Provisional text

JUDGMENT OF THE COURT (Grand Chamber)

30 April 2024 (*)

(Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Confidentiality of communications – Providers of electronic communications services – Directive 2002/58/EC – Article 15(1) – Articles 7, 8, 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union – Access to those data requested by a national authority having competence to prosecute offences of aggravated theft – Definition of the concept of 'serious offence' the prosecution of which is capable of justifying serious interference with fundamental rights – Competence of the Member States – Principle of proportionality – Scope of prior review by a court of the requests to access the data retained by providers of electronic communications services)

In Case C-178/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Giudice delle indagini preliminari presso il Tribunale di Bolzano (the judge in charge of preliminary investigations at the District Court, Bolzano, Italy), made by decision of 20 February 2022, received at the Court on 8 March 2022, in the criminal proceedings

Unknown individuals,

joined party:

Procura della Repubblica presso il Tribunale di Bolzano,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, A. Prechal, K. Jürimäe, T. von Danwitz and Z. Csehi, Presidents of Chambers, J.-C. Bonichot, S. Rodin, P.G. Xuereb (Rapporteur), D. Gratsias, M.L. Arastey Sahún and M. Gavalec, Judges,

Advocate General: A.M. Collins,

Registrar: C. Di Bella, Administrator,

having regard to the written procedure and further to the hearing on 21 March 2023,

after considering the observations submitted on behalf of:

– the Procura della Repubblica presso il Tribunale di Bolzano, by F. Iovene, sostituto procuratore della Repubblica,

– the Italian Government, by G. Palmieri, acting as Agent, and by S. Faraci, avvocato dello Stato,

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

– the Estonian Government, by M. Kriisa, acting as Agent,

– Ireland, by M. Browne, Chief State Solicitor, A. Joyce and M. Tierney, acting as Agents, and by D. Fennelly, Barrister-at-Law,

– the French Government, by A. Daniel, A.-L. Desjonquères, B. Fodda and J. Illouz, acting as Agents,

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

– the Hungarian Government, by Zs. Biró-Tóth and M.Z. Fehér, acting as Agents,

– the Netherlands Government, by M.K. Bulterman, A. Hanje and J. Langer, acting as Agents,

– the Austrian Government, by A. Posch, J. Schmoll, C. Gabauer, K. Ibili and E. Samoilova, acting as Agents,

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

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

after hearing the Opinion of the Advocate General at the sitting on 8 June 2023,

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, 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 a referral to the Giudice delle indagini preliminari presso il Tribunale di Bolzano (the judge in charge of preliminary investigations at the

District Court, Bolzano, Italy) by the Procura della Repubblica presso il Tribunale di Bolzano (Public Prosecutor's Office at the District Court, Bolzano, Italy) ('the Public Prosecutor's Office'), seeking authorisation from that judge in order to access personal data retained by providers of electronic communications services, with a view to identifying the perpetrators of two acts of aggravated theft of a mobile telephone.

Legal context

European Union law

Directive 2002/58

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 Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the 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 Under Article 2 of that directive, headed 'Definitions':

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

The following definitions shall also apply:

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

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

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

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

…’

5 Article 5 of Directive 2002/58, entitled ‘Confidentiality of the communications’, provides:

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

…

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

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

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

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

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

…

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

…'

7 Article 9 of Directive 2002/58, entitled '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 that directive, entitled 'Application of certain provisions of Directive [95/46]', states, in paragraph 1 thereof:

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

Italian law

Legislative Decree No 196/2003

9 Article 132(3) of decreto legislativo n. 196 – Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/EC (Legislative Decree No 196 establishing the Personal Data Protection Code, laying down provisions for the adaptation of national law to 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) of 30 June 2003 (Ordinary Supplement to GURI No 174 of 29 July 2003), in the version applicable to the dispute in the main proceedings ('Legislative Decree No 196/2003'), provides as follows:

‘Within the retention period laid down by law, if there is sufficient evidence of the commission of an offence for which the law prescribes the penalty of life imprisonment or a maximum term of imprisonment of at least three years, determined in accordance with Article 4 of the [codice di procedura penale [(Code of Criminal Procedure)], or of an offence of threatening and harassing or disturbing persons by means of the telephone, where the threat, harassment or disturbance is serious, the data may, if relevant to establishing the facts, be acquired with the prior authorisation of the court, by way of reasoned order, at the request of the Public Prosecutor’s Office or upon an application by the legal representative of the accused, of the person under investigation, of the injured party or of any other private party.’

