Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

2 March 2021 *

(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Directive 2002/58/EC – Providers of electronic communications services – Confidentiality of the communications – Limitations – Article 15(1) – Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union – Legislation providing for the general and indiscriminate retention of traffic and location data by providers of electronic communications services – Access of national authorities to retained data for the purpose of investigations – Combating of crime in general – Authorisation given by the public prosecutor's office – Use of data in criminal proceedings as evidence – Admissibility)

In Case C-746/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the Riigikohus (Supreme Court, Estonia), made by decision of 12 November 2018, received at the Court on 29 November 2018, in criminal proceedings against

H. K.,

other party:

Prokuratuur,

THE COURT (Grand Chamber),

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

Advocate General: G. Pitruzzella,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 15 October 2019,

after considering the observations submitted on behalf of:

– H. K., by S. Reinsaar, vandeadvokaat,

– the Prokuratuur, by T. Pern and M. Voogma, acting as Agents,

* Language of the case: Estonian.

– the Estonian Government, by N. Grünberg, acting as Agent,

– the Danish Government, by J. Nymann-Lindegren and M.S. Wolff, acting as Agents,

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

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

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

– the Hungarian Government, by M.Z. Fehér and A. Pokoraczki, acting as Agents,

– the Polish Government, by B. Majczyna, acting as Agent,

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

– the Finnish Government, by J. Heliskoski, acting as Agent,

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

– the European Commission, initially by H. Kranenborg, M. Wasmeier, P. Costa de Oliveira and K. Toomus, and subsequently by H. Kranenborg, M. Wasmeier and E. Randvere, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 21 January 2020,

gives the following

Judgment

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

2 The request has been made in the context of criminal proceedings brought against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings.

Legal context

EU law

3 Recitals 2 and 11 of Directive 2002/58 state:

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

…

(11) Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual’s right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950,] as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.’

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

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

The following definitions shall also apply:

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

(b) “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

…’

5 As set out in Article 5 of Directive 2002/58, headed ‘Confidentiality of the communications’:

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

…

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

6 Article 6 of Directive 2002/58, headed ‘Traffic data’, provides:

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

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

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

…

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

…'

7 Article 9 of Directive 2002/58, headed 'Location data other than traffic data', provides in paragraph 1:

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

8 Article 15 of Directive 2002/58, headed 'Application of certain provisions of Directive [95/46]', states in paragraph 1:

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

Estonian law

The Law on electronic communications

9 Paragraph 111^1 of the elektroonilise side seadus (Law on electronic communications, RT I 2004, 87, 593; RT I, 22.05.2018, 3), in the version applicable at the material time ('the Law on electronic communications'), a provision which is headed 'Obligation to retain data', states:

'…

(2) Providers of telephone and mobile telephone services and of telephone network and mobile telephone network services are obliged to retain the following data:

1) the number of the calling party and the name and address of the subscriber;

2) the number of the called party and the name and address of the subscriber;

3) when use is made of an additional service, including call forwarding or call transfer, the number dialled and the name and address of the subscriber;

4) the date and time of the start and end of the call;

5) the telephone or mobile telephone service used;

6) the International Mobile Subscriber Identity (IMSI) of the calling and called party;

7) the International Mobile Equipment Identity (IMEI) of the calling and called party;

8) the cell ID at the start of the call;

9) data on the geographical location of the base station by reference to its cell ID during the period for which data are retained;

10) in the case of pre-paid anonymous mobile telephone services, the date and time of the initial activation of the service and the cell ID from which the service was activated.

…

(4) The data referred to in subparagraphs 2 and 3 of this paragraph shall be retained for one year from the time of the communication if those data were generated or processed in the course of providing a communications service. …

…

(11) The data referred to in subparagraphs 2 and 3 of this paragraph shall be forwarded:

1) in accordance with the kriminaalmenetluse seadustik (Code of Criminal Procedure), to an investigating authority, a surveillance authority, the public prosecutor's office and the court;

…'

The Code of Criminal Procedure

10 Paragraph 17 of the Code of Criminal Procedure (kriminaalmenetluse seadustik, RT I 2003, 27, 166; RT I, 31.05.2018, 22) provides:

(1) The parties to court proceedings are the public prosecutor's office …

…'

11 Paragraph 30 of that code is worded as follows:

'(1) The public prosecutor's office shall direct the pre-trial procedure, guaranteeing its lawfulness and effectiveness, and represent the public prosecution before the court.

