11

De dataretentie-uitspraken: is er licht aan het einde van de tunnel?

Hof van Justitie EU
6 oktober 2020, gevoegde zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791
(Lenaerts, Silva de Lapuerta, Bonichot, Arabadjiev, Prechal, Safjan, Xuereb, Rossi, Malenovský, Bay Larsen, Von Danwitz, Toader, Jürimäe, Lycourgos, Piçarra)
Noot prof. mr. dr. J.J. Oerlemans, mr. dr. M. Hagens

E-Privacyrichtlijn. Dataretentie. Nationale veiligheid. Elektronische communicatiediensten.

[Richtlijn 2002/58/EG art. 5, 15; Handvest grondrechten EU art. 7, 8]

Het gaat in deze zaak van het Hof van Justitie van de Europese Unie om de verenigbaarheid van wettelijke regelingen die de mogelijkheid geven om providers van elektronische communicatiediensten te verplichten om algemeen en ongedifferentieerd gegevens te verzamelen ter bescherming van, onder andere, de nationale veiligheid met Richtlijn 2002/58/EG (hierna: de e-Privacyrichtlijn). Het doel van de e-Privacyrichtlijn is om gebruikers van elektronische communicatieservices te beschermen tegen risico's aangaande hun persoonsgegevens en privacy, in het bijzonder risico's in verband met geautomatiseerde opslag en verwerking van gegevens. Art. 5 lid 1 e-Privacyrichtlijn verplicht tot vertrouwelijkheid van communicatie. Lidstaten kunnen daarop op grond van art. 15 lid 1 e-Privacyrichtlijn een uitzondering maken als dat in de democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronische communicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Art. 15 lid 1 moet worden gelezen in het licht van art. 7 en 8 Handvest. De beperkingen moeten daarnaast gebaseerd zijn op objectieve criteria die in verhouding staan tot het doel.
Een nationale regeling die de mogelijkheid geeft om providers van elektronische communicatiediensten te verplichten om algemeen en ongedifferentieerd gegevens te verzamelen ter bescherming van de nationale veiligheid, moet zijn gelimiteerd tot situaties waarin er een ernstige dreiging is voor de nationale veiligheid. De e-Privacyrichtlijn sluit nationale maatregelen uit die providers verplichten om algemene en ongedifferentieerde dataretentie ten aanzien van verkeers-en locatiegegevens uit te voeren als preventieve maatregelen. Dit is in strijd met art. 7 en 8 Handvest. De e-Privacyrichtlijn staat een dergelijke verplichting echter niet in de weg als sprake is van een ernstige bedreiging van de nationale veiligheid die reëel en aanwezig of voorzienbaar is. Een dergelijke verplichting moet wel beperkt zijn in tijdsduur tot het strikt noodzakelijke en onderwerp zijn van een effectieve beoordeling door een rechter of onafhankelijk overheidsorgaan wiens oordeel bindend is. In het licht van de bescherming van de nationale veiligheid en bestrijding van zware criminaliteit wordt een wettelijke regeling waarin providers worden verplicht om gericht of algemeen en ongedifferentieerd data te verzamelen niet uitgesloten door de e-Privacyrichtlijn, mits dit niet langer duurt dan strikt noodzakelijk.

Deze uitspraak is tevens opgenomen in «JBP» 2021/1.

La Quadrature du Net (C-511/18 en C-512/18),
French Data Network (C-511/18 en C-512/18),
Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 en C-512/18),
Igwan.net (C-511/18)
tegen
Premier ministre (C-511/18 en C-512/18),
Garde des Sceaux, ministre de la Justice (C-511/18 en C-512/18),
Ministre de l'Intérieur (C-511/18),
Ministre des Armées (C-511/18),
in tegenwoordigheid van:
Privacy International (C-512/18),
Center for Democracy and Technology (C-512/18),
en
Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,

UA,
Liga voor Mensenrechten VZW,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX,
tegen
Ministerraad,
in tegenwoordigheid van:
Child Focus (C-520/18).

Judgment
(...; *red.*)

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, ECLI: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, ECLI: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 provi-

sion 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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI:EU:C:2013:363, paragraph 38; of 20 March 2018, Commission v Austria (State printing office), C-187/16, ECLI: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, ECLI: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, ECLI: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 Ar-

ticle 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, ECLI: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, ECLI: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, ECLI: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 partic-

ular, 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, ECLI: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, ECLI: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, ECLI: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 avail-

able, 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, ECLI:EU:C:2014:238, paragraphs 25 and 70, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI: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, ECLI:EU:C:2001:127, paragraph 39, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI: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, ECLI: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, ECLI: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, ECLI:EU:C:2014:238, paragraph 27, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI: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, ECLI:EU:C:2014:238, paragraph 28, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI: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, ECLI: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, ECLI:EU:C:2016:84, paragraph 47; of 28 July 2016, JZ, C-294/16 PPU, ECLI:EU:C:2016:610, paragraph 48; and of 19 september 2019, Rayonna prokuratura Lom, C-467/18, ECLI: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, ECLI:EU:C:2019:108, paragraph 57, and of 21 May 2019, Commission v Hungary (Rights of usufruct over agricultural land), C-235/17, ECLI: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, ECLI: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, ECLI:EU:C:2008:727, paragraph 56; of 9 november 2010, Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraphs 76, 77 and 86; and of 8 april 2014, Digital Rights, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 52; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, ECLI: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, ECLI: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, ECLI:EU:C:2014:238, paragraphs 54 and 55, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 117; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, ECLI: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, ECLI:EU:C:2017:592, paragraph 191 and the case-law cited, and judgment of 3 October 2019, A and Others, C-70/18, ECLI: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, ECLI:EU:C:2016:970, paragraph 102, and of 2 October 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, paragraphs 56 and 57; Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, ECLI: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, ECLI: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, ECLI:EU:C:2014:238, paragraphs 57 and 58, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI: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, ECLI:EU:C:2014:238, paragraph 59, and of 21 december 2016, Tele2, C-203/15 and C-698/15, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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 impo-