10 Article 132(3*bis*) of Legislative Decree No 196/2003 provides:

‘Where there are reasons of urgency and reasonable grounds for believing that the delay could result in serious investigative difficulties, the Public Prosecutor’s Office is to order the acquisition of the data by reasoned decision, which shall be communicated immediately, or within 48 hours at the latest, to the court having jurisdiction to grant authorisation in the ordinary way. The court shall, within 48 hours of receipt thereof, adopt a decision on confirmation by way of reasoned order.’

11 Lastly, under Article 132(3*quater*) of that legislative decree, ‘No use may be made of data acquired in breach of the provisions of paragraph 3 or paragraph 3*bis*.’

Criminal Code

12 Article 624 of the codice penale (Criminal Code), entitled ‘Theft’, provides:

‘A person who takes movable property belonging to another, thereby depriving the holder of that property, with a view to making a profit for him or herself or for another shall be liable to imprisonment of between six months and three years and a fine of between EUR 154 and EUR 516.

…

The offence shall be punishable on foot of a complaint by the injured party, unless one or more of the conditions referred to in Article 61(7) and Article 625 are met.’

13 The first paragraph of Article 625 of the Criminal Code, entitled ‘Aggravating circumstances’, provides:

‘The offence referred to in Article 624 shall be punishable by a term of imprisonment of between two and six years and a fine of between EUR 927 and EUR 1 500:

…

(2) if the guilty person uses violence against property or makes use of any fraudulent means;

(3) if the guilty person is carrying weapons or drugs without using them;

(4) in the case of pickpocketing;

(5) if the offence is committed by three or more persons, or by a single person, disguised as or posing as a public officer or a person exercising a public function;

(6) if the offence relates to travellers' luggage in any vehicle, station, airport or on any platform, or in any hotel or any establishment selling food or beverages;

(7) if the offence relates to property present in public offices or establishments, or confiscated or seized, or exposed by necessity or custom or for the purposes of public faith, or intended for public service or public benefit, defence or veneration;

(7*bis*) if the offence relates to metal components or other materials removed from infrastructure intended for the supply of energy, transport, telecommunications or other public services and operated by public or private entities under a public concession;

(8) if the offence relates to three or more heads of cattle in a herd, or to bovine or equine animals, whether or not present in a herd;

(8*bis*) if the offence is committed on public transport;

(8*ter*) if the offence is committed against a person who is using or has just used the services of a credit institution, a post office or an automated teller machine.'

The Code of Criminal Procedure

14 Under Article 4 of the Code of Criminal Procedure, entitled 'Rules for determining jurisdiction':

'The court's jurisdiction shall be determined by considering the penalty imposed by the law for each completed or attempted offence. Continuing offences, recidivism and the circumstances in which the offence is committed shall not be considered, except for aggravating circumstances for which the law sets a type of penalty other than the ordinary penalty for the offence and those having special effect.'

15 Article 269(2) of that code provides:

'… the recordings shall be kept until final judgment is delivered. However, in order to protect confidentiality, the interested parties may, where the documents are not necessary for the purposes of the proceedings, request the judge who authorised or validated the interception to destroy the recordings that have not been included in the file.'

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

16 Following two complaints lodged in respect of acts of mobile phone theft committed on 27 October and 20 November 2021 respectively, the Public Prosecutor's Office brought two sets of criminal proceedings, under Articles 624 and 625 of the Criminal Code, against unknown perpetrators for the commission of offences of aggravated theft.

17 In order to identify the perpetrators of those thefts, the Public Prosecutor's Office requested, on the basis of Article 132(3) of Legislative Decree No 196/2003, on 7 December and 30 December 2021 respectively, from the Giudice delle indagini preliminari presso il Tribunale di Bolzano (judge responsible for preliminary investigations at the District Court, Bolzano), the referring court, authorisation to obtain from all the telephone companies the telephone records of the stolen telephones. Those requests concerned 'all the data in [the possession of the telephone companies], with tracking and localisation methods (in particular, users and possible [International Mobile

Equipment Identity (IMEI)] codes called/callers, sites visited/reached, times and durations of calls/connections and details of the cells and/or towers concerned, users and IMEI codes of senders/receivers of SMS and MMS and, where possible, details of the holders concerned) of incoming and outgoing telephone conversations/communications and connections made, including under roaming and including those not billed (unanswered calls) from the date of the theft to the date the request is processed'.

