminal equipment to be located appears particularly serious, since that data provides the competent national authorities with a means of accurately and permanently tracking the movements of users of mobile telephones. To the extent that that data must therefore be considered to be particularly sensitive, real-time access by the competent authorities to such data must be distinguished from non-real-time access to that data, the first being more intrusive in that it allows for monitoring of those users that is virtually total (see, by analogy, with regard to Article 8 of the ECHR, ECtHR, 8 February 2018, *Ben Faiza v. France* CE:ECHR:2018:0208JUD003144612, § 74). The seriousness of that interference is further aggravated where the real-time collection also extends to the traffic data of the persons concerned.

188 Although the objective of preventing terrorism pursued by the national legislation at issue in the main proceedings is liable, given its importance, to justify interference in the form of the real-time collection of traffic and location data, such a measure may be implemented, taking into account its particularly intrusive nature, only in respect of persons with respect to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities. With regard to persons falling outside of that category, they may only be the subject of non-real-time access, which may occur, in accordance with the Court's case-law, only in particular situations, such as those involving terrorist activities, and where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating terrorism (see, to that effect,

judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119 and the case-law cited).

189 In addition, a decision authorising the real-time collection of traffic and location data must be based on objective criteria provided for in the national legislation. In particular, that legislation must define, in accordance with the case-law cited in paragraph 176 of the present judgment, the circumstances and conditions under which such collection may be authorised and must provide that, as was pointed out in the previous paragraph, only persons with a link to the objective of preventing terrorism may be subject to such collection. In addition, a decision authorising the real-time collection of traffic and location data must be based on objective and non-discriminatory criteria provided for in national legislation. In order to ensure, in practice, that those conditions are observed, it is essential that the implementation of the measure authorising real-time collection be subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding, with that court or body having to satisfy itself, inter alia, that such real-time collection is authorised only within the limits of what is strictly necessary (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 120). In cases of duly justified urgency, the review must take place within a short time.

Notification of persons whose data has been collected or analysed

190 The competent national authorities undertaking real-time collection of traffic and location data must notify the persons concerned, in accordance with the applicable national procedures, to the extent that and as soon as that notification is no longer liable to jeopardise the tasks for which those authorities are responsible. That notification is, indeed, necessary to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal, that right indeed being explicitly guaranteed in Article 15(2) of Directive 2002/58, read in conjunction with Article 79(1) of Regulation 2016/679 (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 121 and the case-law cited, and Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraphs 219 and 220).

191 With regard to the notification required in the context of automated analysis of traffic and location data, the competent national authority is obliged to publish information of a general nature relating to that analysis without having to notify the persons concerned individually. However, if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually. That notification must, however, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible (see, by analogy, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraphs 222 and 224).

192 In the light of all the foregoing, the answer to questions 2 and 3 in Case C-511/18 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 not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:

– recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an 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 a situation justifying that measure exists and that the conditions

and safeguards that must be laid down are observed; and where

– recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

Question 2 in Case C-512/18

193 By question 2 in Case C-512/18, the referring court seeks, in essence, to ascertain whether the provisions of Directive 2000/31, read in the light of Articles 6, 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services.

194 While the referring court maintains that such services fall within the scope of Directive 2000/31 rather than within that of Directive 2002/58, it takes the view that Article 15(1) and (2) of Directive 2000/31, read in conjunction with Articles 12 and 14 of the same, does not, in itself, establish a prohibition in principle on data relating to content creation being retained, which can be derogated from only exceptionally. However, that court is uncertain whether that finding can be made given that the fundamental rights enshrined in Articles 6, 7, 8 and 11 of the Charter must necessarily be observed.

195 In addition, the referring court points out that its question is raised in reference to the obligation to retain provided for in Article 6 of the LCEN, read in conjunction with Decree No 2011-219. The data that must be retained by the service providers concerned on that basis includes, inter alia, data relating to the civil identity of persons who have used those services, such as their surname, forename, their associated postal addresses, their associated email or account addresses, their passwords and, where the subscription to the contract or account must be paid for, the type of payment used, the payment reference, the amount and the date and time of the transaction.

196 Furthermore, the data that is the subject of the obligation to retain covers the identifiers of subscribers, of connections and of terminal equipment used, the identifiers attributed to the content, the dates and times of the start and end of the connections and operations as well as the types of protocols used to connect to the service and transfer the content. Access to that data, which must be retained for one year, may be requested in the context of criminal and civil proceedings, in order to ensure compliance with the rules governing civil and criminal liability, and in the context of the intelligence collection measures to which Article L. 851-1 of the CSI applies.

197 In that regard, it should be noted that, in accordance with Article 1(2) of Directive 2000/31, that directive approximates certain national provisions on information society services that are referred to in Article 2(a) of that directive.

198 It is true that such services include those which are provided at a distance, by means of electronic equipment for the processing and storage of data, at the individual request of a recipient of services, and normally in return for remuneration, such as services providing access to the Internet or to a communication network and hosting services (see, to that effect, judgments of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, paragraph 40; of 16 February 2012, *SABAM*, C-360/10, EU:C:2012:85, paragraph 34; of 15 September 2016, *Mc Fadden*, C-484/14, EU:C:2016:689, paragraph 55; and of 7 August 2018, *SNB-REACT*, C-521/17, EU:C:2018:639, paragraph 42 and the case-law cited).