sing 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 cor-

responds, 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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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 lat-

ter 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, ECLI:EU:C:2016:970, paragraph 121 and the case-law cited, and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, ECLI: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, ECLI: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, ECLI:EU:C:2011:771, paragraph 40; of 16 February 2012, SABAM, C-360/10, ECLI:EU:C:2012:85, paragraph 34; of 15 september 2016, Mc Fadden, C-484/14, ECLI:EU:C:2016:689, paragraph 55; and of 7 August 2018, SNB-REACT, C-521/17, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI:EU:C:2010:363, paragraph 43 and the case-law cited; of 24 June 2019, Popławski, C-573/17, ECLI: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, ECLI: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, ECLI:EU:C:2012:657, paragraphs 89 and 91; of 23 april 2020, Herst, C-401/18, ECLI: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, ECLI: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, ECLI: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, ECLI: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, ECLI:EU:C:2015:662, paragraphs 26 and 27; of 24 October 2018, XC and Others, C-234/17, ECLI:EU:C:2018:853, paragraphs 21 and 22 and the case-law cited; and of 19 december 2019, Deutsche Umwelthilfe, C-752/18, ECLI: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, ECLI: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, ECLI: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 pre-

venting 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.

NOOT

Inleiding

In hoeverre is de ongebreidelde bewaring (dataretentie) dan wel doorzending van communicatiegegevens door aanbieders van openbare elektronische communicatiediensten of -netwerken (hierna: aanbieders van communicatiediensten) ter bestrijding van ernstige criminaliteit en ter bescherming van de nationale veiligheid toegestaan? Op deze vraag en enkele andere prejudiciele vragen geeft het Hof van Justitie van de Europese Unie (hierna: HvJ EU) antwoord in de zaak *La Quadrature du Net e.a./Premier ministre e.a.* (HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791) (hierna: *La Quadrature du Net e.a.*).[1]

In zijn eerdere jurisprudentie heeft het HvJ EU zich al kritisch uitgesproken over retentie van communicatiegegevens bij aanbieders van communicatiediensten (dataretentie). In 2014 verklaarde het HvJ EU in het arrest *Digital Rights*[2] de Dataretentierichtlijn (Richtlijn 2006/24/EG) in strijd met het Unierecht. Veel lidstaten deden na het *Digital Rights*-arrest een beroep op de uitzondering in art. 15 lid 1 e-Privacyrichtlijn (Richtlijn 2002/58/EG) om de bewaring van de communicatiegegevens via een nationale regeling toch verplicht te stellen.

Geschillen over zowel de toelaatbaarheid als de inhoud van dergelijke nationale wetgeving in Zweden en in het Verenigd Koninkrijk leidden uiteindelijk tot prejudiciële vragen en nieuwe arresten over het onderwerp. In 2016 overwoog het HvJ EU in de arresten *Tele2 Sverige AB* en *Watson*[3] dat nationale wetgeving waarin een algemene en ongedifferentieerde bewaarplicht voor aanbieders van communicatiediensten is voorzien met het oog op de bestrijding van ernstige criminaliteit, niet verenigbaar is met de e-Privacyrichtlijn en het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest).

In de zaak *La Quadrature du Net e.a.* bestendigt het HvJ EU deze lijn, zelfs waar het doel van de nationale maatregelen de bescherming van de nationale veiligheid betreft. Tegelijkertijd biedt het HvJ EU in het arrest ruimte voor beperkte vormen van dataretentie, afhankelijk van het inbreukmakende karakter van de te bewaren gegevens en het doel dat met de bewaring wordt nagestreefd.

Deze annotatie bespreekt eerst de overwegingen van het HvJ EU over de prejudiciële vraag of het Europese Hof zich mag uitspreken over nationale wetgeving op het gebied van nationale veiligheid. Verder gaat de annotatie in op de diverse bewaarverplichtingen en verstrekking van gegevens door aanbieders van communicatiediensten die het HvJ EU onder strikte voorwaarden mogelijk acht. Ten slotte bespreken wij kort welke gevolgen de uitspraken hebben voor het nationale veiligheidsdomein in Nederland, specifiek met betrekking tot de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017).

Jurisdictie en HvJ EU over nationale veiligheid

In *La Quadrature du Net e.a.* (par. 85-86) beroepen de betrokken partijen zich op art. 1 lid 3 e-Privacyrichtlijn. Zij stellen dat activiteiten van de lidstaten, in het bijzonder nationale bewaarregelingen die verband houden met openbare veiligheid, defensie en staatsveiligheid van de werkingssfeer van de e-Privacyrichtlijn zijn uitgesloten. Ook verwijzen zij naar art. 4 lid 2 Verdrag betreffende de Europese Unie (hierna: VEU) waarin staat dat de nationale veiligheid tot de

1 Zie op dezelfde dag ook de (vergelijkbare) uitspraak in de zaak *Privacy International/Secretary of State e.a.* (HvJ EU 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790). Onze oorspronkelijke dubbelannotatie in «JBP» 2021/1-2 had ook betrekking op *Privacy International*. Hier richten we ons op *La Quadrature du Net e.a.* en de relevante ontwikkelingen in de jurisprudentie nadien. Daarom verwijzen we niet steeds ook naar de relevante overwegingen in *Privacy International*.