18 The referring court is uncertain whether Article 132(3) of Legislative Decree No 196/2003 is compatible with Article 15(1) of Directive 2002/58 as interpreted by the Court in its judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152).

19 The referring court recalls that, in accordance with paragraph 45 of that judgment, national provisions that permit public authorities to have access to telephone records, containing a set of traffic or location data that are liable to allow precise conclusions to be drawn concerning the private life of the user concerned, are justifiable – having regard to the principle of proportionality laid down in Article 52(1) of the Charter and the seriousness of the interference with the fundamental rights to private life, the protection of personal data and freedom of expression and information, as guaranteed, respectively, in Articles 7, 8 and 11 of the Charter – only if those provisions are intended for the prosecution of serious offences, such as serious threats to public security, understood as that of the State, and other serious crime.

20 In that regard, the referring court states that, in its judgment No 33116 of 7 September 2021, the Corte suprema di cassazione (Supreme Court of Cassation, Italy) held that, having regard to the margin of interpretation concerning the determination of offences constituting serious threats to public security or other forms of serious crime within the meaning of the Court's case-law, that case-law did not have the characteristics required for it to be applied directly by the national courts. Consequently, the Italian legislature amended Article 132(3) of Legislative Decree No 196/2003 in order to classify as serious offences, for which telephone records may be obtained, offences which are punishable by law by a maximum term of imprisonment 'of at least three years'.

21 According to the referring court, that three-year minimum period above which the maximum term of imprisonment for an offence justifies that that offence can give rise to disclosure of telephone records to the public authorities is such that those records could be disclosed to them in order to prosecute offences which cause only a limited social disturbance and which are punishable only on foot of a complaint by a private party, in particular low-value thefts such as mobile phone or bicycle theft.

22 In that court's view, the national provision at issue would thus fail to observe the principle of proportionality laid down in Article 52(1) of the Charter, which requires the seriousness of the offence being prosecuted to be weighed against the fundamental rights which are infringed in order to prosecute that offence. That principle of proportionality would preclude an infringement of the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter from being justified by the prosecution of an offence such as theft.

23 The referring court states that Italian courts have a very limited margin of discretion to refuse authorisation to obtain telephone records since, pursuant to the provision at issue, authorisation must be granted where there is 'sufficient evidence of the commission of an offence' and the data requested are 'relevant to establishing the facts'. The Italian courts have, therefore, no margin of discretion as to the actual seriousness of the offence under investigation. That assessment was definitively carried out by the Italian legislature when it laid down that the authorisation to obtain

data had to be granted in respect, inter alia, of all offences punishable by a maximum term of imprisonment of at least three years.

24 In those circumstances the Giudice delle indagini preliminari presso il Tribunale di Bolzano (judge responsible for preliminary investigations at the District Court, Bolzano) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

'Does Article 15(1) of Directive [2002/58] preclude a provision of national law such as that contained in Article 132[(3)] of Legislative Decree [No 196/2003], … [which] … provides:

"3. Within the retention period laid down by law, if there is sufficient evidence of the commission of an offence for which the law prescribes the penalty of life imprisonment or a maximum term of imprisonment of at least three years, determined in accordance with Article 4 of the Code of Criminal Procedure, or of an offence of threatening and harassing or disturbing persons by means of the telephone, where the threat, harassment or disturbance is serious, the data may, if relevant to establishing the facts, be acquired with the prior authorisation of the court, by way of reasoned order, at the request of the Public Prosecutor's Office or upon an application by the legal representative of the accused, of the person under investigation, of the injured party or of any other private party"?'

Admissibility of the request for a preliminary ruling

25 The Italian Government and Ireland submit that the request for a preliminary ruling is in part inadmissible. They note that the requests for access to the data retained by providers of electronic communications services were submitted by the Public Prosecutor's Office, on the basis of Article 132(3) of Legislative Decree No 196/2003, in order to prosecute offences of aggravated theft of mobile telephones. However, by its question, the referring court also asks the Court whether Article 15(1) of Directive 2002/58 precludes a national provision allowing access to data retained by providers of electronic communications services, in order to prosecute offences falling within the scope of Article 132(3) of Legislative Decree No 196/2003 other than those at issue in the main proceedings, such as simple theft or serious harassment by telephone. Accordingly, the request for a preliminary ruling is hypothetical in so far as it relates to those other offences.