(2) The powers of the public prosecutor's office in criminal proceedings shall be exercised in the name of the public prosecutor's office by a public prosecutor who acts independently and is only bound by the law.'

12 Paragraph 90[1] of the code provides:

'…

(2) The investigating authority may, in the pre-trial procedure with the authorisation of the public prosecutor's office or in judicial proceedings with the authorisation of the court, ask an electronic communications undertaking for the data listed in Paragraph 111[1](2) and (3) of the Law on electronic communications which is not specified in subparagraph 1 of the present paragraph. The authorisation of the request shall note the period for which the data request is allowed with precise date indications.

(3) A request may be made pursuant to this paragraph only where this is essential for achieving the objective of the criminal proceedings.'

13 Paragraph 211 of the code states:

'(1) The objective of the pre-trial procedure is to gather evidence and create the other conditions for judicial proceedings.

(2) In the pre-trial procedure, the investigating authority and the public prosecutor's office shall ascertain the circumstances exonerating and incriminating the suspect or accused.'

The Law on the public prosecutor's office

14 Paragraph 1 of the prokuratuuriseadus (Law on the public prosecutor's office, RT I 1998, 41, 625; RT I, 06.07.2018, 20), in the version applicable at the material time, provides:

'(1) The public prosecutor's office is a government authority falling under the jurisdiction of the Ministry of Justice which participates in planning the monitoring activities necessary for fighting and investigating criminal offences, directs the pre-trial procedure, guaranteeing its lawfulness and effectiveness, represents the public prosecution before the court, and performs other duties assigned to the prosecutor's office by law.

(1[1]) The public prosecutor's office shall perform its statutory duties independently and act in accordance with the present law, other laws and legislation adopted on the basis of those laws.

…'

15 Paragraph 2(2) of that law states:

'The public prosecutor shall perform his or her duties independently and act exclusively according to the law and his or her convictions.'

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

16 By judgment of 6 April 2017, the Viru Maakohus (Court of First Instance, Viru, Estonia) imposed on H. K. a custodial sentence of two years for having committed, between 17 January 2015 and 1 February 2016, a number of thefts of goods (of a value ranging from EUR 3 to EUR 40) and cash (in amounts between EUR 5.20 and EUR 2 100), used another person's bank card, causing that person a loss of EUR 3 941.82, and performed acts of violence against persons party to court proceedings concerning her.

17 In order to find H. K. guilty of those acts, the Viru Maakohus (Court of First Instance, Viru) relied, inter alia, on several reports which were drawn up on the basis of data relating to electronic communications, as referred to in Paragraph 111^{1}(2) of the Law on electronic communications, that the investigating authority had obtained in the pre-trial procedure from a provider of electronic telecommunications services, after having been granted several authorisations for that purpose by the Viru Ringkonnaprokuratuur (Viru District Public Prosecutor's Office, Estonia) in accordance with Paragraph 90^{1} of the Code of Criminal Procedure. Those authorisations, granted on 28 January and 2 February 2015, 2 November 2015 and 25 February 2016, related to data concerning several telephone numbers of H. K. and various IMEI codes of hers, in respect of the period from 1 January to 2 February 2015, of 21 September 2015, and of the period from 1 March 2015 to 19 February 2016.

18 H. K. brought an appeal against the judgment of the Viru Maakohus (Court of First Instance, Viru) before the Tartu Ringkonnakohus (Court of Appeal, Tartu, Estonia), which dismissed the appeal by judgment of 17 November 2017.

19 H. K. lodged an appeal on a point of law against the latter judgment before the Riigikohus (Supreme Court, Estonia), contesting, inter alia, the admissibility of the reports drawn up on the basis of the data obtained from the provider of electronic communications services. In her submission, it follows from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, '*Tele2*', EU:C:2016:970), that the provisions of Paragraph 111^{1} of the Law on electronic communications which lay down the obligation on service providers to retain communications data, as well as the use of such data for the purpose of her conviction, are 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.