2 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights/Ierland*).

3 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970 (*Tele2 Sverige AB* en *Watson)*.

uitsluitende verantwoordelijkheid van de lidstaten behoort. Ten slotte wijzen zij erop dat als de betreffende activiteiten wel binnen de reikwijdte van de e-Privacyrichtlijn vallen, deze in art. 15 uitzonderingen op de bescherming van vertrouwelijke communicatie toelaten, onder meer in het belang van de nationale veiligheid en criminaliteitsbestrijding.

Het HvJ EU gaat niet mee met de stelling dat nationale wetgeving die gericht is op het waarborgen van de nationale veiligheid buiten de werkingssfeer van de e-Privacyrichtlijn valt. De e-Privacyrichtlijn reguleert de verwerking van persoonsgegevens (verkeers-, locatie- en gebruikersgegevens) door aanbieders van communicatiediensten in het elektronische communicatiedomein. De belangrijkste verplichtingen in de e-Privacyrichtlijn zien op het waarborgen van de vertrouwelijkheid van deze gegevens en beperking van opslag van deze gegevens voor andere doeleinden dan bedrijfsvoering en door andere partijen zonder toestemming van de gebruikers. De e-Privacyrichtlijn is gestoeld op het Handvest, met name art. 7 (gegevensbescherming), art. 8 (privacy) en art. 11 (vrijheid van meningsuiting). Nationale dataretentiewetgeving impliceert dat die aanbieders gegevens verwerken en dat de verwerking en daarmee de wetgeving binnen de werkingssfeer van de e-Privacyrichtlijn valt (*La Quadrature du Net e.a.*, par. 93, 95, 96, 104).

Het enkele feit dat een nationale regeling is getroffen met het oog op de bescherming van de nationale veiligheid kan er niet toe leiden dat het Unierecht niet van toepassing is en dat lidstaten worden ontheven van hun verplichting om dit recht te eerbiedigen. De uitzondering moet met andere woorden niet de regel worden (*La Quadrature du Net e.a.*, par. 111). Dit laat onverlet dat lidstaten zelf hun wezenlijke veiligheidsbelangen mogen definiëren en passende maatregelen mogen nemen ter bescherming hiervan (*La Quadrature du Net e.a.*, par. 99). Het HvJ EU overweegt verder dat nationale wetgeving die aanbieders van communicatiediensten verplicht om verkeers- en locatiegegevens te bewaren (opslaan) en de autoriteiten toegang tot die gegevens te verlenen, impliceert dat die aanbieders gegevens verwerken en dat de verwerking en daarmee de wetgeving binnen de werkingssfeer van de e-Privacyrichtlijn valt (*La Quadrature du Net e.a.*, par. 93, 95, 96, 104). Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronische communicatiediensten, wordt de bescherming van de gegevens van de betrokken gebruikers niet beheerst door de e-Privacyrichtlijn. De betrokken maatregelen moeten dan met name in overeenstemming zijn met het nationale constitutionele recht en met de vereisten van het Europees Verdrag van de Rechten van de Mens (EVRM) (*La Quadrature du Net e.a.*, par. 103).

Het arrest in *La Quadrature du Net* onderscheidt zich ten opzichte van (de eerdergenoemde) 'oude' dataretentiearresten met name in het feit dat het HvJ EU eisen stelt aan de dataretentie en de bewaring van gegevens ten behoeve van het nationale veiligheidsdomein.[4] Dat is goed nieuws voor privacyvoorvechters, maar mogelijk minder goed nieuws voor staten die hun autonomie willen behouden in de bescherming van de nationale veiligheid. Het HvJ EU beperkt namelijk in het arrest de mogelijkheden tot de bewaring (verstrekking) van communicatiegegevens en verbindt daar bovendien stevige (en helaas soms onduidelijke) kwalitatieve vereisten aan (zie verder paragraaf 4 van deze noot). In *La Quadrature du Net* beperkt het HvJ EU de mogelijkheid – anders gezegd: de soevereiniteit – van lidstaten hun nationale veiligheid met eigen wetgeving te beschermen, ondanks het feit dat in art. 4 lid 2 VEU staat dat de bescherming van de nationale veiligheid de *uitsluitende verantwoordelijkheid van de staat* blijft. Gezien het aantal staten dat zich bij de prejudiciële vragen heeft gevoegd ligt deze beperking van soevereiniteit zeer gevoelig bij staten.[5] Niet alle staten lijken zich ook na het arrest daarbij neer te leggen.

Na het arrest in *La Quadrature du Net e.a.* ging de zaak bijvoorbeeld terug naar de Franse Raad van State ('Conseil d'État') voor een definitieve uitspraak over de vraag of de Franse datareten-

4 Zie ook S. Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and Others and Privacy International', *European Data Protection Law Review*, 8, p. 147.