26 In that regard, it should be noted that, according to settled case-law, in the context of the cooperation between the Court and the national courts provided for in Article 267 TFEU, it is solely for the national court before which a dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions submitted by the national court concern the interpretation of EU law, the Court is, in principle, bound to give a ruling (judgment of 21 March 2023, *Mercedes-Benz Group (Liability of manufacturers of vehicles fitted with defeat devices)*, C-100/21, EU:C:2023:229, paragraph 52 and the case-law cited).

27 It follows that questions relating to EU law enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 21 March 2023, *Mercedes-Benz Group (Liability of manufacturers of vehicles fitted with defeat devices)*, C-100/21, EU:C:2023:229, paragraph 53 and the case-law cited).

28 As it is, by reproducing in full Article 132(3) of Legislative Decree No 196/2003, the question referred for a preliminary ruling, even though it fails to distinguish between the types of offences to which that provision applies, necessarily encompasses the offences of aggravated theft for which the requests for access to personal data were submitted in the main proceedings.

29 Accordingly, that question is not hypothetical and is, therefore, admissible.

Consideration of the question referred

30 As the French Government stated in its written observations, the question referred by the national court, as worded, invites the Court to rule on the compatibility of Article 132(3) of Legislative Decree No 196/2003 with Article 15(1) of Directive 2002/58.

31 In that regard, it should be borne in mind that, in the context of the procedure established by Article 267 TFEU, the Court has no jurisdiction to rule on the interpretation of provisions of national laws or regulations or on their conformity with EU law. It is settled case-law that, in a request for a preliminary ruling pursuant to Article 267 TFEU, the Court may interpret EU law only within the parameters of the jurisdiction conferred on the European Union (judgment of 14 December 2023, *Getin Noble Bank (Limitation period for actions for restitution)*, C-28/22, EU:C:2023:992 paragraph 53 and the case-law cited).

32 That said, it is settled case-law that, if questions have been improperly formulated or if they go beyond the scope of the powers conferred on the Court by Article 267 TFEU, the Court is free to extract from all the information provided by the referring court and, in particular, from the statement of grounds in the order for reference the elements of EU law which, having regard to the subject matter of the dispute, require interpretation. To that end, the Court may have to reformulate the questions referred to it (judgment of 14 December 2023, *Sparkasse Südpfalz*, C-206/22, EU:C:2023:984, paragraph 20 and the case-law cited).

33 Furthermore, the Court may decide to take into consideration rules of EU law to which the national court has made no reference in the wording of its question (judgment of 17 November 2022, *Harman International Industries*, C-175/21, EU:C:2022:895, paragraph 31 and the case-law cited).

34 In the light of the foregoing, it must be held that by its question the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as precluding a national provision which requires a national court, acting in the context of a prior review carried out following a reasoned request for access to a set of traffic or location data – which are liable to allow precise conclusions to be drawn concerning the private life of a user of a means of electronic communication and are retained by providers of electronic communications services – submitted by a competent national authority in the context of a criminal investigation, to authorise that access if it is requested for the purposes of investigating criminal offences punishable under national law by a maximum term of imprisonment of at least three years, provided that there is sufficient evidence of the commission of such offences and that those data are relevant to establishing the facts.

35 As a preliminary point, it should be borne in mind that, 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 legislative 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 those providers in a manner consistent with that directive (see, to that effect, judgment of today's date, *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)*, C-470/21, paragraph 65 and the case-law cited). 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 (judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 30 and the case-law cited).

36 It is also appropriate to recall the case-law of the Court according to which only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, arising from public authorities' access to a set of traffic or location data, which 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 which allow precise conclusions to be drawn concerning the private lives of the persons concerned; 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 (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 35 and the case-law cited).

37 By its question, the referring court seeks, in essence, to ascertain whether such a serious interference may be authorised for offences such as those referred to in the national legislation at issue in the main proceedings.

38 As regards, first of all, the question of whether access such as that at issue in the main proceedings may be classified as serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, it should be noted that, in order to identify the perpetrators of the alleged thefts which gave rise to those proceedings, the Public Prosecutor's Office requested, for each of the mobile telephones concerned, authorisation from the referring court – on the basis of Article 132(3) of Legislative Decree No 196/2003 – to collect all the data in the possession of the telephone companies, obtained by means of tracking or localisation methods, concerning the telephone conversations and communications and the connections made with those telephones. More specifically, those requests concerned the users and IMEI codes of the devices called or making the calls, the sites visited and reached, the times and durations of calls and connections, the details of the cells and/or towers concerned, as well as the users and IMEI codes of senders/receivers of SMS and MMS.