20 According to the referring court, the question arises whether the reports drawn up on the basis of data referred to in Paragraph 111^{1}(2) of the Law on electronic communications may be regarded as constituting admissible evidence. That court observes that the admissibility of the reports at issue in the main proceedings as evidence depends on the question of the extent to which the gathering of the data on the basis of which those reports were drawn up was in conformity 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.

21 The referring court considers that, in order to answer that question, it needs to be determined whether Article 15(1) of Directive 2002/58, read in the light of the Charter, must be interpreted as meaning that the access of State authorities to data making it possible to identify the source and destination of a telephone communication from a suspect's landline or mobile telephone, to determine the date, time, duration and type of that communication, to identify the communications equipment used and to establish the location of the mobile communication

equipment used amounts to interference with the fundamental rights at issue which is so serious that such access should be restricted to combating serious crime, regardless of the period in respect of which the State authorities have sought access to the retained data.

22 The referring court takes the view, however, that the length of that period is an essential factor for assessing the seriousness of the interference represented by access to traffic and location data. Thus, where that period is very short or the quantity of data gathered is very limited, the question should be raised whether the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference.

23 Finally, the referring court has doubts as to whether it is possible to regard the Estonian public prosecutor's office as an independent administrative authority, for the purposes of paragraph 120 of the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970), which is capable of authorising access of the investigating authority to data relating to electronic communications such as the data referred to in Paragraph 111[1](2) of the Law on electronic communications.

24 The referring court states that the public prosecutor's office directs the pre-trial procedure, while guaranteeing its lawfulness and effectiveness. Since the objective of that procedure is, inter alia, to gather evidence, the investigating authority and the public prosecutor's office verify the circumstances incriminating and exonerating any suspect or person accused. If the public prosecutor's office is satisfied that all the necessary evidence has been gathered, it brings the public prosecution against the accused. The powers of the public prosecutor's office are exercised in its name by a public prosecutor who carries out his or her duties independently, as follows from Paragraph 30(1) and (2) of the Code of Criminal Procedure and Paragraphs 1 and 2 of the Law on the public prosecutor's office.

25 In that context, the referring court observes that its doubts as to the independence required by EU law are principally attributable to the fact that the public prosecutor's office not only directs the pre-trial procedure, but also represents the public prosecution at the trial, that authority being, pursuant to national law, party to the criminal proceedings.

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

'(1) Is Article 15(1) of Directive [2002/58], in conjunction with Articles 7, 8, 11 and 52(1) of the [Charter], to be interpreted as meaning that in criminal proceedings the access of State authorities to data making it possible to establish the source and destination, the date, the time, the duration and the type of the communication, the terminal used and the location of the mobile terminal used, in relation to a telephone or mobile telephone communication of a suspect, constitutes so serious an interference with the fundamental rights enshrined in those articles of the Charter that that access in the area of prevention, investigation, detection and prosecution of criminal offences must be restricted to the fighting of serious crime, regardless of the period to which the retained data to which the State authorities have access relate?

(2) Is Article 15(1) of Directive [2002/58], on the basis of the principle of proportionality expressed in the judgment of [2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788)], paragraphs 55 to 57, to be interpreted as meaning that, if the amount of data mentioned in the first question, to which the State authorities have access, is not large (both in terms of the type of data and in terms of its temporal extent), the associated interference with fundamental

rights is justified by the objective of prevention, investigation, detection and prosecution of criminal offences generally, and that the greater the amount of data to which the State authorities have access, the more serious the criminal offences which are intended to be fought by the interference must be?

(3) Does the requirement mentioned in the judgment of [21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970)], second point of the operative part, that the data access of the competent State authorities must be subject to prior review by a court or an independent administrative authority mean that Article 15(1) of Directive [2002/58] must be interpreted as meaning that the public prosecutor's office which directs the pre-trial procedure, with it being obliged by law to act independently and only being bound by the law, and ascertains the circumstances both incriminating and exonerating the accused in the pre-trial procedure, but later represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative authority?'