5 In *La Quadrature du Net e.a.* hebben zich naast de regering van het Verenigd Koninkrijk en Frankrijk, ook de Tsjechische, Estse, Ierse, Cypriotische, Hongaarse, Poolse en Zweedse regeringen gevoegd (par. 89).

tiewetgeving voldeed aan de criteria van het Unierecht, zoals door het HvJ EU uiteengezet. De Franse regering beargumenteerde dat het HvJ EU buiten zijn boekje was gegaan ('ultra vires') door de EU een belangrijke 'soevereine' bevoegdheid toe te eigenen – nationale veiligheid en bescherming van de openbare orde – die de lidstaten nooit aan het HvJ EU hebben overgedragen. Zij vroeg haar hoogste rechterlijke instantie een keuze te maken tussen de plicht van een EU-lidstaat om uit principe de jurisprudentie van het HvJ EU te respecteren en de eigen interpretatie van de belangrijkste grondwettelijke beginselen van die lidstaat.[6]

In zijn beslissing van 21 april 2021 weigerde de Franse Raad van State een *ultra vires*-toetsing uit te voeren, maar benadrukte ook dat hij ervoor moest zorgen dat de door het HvJ EU opgelegde beperkingen de Franse grondwettelijke beginselen niet in gevaar zouden brengen. De Franse Raad van State oordeelde dat de bestaande dreiging voor de nationale veiligheid momenteel de algemene bewaring van communicatiegegevens door communicatieaanbieders rechtvaardigt. Dit lijkt ons overigens wel heel kort door de bocht gezien de overige criteria die het HvJ EU voor een algemene bewaarplicht vereist (zie paragraaf 3 en 4). Wel merkt de Franse Raad van State op dat het Franse rechtskader niet voorziet in een voorafgaande toetsing door een onafhankelijke autoriteit en daarmee niet voldoet. Het advies van de 'Commission Nationale de contrôle des Techniques d'Intelligence' (CNCTR) is niet voldoende, omdat deze niet bindend is. De Franse Raad van State gelast daarom de minister-president het regelgevingskader met betrekking tot dit aspect te wijzigen.

In België daarentegen vernietigde het Grondwettelijk Hof met een arrest van 22 april 2021 (nr. 57/2021) de bepalingen van de wet van 29 mei 2016 die voorzagen in de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie naar aanleiding van *La Quadrature du Net e.a.* Het Grondwettelijk Hof overwoog dat het aan de wetgever is om een regeling tot stand te brengen waarbij toepasselijke beginselen in acht worden genomen, in het licht van de rechtspraak van het HvJ EU. Op 20 juli 2022 werd een nieuwe dataretentiewet aangenomen in het Belgische Parlement en deze trad op 18 augustus 2022 in werking.[7]

De bewaring en verstrekking van communicatiegegevens

Het HvJ EU acht een algemene en ongedifferentieerde bewaarplicht van communicatiegegevens (d.w.z. metadata over inhoudelijke telecommunicatie) ter bestrijding van (ernstige) criminaliteit in *La Quadrature du Net e.a.* nog steeds onevenredig en in strijd met art. 7, 8 en 11 en art. 52 lid 1 Handvest (par. 141).[8] Meer recent is dit uitgangspunt bevestigd in *SpaceNet AG*[9] en *Commissioner of the Garda Síochána e.a.*[10] Ten opzichte van *Digital Rights* en *Tele2* maakt het HvJ EU echter belangrijke nuanceringen met betrekking tot de bewaarplicht als maatregel en het opvragen van communicatiegegevens bij aanbieders van communicatiediensten.

Telkens past het HvJ EU in zijn toetsing een evenredigheidstoets toe door de ernst van de inmenging veroorzaakt door de bewaarplicht als maatregel te meten en na te gaan of deze inmenging evenredig is aan het algemeen belang dat wordt nagestreefd. In deze proportionaliteitstest komt naar voren dat verkeersgegevens en in het bijzonder locatiegegevens gevoelig zijn en een ernstige inmenging vormen in de vertrouwelijkheid van de te beschermen gegevens en het recht op eerbiediging van het privéleven (zie *La Quadrature du Net e.a.*, par. 117). IP-adressen en andere registratiegegevens van gebruikers van

6 Zie T. Christakis & K. Propp, 'How Europe's Intelligence Services aim to avoid the EU's Highest Court – and what it means for the United States', *Lawfare*, 8 maart 2021.

7 Zie verder L. van Roy & S. Royer, 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *Nullum Crimen: Tijdschrift voor Straf- en Strafprocesrecht* 2023.

8 Met verwijzing naar HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 en ECLI:EU:C:2016:970, par. 107, «EHRC» 2017/79, m.nt. Koning, par. 98-99 (*Tele2 Sverige AB* en *Watson).*

9 HvJ EU 20 september 2022, C-793/19 en C-794/19, ECLI:EU:C:2022:702, par. 74 (*Duitsland/SpaceNet AG & Telecom Deutschland GmbH).*