39 Access to such a set of traffic or location data appears liable to allow precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152 paragraph 36 and the case-law cited). The interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter caused by access to such data therefore appears likely to be classified as serious.

40 As is apparent from paragraph 39 of the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), that

assessment cannot be rejected solely because the two requests for access to the traffic or location data at issue concerned only short periods, of less than two months, from the dates of the alleged thefts of the mobile telephones to the dates on which those requests were drafted, since those requests related to a set of such data liable to provide precise information concerning the private lives of the persons using the mobile telephones concerned.

41 Similarly, for the purposes of assessing the existence of a serious interference with the rights guaranteed in Articles 7 and 8 of the Charter, the fact that the data to which the Public Prosecutor's Office requested access may not be the data of the owners of the mobile telephones at issue, but the data of the persons who communicated with each other by using those telephones after their alleged theft, is irrelevant. Indeed, it is apparent from Article 5(1) of Directive 2002/58 that the obligation of principle to ensure the confidentiality of the electronic communications and the related traffic data effected by means of a public communications network and publicly available electronic communications services covers communications made by the users of that network. Article 2(a) of that directive defines the concept of 'user' as meaning any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service.

42 Consequently, in the light of the case-law cited in paragraph 36 above, since the interferences with fundamental rights caused by access to data, such as those at issue in the main proceedings, are liable to be regarded as serious, they can be justified only by the objectives of combating serious crime or preventing serious threats to public security.

43 Next, while it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in those providers' possession, such legislation must lay down clear and precise rules governing the scope and conditions for the application of such access. 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 being implicated in a serious crime. In order to ensure, in practice, that those conditions ensuring that the interference is limited to what is strictly necessary are fully observed, it is essential that access of the competent national authorities to retained data be subject, except in cases of duly justified urgency, to a prior review carried out either by a court or by an independent administrative body (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraphs 48 to 51).

44 As regards, lastly, the definition of the concept of 'serious offence', it is apparent from the case-law that, in so far as the European Union has not legislated in that field, criminal legislation and the rules of criminal procedure fall within the competence of the Member States. They must, however, exercise that competence in line with EU law (see, to that effect, judgment of 26 February 2019, *Rimšēvičs and ECB* v *Latvia*, C-202/18 and C-238/18, EU:C:2019:139, paragraph 57 and the case-law cited).

45 In that regard, it should be noted that the definition of criminal offences, mitigating and aggravating circumstances and penalties reflects both social realities and legal traditions, which vary not only between the Member States but also over time. However, those realities and traditions are of undoubted importance in determining which offences are considered to be of a serious nature.

46 Consequently, in view of the division of competences between the European Union and the Member States under the FEU Treaty and the considerable differences between the legal systems of the Member States in the area of criminal law, it must be found that it is for the Member States to define 'serious offences' for the purposes of applying Article 15(1) of Directive 2002/58.

47 However, the definition of ‘serious offences’, adopted by the Member States, must comply with the requirements arising from Article 15(1) of that directive, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

48 It should be borne in mind, in that regard, that, in so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that ‘restrict the scope’ of the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of that directive – such as those arising from the principles of confidentiality of communications and the prohibition on storing related data – that provision provides for an exception to the general rule laid down, in particular, in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. Such a provision, therefore, cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto to become the rule, if Article 5 of Directive 2002/58 is not to be rendered largely meaningless (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 40).

49 Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States under that provision must comply with the general principles of EU law, which include the principle of proportionality, and ensure respect for the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 42).

50 It follows that the Member States cannot distort the concept of ‘serious offence’ and, by extension, that of ‘serious crime’, by including within it, for the purposes of applying Article 15(1), offences which are manifestly not serious offences, in the light of the societal conditions prevailing in the Member State concerned, even though the legislature of that Member State has provided for such offences to be punishable by a maximum term of imprisonment of three years.

51 It is in particular in order to ascertain that there is no such distortion that it is essential that, where access by the competent national authorities to retained data carries the risk of a serious interference with the fundamental rights of the person concerned, that access be subject to a prior review carried out either by a court or by an independent administrative body (see, to that effect, judgment of today’s date, *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)*, C-470/21, paragraphs 124 to 131).

52 In the present case, it is apparent from the order for reference that Article 132(3) of Legislative Decree No 196/2003 lays down the conditions under which access to data retained by providers of electronic communications services may be granted by a court hearing a reasoned request from a public authority. That provision defines the offences, for the prosecution of which access to data retained by providers of electronic communications services may be granted, by reference to a maximum term of imprisonment of at least three years. It makes that access subject to the twofold condition that there must be ‘sufficient evidence of the commission of an offence’ and that those data be ‘relevant to establishing the facts’.