199 However, Article 1(5) of Directive 2000/31 provides that that directive is not to apply to questions relating to information society services covered by Directives 95/46 and 97/66. In that regard, it is

clear from recitals 14 and 15 of Directive 2000/31 that the protection of the confidentiality of communications and of natural persons with regard to the processing of personal data in the context of information society services are governed only by Directives 95/46 and 97/66, the latter of which prohibits, in Article 5 thereof, all forms of interception or surveillance of communications, in order to protect confidentiality.

200 Questions related to the protection of the confidentiality of communications and personal data must be assessed on the basis of Directive 2002/58 and Regulation 2016/679, which replaced Directive 97/66 and Directive 95/46 respectively, and it should be noted that the protection that Directive 2000/31 is intended to ensure cannot, in any event, undermine the requirements under Directive 2002/58 and Regulation 2016/679 (see, to that effect, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 57).

201 The obligation imposed by the national legislation referred to in paragraph 195 of the present judgment on providers of access to online public communication services and hosting service providers requiring them to retain personal data relating to those services must, therefore – as the Advocate General proposed in point 141 of his Opinion in Joined Cases *La Quadrature du Net and Others* (C-511/18 and C-512/18, EU:C:2020:6) – be assessed on the basis of Directive 2002/58 or Regulation 2016/679.

202 Accordingly, depending on whether the provision of services covered by that national legislation falls within the scope of Directive 2002/58 or not, it is to be governed either by that directive, specifically by Article 15(1) thereof, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, or by Regulation 2016/679, specifically by Article 23(1) of that regulation, read in the light of the same articles of the Charter.

203 In the present instance, it is conceivable, as the European Commission submitted in its written observations, that some of the services to which the national legislation referred to in paragraph 195 of the present judgment is applicable constitute electronic communications services within the meaning of Directive 2002/58, which is for the referring court to verify.

204 In that regard, Directive 2002/58 covers electronic communications services that satisfy the conditions set out in Article 2(c) of Directive 2002/21, to which Article 2 of Directive 2002/58 refers and which defines an electronic communications service as ‘a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting’. As regards information society services, such as those referred to in paragraphs 197 and 198 of the present judgment and covered by Directive 2000/31, they are electronic communications services to the extent that they consist wholly or mainly in the conveyance of signals on electronic communications networks (see, to that effect, judgment of 5 June 2019, *Skype Communications*, C-142/18, EU:C:2019:460, paragraphs 47 and 48).

205 Therefore, Internet access services, which appear to be covered by the national legislation referred to in paragraph 195 of the present judgment, constitute electronic communications services within the meaning of Directive 2002/21, as is confirmed by recital 10 of that directive (see, to that effect, judgment of 5 June 2019, *Skype Communications*, C-142/18, EU:C:2019:460, paragraph 37). That is also the case for web-based email services, which, it appears, could conceivably also fall under that national legislation, since, on a technical level, they also involve wholly or mainly the conveyance of signals on electronic communications networks (see, to that effect, judgment of 13 June 2019, *Google*, C-193/18, EU:C:2019:498, paragraphs 35 and 38).

206 With regard to the requirements resulting from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, it is appropriate to refer back to all of the findings and assessments made in the context of the answer given to question 1 in each of Cases C-511/18 and C-512/18 and to questions 1 and 2 in Case C-520/18.

207 As regards the requirements stemming from Regulation 2016/679, it should be noted that the purpose of that regulation is, inter alia, as is apparent from recital 10 thereof, to ensure a high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 101).

208 To that end, any processing of personal data must, subject to the derogations permitted in Article 23 of Regulation 2016/679, observe the principles governing the processing of personal data and the rights of the person concerned set out, respectively, in Chapters II and III of that regulation. In particular, any processing of personal data must, first, comply with the principles set out in Article 5 of that regulation and, second, satisfy the lawfulness conditions listed in Article 6 of that regulation (see, by analogy, with regard to Directive 95/46, judgment of 30 May 2013, *Worten*, C-342/12, EU:C:2013:355, paragraph 33 and the case-law cited).

209 With regard, more specifically, to Article 23(1) of Regulation 2016/679, that provision, much like Article 15(1) of Directive 2002/58, allows Member States to restrict, for the purposes of the objectives that it provides for and by means of legislative measures, the scope of the obligations and rights that are referred to therein ‘when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard’ the objective pursued. Any legislative measure adopted on that basis must, in particular, comply with the specific requirements set out in Article 23(2) of that regulation.

210 Accordingly, Article 23(1) and (2) of Regulation 2016/679 cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein (see, by analogy, with regard to Directive 95/46, judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 91). In particular, as is the case for Article 15(1) of Directive 2002/58, the power conferred on Member States by Article 23(1) of Regulation 2016/679 may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (see, by analogy, with regard to Directive 95/46, judgment of 7 November 2013, *IPI*, C-473/12, EU:C:2013:715, paragraph 39 and the case-law cited).