10 HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, par. 59 (*G.D./the Commissioner of the Garda Síochána e.a.*).

de communicatiediensten worden als minder gevoelig gezien (zie par. 152).
Voor de afweging met het algemeen belang valt op dat het HvJ EU deze in *La Quadrature du Net e.a.* duidelijk rangschikt, waarbij de bescherming van de nationale veiligheid als het hoogst te beschermen belang wordt gezien, vervolgens de bestrijding van ernstige criminaliteit en ten slotte het beschermen van de openbare veiligheid (par. 136).[11] Het HvJ EU bevestigt ook in meer recente jurisprudentie dat er een hiërarchie bestaat in de doelstellingen van algemeen belang die een krachtens art. 15 lid 1 van de e-privacyrichtlijn genomen maatregel kunnen rechtvaardigen (*SpaceNet AG*, par. 71, *Commissioner of the Garda Síochána e.a.* par. 56). In paragraaf 100 van het arrest *Commissioner of the Garda Síochána e.a.* verduidelijkt het HvJ EU dat als verkeers- en locatiegegevens onder de vermelde voorwaarden algemeen en ongedifferentieerd zijn bewaard om de nationale veiligheid te beschermen tegen een bedreiging die reëel en actueel of voorzienbaar is, de nationale autoriteiten die bevoegd zijn voor strafonderzoeken daar geen toegang toe mogen hebben in het kader van een strafvervolging.[12]
Wil het HvJ EU tot het oordeel kunnen komen dat een maatregel de proportionaliteitstoets doorstaat, dan moet de nationale wetgeving van de lidstaten telkens duidelijke en precieze regels bevatten die de reikwijdte en de toepassing van de maatregel in kwestie uiteenzetten, en minimumwaarborgen opleggen, zodat de personen van wie de persoonsgegevens worden bewaard voldoende waarborgen hebben dat de gegevens effectief worden beschermd tegen het risico op misbruik. Die wetgeving moet met name aangeven onder welke omstandigheden en voorwaarden een maatregel voor de verwerking van dergelijke gegevens kan worden vastgesteld, zodat de inmenging beperkt blijft tot het strikt noodzakelijke (*La Quadrature du Net e.a.*, par. 132).

Een opsomming van de verschillende situaties waarin het preventief bewaren van communicatiegegevens door aanbieders van communicatiediensten aan de orde kan zijn en de daarbij gestelde voorwaarden is te vinden in paragraaf 168 van het arrest *La Quadrature du Net e.a.*

Beperkte algemene en ongedifferentieerde bewaarplicht ter bescherming van de nationale veiligheid
Het HvJ EU acht in *La Quadrature du Net e.a.* een algemene bewaarplicht mogelijk bij een 'ernstige dreiging voor de nationale veiligheid' voor zover deze werkelijk, actueel of voorzienbaar is (par. 137). Het Hof schaart onder nationale veiligheid 'het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten' (*La Quadrature du Net e.a.,* par. 135 en *SpaceNet AG*, par. 92 en *Commissioner of the Garda Síochána e.a.*, par. 61). Bijzonder zware criminaliteit kan dus niet gelijk worden gesteld met een bedreiging voor de nationale veiligheid. Een bedreiging voor de nationale veiligheid moet reëel en actueel zijn of op zijn minst voorzienbaar– wat onderstelt dat zich voldoende concrete omstandigheden voordoen – om een rechtvaardiging te kunnen vormen voor een maatregel die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens gedurende een beperkte periode (*Spacenet AG*, par. 93).
Het HvJ EU stelt nadere voorwaarden aan een dergelijke bewaarplicht. Volgens het HvJ EU moet daarbij ook uiteindelijk een 'verbinding te leggen zijn met tussen de bewaarde gegevens en de dreiging voor de nationale veiligheid' (par. 137). Deze beperkte bewaarplicht is slechts mogelijk voor een (zo kort mogelijke) bepaalde periode, waarbij deze bewaarplicht kan worden herhaald tot een maximale bewaartermijn (par. 138). In nationale wetgeving moeten er waarborgen tegen misbruik bestaan, waaronder de controle (*effective review*) door een rechtelijke instantie of onafhankelijke administratieve instantie met bindende bevoegdheden (par. 139) (zie ook *Spa-*

11 Zie ook J. Schoers, 'HvJ EU La Quadrature du Net (HvJ EU, C-511/18 e.a.) – Het Hof van Justitie en de voorwaarden voor dataretentie', *EHRC Updates* 2021 (annotatie).
12 Zie ook R.H.T. Jansen & R.M te Molder, 'G.D. t. the Commissioner of the Garda Síochána e.a. (HvJ EU, C-140/20) – Een nieuwe episode in de dataretentierisprudentie', *EHRC Updates* 2022-0117 (annotatie).

ceNet AG, par. 72 en 131 en *Commissioner of the Garda Síochána e.a.*, par. 58).
Het blijft voor ons echter onduidelijk wat wordt verstaan onder een 'ernstige dreiging voor de nationale veiligheid' die 'reëel, actueel of voorzienbaar is'. Gaat het daarbij enkel om een reële dreiging van een (terroristische) aanslag of valt hier meer onder, zoals het beschermen van de nationale veiligheid tegen contraspionage door buitenlandse inlichtingenofficieren? De overweging in paragraaf 135 in *La Quadrature du Net e.a.* over wat nationale veiligheid behelst, duidt meer op nationale ontwrichting en de bescherming van de binnenlandse veiligheid. Het is uit het arrest niet op te maken of het HvJ EU hiermee uitputtend wil zijn of meer ruimte aan de lidstaten laat. Ook uit de meer recente arresten van *SpaceNet AG* en *Commissioner of the Garda Síochána e.a.* wordt dit niet duidelijk. De invulling van nationale veiligheid is op grond van art. 4 lid 2 VEU immers een nationale aangelegenheid. Het is goed denkbaar dat ook dit keer lidstaten hierover prejudiciële vragen zullen stellen aan het HvJ EU.