53 The referring court is, however, uncertain whether the definition of ‘serious offences’, for the prosecution of which access to data may be granted, resulting from that provision, is too broad since it covers offences which cause only a limited social disturbance.

54 In that regard, it should be noted, first, that a definition according to which ‘serious offences’, for the prosecution of which access to data may be granted, are those for which the maximum term of imprisonment is at least equal to a period determined by law, is based on an objective criterion.

That is consistent with the requirement that 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 (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 105 and the case-law cited).

55 Secondly, it follows from the case-law cited in paragraph 48 above that the definition given, in national law, of 'serious offences' that may allow access to data retained by providers of electronic communications services, allowing precise conclusions to be drawn concerning the private lives of the persons concerned, must not be so broad that access to those data becomes the rule rather than the exception. Thus, that definition cannot cover the vast majority of criminal offences, which would be the case if the minimum period above which the maximum term of imprisonment for an offence justifies its classification as a serious offence were set at an excessively low level.

56 A minimum period fixed by reference to a maximum term of imprisonment of three years does not appear, in that regard, to be excessively low (see, to that effect, judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 150).

57 Admittedly, since the definition of 'serious offences', in respect of which access to data retained by electronic communications service providers may be requested, is established by reference not to a minimum applicable penalty but to a maximum applicable penalty, it cannot be excluded that access to data, constituting a serious interference with fundamental rights, may be requested for the purposes of prosecuting offences which do not, in actual fact, constitute serious crime (see, by analogy, judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 151).

58 Setting a minimum period above which the maximum term of imprisonment for an offence justifies the classification of that offence as a serious offence is not, however, necessarily contrary to the principle of proportionality.

59 First, this appears to be the case of a provision such as that at issue in the main proceedings, since, as is apparent from the order for reference, that provision refers in a general manner to access to data retained by providers of electronic communications services, without specifying the nature of those data. Thus, that provision appears to cover, inter alia, cases in which access cannot be classified as a serious interference, since it does not relate to a set of data liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned.

60 Secondly, the court or independent administrative body, acting in the context of a prior review carried out following a reasoned request for access, must be entitled to refuse or restrict that access where it finds that the interference with fundamental rights which such access would constitute is serious even though it is clear that the offence at issue does not actually constitute serious crime (see, by analogy, judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 152).

61 Indeed, the court or body entrusted with carrying out the review must be able to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation in the context of combating crime and, on the other hand, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of today's date, *La Quadrature du Net and Others (Personal data and combating counterfeiting)*, C-470/21, paragraph 125 and the case-law cited).

62 In particular, as part of its examination of the proportionality of the interference with the fundamental rights of the person concerned caused by the request for access, that court or body must be able to exclude such access where it is sought in the context of proceedings for an offence which is manifestly not a serious offence, within the meaning of paragraph 50 above.

63 It follows from the foregoing that the answer to the question referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding a national provision which requires a national court, acting in the context of a prior review carried out following a reasoned request for access to a set of traffic or location data – which are liable to allow precise conclusions to be drawn concerning the private life of a user of a means of electronic communication and retained by providers of electronic communications services – submitted by a competent national authority in the context of a criminal investigation, to authorise such access if it is requested for the purposes of investigating criminal offences punishable under national law by a maximum term of imprisonment of at least three years, provided that there is sufficient evidence of the commission of such offences and that those data are relevant to establishing the facts, on condition, however, that that court is entitled to refuse such access if it is requested in the context of an investigation into an offence which is manifestly not a serious offence, in the light of the societal conditions prevailing in the Member State concerned.

Costs

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

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

Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union,

must be interpreted as not precluding a national provision which requires a national court, acting in the context of a prior review carried out following a reasoned request for access to a set of traffic or location data – which are liable to allow precise conclusions to be drawn concerning the private life of a user of a means of electronic communication and retained by providers of electronic communications services – submitted by a competent national authority in the context of a criminal investigation, to authorise such access if it is requested for the purposes of investigating criminal offences punishable under national law by a maximum term of imprisonment of at least three years, provided that there is sufficient evidence of the commission of such offences and that those data are relevant to establishing the facts, on condition, however, that that court is entitled to refuse such access if it is requested in the context of an investigation into an offence which is manifestly not a serious offence, in the light of the societal conditions prevailing in the Member State concerned.

[Signatures]

* Language of the case: Italian.