211 It follows that the findings and assessments made in the context of the answer given to question 1 in each of Cases C-511/18 and C-512/18 and to questions 1 and 2 in Case C-520/18 apply, *mutatis mutandis*, to Article 23 of Regulation 2016/679.

212 In the light of the foregoing, the answer to question 2 in Case C-512/18 is that Directive 2000/31 must be interpreted as not being applicable in the field of the protection of the confidentiality of communications and of natural persons as regards the processing of personal data in the context of information society services, such protection being governed by Directive 2002/58 or by Regulation 2016/679, as appropriate. Article 23(1) of Regulation 2016/679, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services.

Question 3 in Case C-520/18

213 By question 3 in Case C-520/18, the referring court seeks, in essence, to ascertain whether a national court may apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, pursuing

the objectives of safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data, owing to the fact that that legislation is incompatible 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.

214 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 EU provisions, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States (judgments of 15 July 1964, *Costa*, 6/64, EU:C:1964:66, pp. 593 and 594, and 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 and 158 and the case-law cited).

215 In the light of the primacy principle, where it is unable to interpret national law 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 (judgments of 22 June 2010, *Melki and Abdeli*, C-188/10 and C-189/10, EU:C:2010:363, paragraph 43 and the case-law cited; of 24 June 2019, *Popławski*, C-573/17, EU:C:2019:530, paragraph 58; and 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, paragraph 160).

216 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 (see, to that effect, judgments of 23 October 2012, *Nelson and Others*, C-581/10 and C-629/10, EU:C:2012:657, paragraphs 89 and 91; of 23 April 2020, *Herst*, C-401/18, EU:C:2020:295, paragraphs 56 and 57; and of 25 June 2020, *A and Others (Wind turbines at Aalter and Nevele)*, C-24/19, EU:C:2020:503, paragraph 84 and the case-law cited).

217 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 (see, to that effect, judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, paragraph 177 and the case-law cited).

218 However, 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).

219 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. Maintaining the effects of national legislation such as that at issue in the main proceedings 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 has been retained.

220 Therefore, the referring court cannot apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of the national legislation at issue in the main proceedings.

221 That said, in their observations submitted to the Court, VZ, WY and XX contend that question 3 implicitly yet necessarily asks whether EU law precludes the use, in criminal proceedings, of information and evidence obtained as a result of the general and indiscriminate retention of traffic and location data in breach of that law.

222 In that regard, and in order to give a useful answer to the referring court, it should be recalled that, as EU law currently stands, it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence obtained by such retention of data contrary to EU law.

223 The Court has consistently held that, in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish, in accordance with the principle of procedural autonomy, procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar domestic actions (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (see, to that effect, judgments of 6 October 2015, *Târşia*, C-69/14, EU:C:2015:662, paragraphs 26 and 27; of 24 October 2018, *XC and Others*, C-234/17, EU:C:2018:853, paragraphs 21 and 22 and the case-law cited; and of 19 December 2019, *Deutsche Umwelthilfe*, C-752/18, EU:C:2019:1114, paragraph 33).

224 As regards the principle of equivalence, it is for the national court hearing criminal proceedings based on information or evidence obtained in contravention of the requirements stemming from Directive 2002/58 to determine whether national law governing those proceedings lays down less favourable rules on the admissibility and use of such information and evidence than those governing information and evidence obtained in breach of domestic law.

225 As for the principle of effectiveness, it should be noted that the objective of national rules on the admissibility and use of information and evidence is, in accordance with the choices made by national law, to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences. That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence.

226 That said, it is apparent from the Court's case-law that in deciding whether to exclude information and evidence obtained in contravention of the requirements of EU law, regard must be had, in particular, to the risk of breach of the adversarial principle and, therefore, the right to a fair trial entailed by the admissibility of such information and evidence (see, to that effect, judgment of 10 April 2003, *Steffensen*, C-276/01, EU:C:2003:228, paragraphs 76 and 77). If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence to avoid such an infringement (see, to that effect, judgment of 10 April 2003, *Steffensen*, C-276/01, EU:C:2003:228, paragraphs 78 and 79).

227 Therefore, the principle of effectiveness requires national criminal courts to disregard information

and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

228 In the light of the foregoing, the answer to question 3 in Case C-520/18 is that a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible 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. Article 15(1), interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

Costs

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

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

1. **Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, 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, does not preclude legislative measures that:**

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

   – **provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention**

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

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

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

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

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

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 not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:**

– **recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an 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 a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; and where**

– **recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.**

3. **Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), must be interpreted as not being applicable in the field of the protection of the confidentiality of communications and of natural persons as regards the processing of personal data in the context of information society services, such protection being governed by Directive 2002/58, as amended by Directive 2009/136, or by Regulation (EU) 2016/679 of the European**

Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as appropriate. Article 23(1) of Regulation 2016/679, 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 which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services.

4. **A national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with 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. Article 15(1), interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.**

[Signatures]

---

* Language of the case: French.