Kwalitatieve vereisten bij de preventieve bewaring van gegevens
De preventieve (gerichte) bewaring van verkeersgegevens en locatiegegevens van gebruikers van communicatiediensten is slechts onder strikte voorwaarden mogelijk voor de vervolging van ernstige criminaliteit of voor de bescherming van de openbare veiligheid. Volgens het HvJ EU verzet art. 15 e-Privacyrichtlijn zich niet tegen nationale wetgeving die voorziet in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend. Ten eerste kan worden gemikt op personen waarvan aan de hand van verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kan worden gebracht. Daarmee kan worden bijgedragen aan de bestrijding van zware criminaliteit of een ernstig risico voor de openbare of nationale veiligheid kan worden voorkomen. Een ander criterium is geografisch, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd (*Tele2 Sverige* en *Watson*, par. 111, *La Quadrature du Net e.a.*, par. 148, *Commissioner of the Garda Síochána e.a.*, par. 76). Overheidsinstanties leggen dan de verplichting op gegevens niet te wissen die worden verwerkt in het kader van de normale bedrijfsvoering (zoals facturering). Een dergelijk bevel tot het bewaren van deze gegevens (gevolgd door een vordering van de gegevens) moet volgens het HvJ EU dus tot het strikt noodzakelijke worden beperkt, bijvoorbeeld in tijd, kring van personen en/of geografische locatie (*La Quadrature du Net e.a.*, par. 144, *SpaceNet AG*, par. 75).
In de arresten *SpaceNet AG* en *Commissioner of the Garda Síochána e.a.* concretiseert het HvJ EU de wijze waarop hier invulling aan kan worden gegeven. Met betrekking tot de kring van personen geldt dat lidstaten met name de mogelijkheid hebben bewaringsmaatregelen te nemen ten aanzien van personen die worden geïdentificeerd als personen naar wie een onderzoek loopt of voor wie op dat moment al andere surveillancemaatregelen gelden, dan wel personen die een nationaal strafblad hebben waaruit blijkt dat zij reeds zijn veroordeeld voor zware strafbare feiten met mogelijk een groot recidivegevaar. (*SpaceNet AG*, par. 107 en *Commissioner of the Garda Síochána e.a.*, par. 78).
Wat betreft geografische gebieden kan het met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware strafbare feiten, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations, zeehavens of tolzones (*SpaceNet AG*, par. 108 en *Commissioner of the Garda Síochána e.a.*, par. 79). Het blijft echter onduidelijk wat het HvJ EU onder 'zware criminaliteit' verstaat. In Nederland wordt bijvoorbeeld voor het begrip 'ernstig misdrijf' vaak de categorie misdrijven in art. 67 Sv aangehouden, op basis waarvan personen in voorlopige hechtenis mogen worden gesteld. Het is niet duidelijk of het HvJ EU aan andere (nog zwaardere) misdrijven denkt, zoals misdrijven op basis waarop een gevangenisstraf staat van vier jaar of meer.[13] De Hoge Raad heeft daarom een prejudiciële vraag geformuleerd om na te gaan of het aan de bevoegde nationale autoriteiten is om zelf mede invulling te geven aan de begrip-

13 Zie ook J.J. Oerlemans, M. Hagens & S. Royer, 'Tijd voor een nieuwe bewaarplicht?', *Computerrecht* 2021/59, nr. 2, p. 158.

pen 'ernstige strafbare feiten'/'ernstige criminaliteit'/'zware criminaliteit'.[14]

Voor wat betreft de duur van de gegevensbewaring is de uitspraak in *SpaceNet AG* interessant omdat het in casu ging om relatief korte bewaarperioden, in ieder geval aanzienlijk korter dan de duur van de bewaarperioden in de eerdere dataretentiearresten, namelijk maximaal vier weken voor locatiegegevens en maximaal tien weken voor de overige gegevens voor de bestrijding van (ernstige) criminaliteit.[15] De duur van de gegevensbewaring is een relevante factor om te bepalen of het Unierecht zich verzet tegen een nationale regeling waarbij een algemene en ongedifferentieerde bewaring van communicatiegegevens wordt opgelegd, aangezien deze periode 'beperkt' dient te zijn. Echter, het Hof herhaalt dat, met name gelet op de talrijkheid en verscheidenheid van de gegevens, deze het in hun geheel beschouwd mogelijk maken zeer precieuze conclusies te trekken over het privéleven van de persoon/personen van wie de gegevens zijn bewaard en dat van hen een profiel kan worden opgesteld.

Het Hof benadrukt in *Spacenet AG* dat de bewaring van communicatiegegevens hoe dan ook een ernstige inmenging vormt op het privéleven van de betrokken persoon of personen, zelfs bij een korte bewaarduur van vier weken voor locatiegegevens en maximaal tien weken voor de overige gegevens (*Spacenet AG*, par. 88). Bij het toepassen op de feiten in de zaak komt het Hof tot de conclusie dat, ondanks de korte bewaarperioden, zeer precieze conclusies over het privéleven kunnen worden getrokken, zoals over de dagelijkse gewoonten van de gebruikers, hun permanente en tijdelijke verblijfsplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren, en dat aan de hand van deze gegevens een profiel over deze personen kan worden opgesteld (*SpaceNet AG*, par. 90).

Kwalitatieve vereisten bij het realtime verzamelen van gegevens

Het *realtime* verzamelen van gegevens op last van een (in dit geval Franse) overheidsinstantie dient volgens het HvJ EU te worden beperkt tot personen bij wie er een gegronde reden is om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten. Het gaat hier bijvoorbeeld om het realtime verstrekken van belgegevens en locaties van antennes waarmee mobiele telefoons verbinding maken. Het HvJ EU acht deze vorm van realtime 'tracking' een nog ernstigere inmenging dan het achteraf toegang krijgen tot verkeersgegevens.[16] Ook moet het bevel tot verstrekking onderworpen worden aan een voorafgaande goedkeuring (*prior review*) die wordt uitgevoerd door een rechterlijk college of door een onafhankelijk administratief orgaan, waarvan de beslissing bindend is (par. 189).