Consideration of the questions referred

The first and second questions

27 By its first and second questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime, regardless of the length of the period in respect of which access to those data is sought and the quantity and the nature of the data available in respect of such a period.

28 It is apparent from the request for a preliminary ruling that, as the Estonian Government confirmed at the hearing, the data to which the national investigating authority had access in the main proceedings is the data kept under Paragraph 111^{1}(2) and (4) of the Law on electronic communications, which obliges providers of electronic communications services to retain, generally and indiscriminately, for one year traffic and location data so far as concerns fixed and mobile telephony. Those data make it possible, in particular, to trace and identify the source and destination of a communication from a person's landline or mobile telephone, to determine the date, time, duration and type of that communication, to identify the communications equipment used, and to establish the location of the mobile telephone without a communication necessarily being conveyed. In addition, they enable the frequency of a user's communications with certain persons over a given period of time to be established. Furthermore, as the Estonian Government confirmed at the hearing, access to those data may, in relation to combating crime, be sought in respect of any type of criminal offence.

29 As regards the circumstances in which access to traffic and location data retained by providers of electronic communications services may, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, be granted to public authorities, pursuant to a measure adopted under Article 15(1) of Directive 2002/58, the Court has held that such access

may be granted only in so far as those data have been retained by a provider in a manner that is consistent with Article 15(1) (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 167).

30 In this connection, the Court has also held 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, precludes legislative measures which, for such purposes, provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168).

31 As to the objectives capable of justifying public authorities having access to data retained by providers of electronic communications services pursuant to a measure consistent with those provisions, it is apparent, first, from the Court's case-law that such access may be justified only by the public interest objective for which those service providers were ordered to retain the data (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166).

32 Second, the Court has held 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 the seriousness of the interference (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131 and the case-law cited).

33 So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue in the main proceedings, 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, whether the retention be general and indiscriminate or targeted. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective, pursued by the legislation at issue in the main proceedings, of preventing, investigating, detecting and prosecuting criminal offences in general (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 140 and 146).

34 In that regard, it has inter alia been held that legislative measures concerning the processing of data in themselves relating to the civil identity of users of electronic communications systems, including the retention of and access to those data, solely for the purpose of identifying the user concerned, and without it being possible for those 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. Those data do not, in themselves, 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 they do not provide, apart from the contact details of users of means of electronic communication, such as their addresses, any information on the communications sent and, consequently, on the users' private lives. Thus, the interference entailed by a measure relating to

those data cannot, in principle, be classified as serious (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 157 and 158 and the case-law cited).

35 Accordingly, only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and that allow precise conclusions to be drawn concerning the private lives of the persons concerned (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 54), and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.

36 Access to a set of traffic or location data, such as the data retained pursuant to Paragraph 111[1] of the Law on electronic communications, is indeed liable to allow precise, or even 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 (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117).

37 It is true that, as the referring court suggests, the longer that the period is in respect of which access is sought, the greater, in principle, is the quantity of data liable to be retained by providers of electronic communications services, regarding the electronic communications sent, the places of residence stayed in and the movements made by the user of a means of electronic communication, thus allowing a greater number of conclusions concerning that user's private life to be drawn from the data consulted. A similar finding may be made so far as concerns the categories of data sought.

38 It is, therefore, for the purpose of satisfying the requirement of proportionality, under which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130 and the case-law cited), that it is for the competent national authorities to ensure, in each individual case, that both the category or categories of data covered and the period in respect of which access to those data is sought are, on the basis of the circumstances of the case, limited to what is strictly necessary for the purposes of the investigation in question.

39 However, the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that is entailed by a public authority's access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period, when, as in the main proceedings, that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned.