Zoals ook beschreven in paragraaf 3.2 acht het HvJ verkeers- en locatiegegevens als mogelijk gevoelige informatie. Het betreft informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (*La Quadrature du Net e.a.*, par. 117, *SpaceNet AG,* par. 61 en *Commissioner of the Garda Síochána e.a.*, par. 45).

In andere jurisprudentie, waarbij het arrest *Prokuratuur* het belangrijkste is, legt het HvJ EU uit dat het aan de lidstaten is om in het nationale recht voorwaarden te stellen over toegang tot verkeers- en locatiegegevens bij elektronische communicatiediensten.[17] Het moet duidelijke en nauwkeurige regels bevatten die de reikwijdte en de toepassing van de betrokken maatregel vastleggen en minimumvereisten opleggen, zodat degenen van wie de persoonsgegevens aan de orde zijn over voldoende waarborgen beschikken dat die gegevens doeltreffend worden be-

14 HR 5 april 2022, ECLI:NL:HR:2022:475, par. 6.7 en 6.8.

15 Zie ook D.A.G. van Toor, 'Prokuratuur (HvJ EU, C-746/18) – Differentiatie en beperkingen van dataretentie door telecommunicatieaanbieders en de vorderingsvoorwaarden', *EHRC Updates* 2021-0088 (annotatie).

16 Zie ook J. Schoers, 'HvJEU La Quadrature du Net (HvJ EU, C-511/18 e.a.) – Het Hof van Justitie en de voorwaarden voor dataretentie', *EHRC-Updates 2020-0253* (annotatie).

17 Zie ook zie ook D.A.G. van Toor, 'Prokuratuur (HvJ EU, C-746/18) – Differentiatie en beperkingen van dataretentie door telecommunicatieaanbieders en de vorderingsvoorwaarden', *EHRC Updates* 2021-0088 (annotatie).

schermd tegen het risico van misbruik.[18] Het HvJ EU vindt het daarbij van wezenlijk belang dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens wordt onderworpen aan voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze instanties dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten (*Prokuratuur*, par. 51).

Mogelijkheid van bewaarplicht van gebruikersgegevens

Het HvJ EU acht IP-adressen en identiteitsgegevens van gebruikers van communicatiediensten minder gevoelig dan andere verkeersgegevens (*La Quadrature du Net e.a.*, par. 152, *Commissioner of the Garda Síochána e.a.*, par. 73). Bij cybercriminaliteit is het IP-adres vaak het enige opsporingsmiddel voor het onderzoek. Door op te zoeken door welke internet access-provider het IP-adres is uitgegeven en door de naam- en adresgegevens op te vragen van de abonneehouder kan mogelijk een adres van de verdachte worden achterhaald. De beschikking over deze gegevens kan daarom belangrijk zijn voor opsporingsonderzoeken.[19]

Een bewaarplicht die enkel voorziet in de algemene en ongedifferentieerde bewaring van IP-adressen van de bron van de communicatie (dus van de internetverbinding van gebruikers (par. 152)) en andere gebruikersgegevens ter bescherming van de nationale veiligheid, ter bestrijding van ernstige criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid, is volgens het HvJ EU mogelijk (par. 155-159) (zie ook *SpaceNet AG*, par. 97 en *Commissioner of the Garda Síochána e.a.*, par. 74). De bewaartermijn van deze gebruikersgegevens mag niet langer zijn dan wat strikt noodzakelijk is in het licht van het nagestreefde doel. De regels die dat mogelijk maken moeten in nationale wetgeving worden gevat, waarbij de betrokken personen beschikken over waarborgen tegen het risico van misbruik (par. 168).

De overwegingen van het HvJ EU over de privacygevoeligheid van gebruikersgegevens komen overigens in grote lijnen overeen met de overwegingen van het EHRM over het recht op privacy en gebruikersgegevens in *Breyer*.[20]

In de reeds aanhangige nieuwe *La Quadrature du Net*-zaak, gericht tegen de Franse auteursrechtautoriteit 'HADOPI', concludeerde de A-G dat een algemene en ongedifferentieerde opslag van IP-adressen ook mogelijk moet zijn voor niet-ernstige criminaliteitsbestrijding (*in casu* intellectuele eigendomsrechtschendingen).[21] De belangrijkste reden daarvoor is dat het IP-adres het enige aanknopingspunt kan zijn voor het voorkomen, opsporen, detecteren en vervolgen voor onlinecriminaliteit (par. 83). Het is afwachten in hoeverre het Hof hierin meegaat en mogelijk een autonome interpretatie van het begrip 'zware criminaliteit' formuleert.

Gevolgen voor de wetgeving met betrekking tot nationale veiligheid in Nederland

Uit het voorgaande blijkt dat het HvJ EU zich ook uitspreekt over nationale dataretentiewetgeving die de nationale veiligheid betreft, voor zover Europese wet- en regelgeving daarop van toepassing is. In Nederland reguleert de Wet op de inlichtingen- en Veiligheidsdiensten 2017 (Wiv) het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Deze diensten beschermen de nationale veiligheid en mogen in het kader van deze taakuitvoering bijzondere bevoegdheden inzetten.

De zaak *La Quadrature du Net e.a.* zou gevolgen moeten hebben voor de Wiv 2017. In art. 54-56 Wiv 2017 zijn de medewerkingsbepalingen neergelegd bij vorderingen van gegevens bij aanbie-

18 HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, par. 48 (*H.K./Prokuratuur*).

19 Zie uitgebreid W.N. Ferdinandusse, D. Laheij & J.C. Hendriks, 'De bewaarplicht telecomgegevens en de opsporing. Het belang van historische verkeersgegevens voor de opsporing', Openbaar Ministerie & Nationale Politie 2015. Zie ook J.J. Oerlemans, M. Hagens & S. Royer, 'Tijd voor een nieuwe bewaarplicht?', *Computerrecht* 2021/59, nr. 2, p. 151-159.

20 EHRM 30 januari 2020, 50001/12, ECLI:CE:ECHR:2020:0130JUD005000112, par. 92 en 94 (*Duitsland/Breyer*). Zie ook H.R. Kranenborg, 'Verplichte registratie van prepaid simkaarthouders in overeenstemming met het EVRM?', in *EHRC-Updates* 2020/78 (annotatie) en «JBP» 2020/29, m.nt. Kranenborg.

21 Conclusie van A-G Szpunar van 27 oktober 2022, C-470/21 (*La Quadrature du Net e.a.*).

ders van communicatiediensten en aanbieders van cloudopslagdiensten. Over het geheel genomen voldoen de bepalingen aan de vereisten van het HvJ EU, mede vanwege de verschillende waarborgen die gedifferentieerd worden aan de hand van het type gegevens (d.w.z. inhoudelijke gegevens, verkeersgegevens en gebruikersgegevens). Het HvJ EU vereist in *La Quadrature du Net e.a.* voorafgaand bindend toezicht bij het vorderen van toekomstige (*realtime*) verkeersgegevens (*La Quadrature du Net e.a.*, par. 189). De huidige bevoegdheid in art. 55 Wiv 2017 vereist geen toets van de Toetsingscommissie Inzet Bevoegdheden (TIB) en voldoet daarom niet aan de kwalitatieve vereisten van het HvJ EU.

De regering stelt dan ook voor deze bevoegdheid in art. 55 Wiv 2017 aan te passen in de op 16 januari 2023 voorgestelde nota van wijziging van de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma. De aanpassing ziet erop dat voor het vorderen van toekomstige (*realtime*) verkeersgegevens een toets van de TIB plaatsvindt. In de tussentijd zou ervoor worden gezorgd dat in de praktijk al in lijn met deze wijziging wordt gehandeld. Echter, in het eerder aangehaalde arrest van *Prokuratuur* verwoordt het HvJ EU dat ook voor toegang tot *historische* verkeers- en locatiegegevens binnen de context van opsporing, een voorafgaande onafhankelijke toets is vereist. Dit uitgangspunt is door de Hoge Raad in een arrest van 5 april 2022 (ECLI:NL:HR:2022:475) voor de opsporingspraktijk bevestigd met de nodige gevolgen voor strafvordering. Oerlemans en Berlee hebben daarom in hun annotatie bij deze bepleit art. 55 Wiv 2017 op dit punt aan te passen.[22] Hoewel het te beschermen belang en daarmee het evenredigheidsbeginsel anders kan uitpakken bij de vordering van verkeers- en locatiegegevens binnen de opsporing, dan binnen de context van nationale veiligheid, is de inmenging met fundamentele rechten vergelijkbaar. Op zijn minst zou de wetgever een bredere aanpassing van art. 55 Wiv 2017 moeten overwegen, met aandacht voor eventuele gevolgen voor de werkbaarheid en eventuele gevolgen voor de capaciteit van de TIB.

Tot slot

Het arrest *La Quadrature du Net e.a.* van het HvJ EU is belangrijk geweest ten aanzien van dataretentie omdat het Hof voor het eerst aangaf welke mogelijkheden er nog wel voor bepaalde vormen van dataretentie bestaan. Het is ook belangrijk geweest voor het vaststellen van hiërarchie in de doelstellingen van algemeen belang, opsporing en nationale veiligheid. Gezien de uitkomst van het arrest van de Franse Raad van State naar aanleiding van *La Quadrature du Net e.a.* en de opvolgende arresten naar aanleiding van prejudiciële vragen in *SpaceNet AG* en *Commissioner of the Garda Síochána e.a.*, blijven lidstaten zoeken naar ruimte voor dataretentiewetgeving ten behoeve van de opsporing en vervolging van (zware) criminaliteit en geven zij tegengas op de (ervaren) inperking van hun autonomie op het gebied van nationale veiligheid.

In de meer recente arresten tracht het HvJ EU een duidelijker invulling te geven van de criteria waarbij een vorm van gerichte bewaring van verkeers- en locatiegegevens mogelijk kan zijn. Toch blijven lidstaten vragen houden over het bewaren en de toegang van verkeers- en locatiegegevens. De prejudiciële vragen van Nederland of staten zelf invulling mogen geven aan de begrippen 'ernstige strafbare feiten'/'ernstige criminaliteit'/'zware criminaliteit' is daarbij illustratief. Ook blijft onduidelijk wat precies in het nationale veiligheidsbegrip van het HvJ EU is te plaatsen, zoals de contra-inlichtingentaak van inlichtingen- en veiligheidsdiensten. De HvJ EU heeft zich in ieder geval in de loop der jaren onverzettelijk getoond ten aanzien van een algemene en ongedifferentieerde bewaarplicht en wij zijn benieuwd hoe het om zal gaan met de politieke inspanningen van lidstaten, zoals Frankrijk, die trachtten hun autonomie te bewaren.

Deze bijdrage is op persoonlijke titel geschreven.

prof. mr. dr. J.J. Oerlemans
mr. dr. M. Hagens

22 HR 5 april 2022, ECLI:NL:HR:2022:475, *Computerrecht* 2022/186, m.nt. Oerlemans en Berlee.