40 Even access to a limited quantity of traffic or location data or access to data in respect of a short period may be liable to provide precise information on the private life of a user of a means of electronic communication. Furthermore, the quantity of the data available and the specific information on the private life of the person concerned that results from the data are matters that can be assessed only after the data have been consulted. However, authorisation of access, granted by the court having jurisdiction or the competent independent authority, necessarily occurs before the data and the information resulting therefrom can be consulted. Thus, the assessment of the seriousness of the interference that the access constitutes is necessarily carried out on the basis of the risk generally pertaining to the category of data sought for the private lives of the persons concerned, without it indeed mattering whether or not the resulting information relating to the person's private life is in actual fact sensitive.

41 Finally, given the fact that the referring court has before it a claim that the reports drawn up on the basis of the traffic and location data are inadmissible, on the ground that Paragraph 111[1] of the Law on electronic communications is contrary to Article 15(1) of Directive 2002/58 as regards both retention of and access to data, it should be noted 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 criminal offences, of information and evidence obtained by general and indiscriminate retention of such data contrary to EU law (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 222) or by access of the national authorities thereto contrary to EU law.

42 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, in accordance with the principle of procedural autonomy, to establish 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 situations subject to domestic law (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) (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 223 and the case-law cited).

43 As regards the principle of effectiveness in particular, 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 (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 225).

44 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, of the right to a fair trial entailed by the admissibility of such information and evidence. 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 that 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 in order to avoid such an infringement. 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 or by means of access of the competent authority thereto 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 (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 226 and 227).

45 In the light of the foregoing considerations, the answer to the first and second questions is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.

The third question

46 By its third question, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

47 The referring court explains in this connection that, whilst the Estonian public prosecutor's office is, under national law, obliged to act independently, is subject only to the law and must examine the incriminating and exculpatory evidence in the pre-trial procedure, the objective of that procedure nevertheless remains the gathering of evidence and fulfilment of the other conditions necessary for judicial proceedings. It states that it is that authority which represents the public prosecution at the trial and it is therefore also party to the proceedings. Furthermore, it is apparent from the documents before the Court that, as the Estonian Government and the Prokuratuur also confirmed at the hearing, the Estonian public prosecutor's office is organised hierarchically and that requests for access to traffic and location data are not subject to particular formal requirements and may be made by the public prosecutor him or herself. Finally, the persons to whose data access may be granted are not only those suspected of involvement in a criminal offence.

48 It is true that, as the Court has already held, it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality, such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and 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 (see, to that effect, judgments of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 117 and 118; of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 68; and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

49 In particular, national legislation governing the access of the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgments of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 77, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 176 and the case-law cited).

50 Accordingly, and since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities (see, to that effect, judgments of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 188).

51 In order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189 and the case-law cited).

52 As the Advocate General has observed, in essence, in point 105 of his Opinion, one of the requirements for that prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access.

53 Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence (see, to that effect, judgment of 9 March 2010, *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 25, and Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraphs 229 and 230).

54 It follows from the foregoing considerations that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review referred to in paragraph 51 of the present judgment means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field, as the Advocate General has observed, in essence, in point 126 of his Opinion, the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings.

55 That is not so in the case of a public prosecutor's office which directs the investigation procedure and, where appropriate, brings the public prosecution. The public prosecutor's office has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of putting it, where appropriate, before the court that has jurisdiction.

56 The fact that the public prosecutor's office may, in accordance with the rules governing its powers and status, be required to verify the incriminating and exculpatory evidence, to guarantee the lawfulness of the pre-trial procedure and to act exclusively according to the law and the prosecutor's convictions cannot be sufficient to confer upon it the status of a third party in relation to the interests at issue as referred to in paragraph 52 of the present judgment.

57 It follows that the public prosecutor's office is not in a position to carry out the prior review referred to in paragraph 51 of the present judgment.

58 Since the referring court has raised, furthermore, the issue whether the lack of a review by an independent authority may be made up for by a subsequent review carried out by a court as to whether a national authority's access to traffic and location data was lawful, it must be pointed out that, as required by the case-law recalled in paragraph 51 of the present judgment, the independent review must take place before any access, except in the event of duly justified urgency, in which case the review must take place within a short time. As the Advocate General has stated in point 128 of his Opinion, such subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met.

59 Accordingly, the answer to the third question referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

Costs

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

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

1. **Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.**

2. **Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.**

[Signatures]