Reports of Cases

OPINION OF ADVOCATE GENERAL
COLLINS
delivered on 8 June 2023 [1]

Case C-178/22

Unknown individuals
joined party:
Procura della Repubblica presso il Tribunale di Bolzano

(Request for a preliminary ruling from the Tribunale di Bolzano (District Court, Bolzano, Italy))

(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 1(3) and Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Request by a public prosecutor for access to data for the investigation and prosecution of aggravated theft of a mobile telephone – Definition of 'serious crime' capable of justifying serious interference with fundamental rights – Scope of prior review to ensure compliance with the requirement of the commission of a serious crime – Principle of proportionality)

I. Introduction

1. The Procura della Repubblica presso il Tribunale di Bolzano (Public Prosecutor's Office at the District Court, Bolzano, Italy) ('the Public Prosecutor (Bolzano)') requests the Tribunale di Bolzano (District Court, Bolzano, Italy) to authorise access to data retained by providers of electronic communications services pursuant to national law that make it possible, inter alia, to trace and identify the source and destination of communications from mobile telephones.

2. In the context of that request the Tribunale di Bolzano (District Court, Bolzano) asks the Court of Justice to interpret Article 15(1) of Directive 2002/58/EC. [2] That provision enables the Member States to introduce legislative exceptions to the obligation, laid down in that directive, [3] to ensure the confidentiality of electronic communications. In the judgment in *Prokuratuur*, [4] the Court held that access to data that enables precise conclusions to be drawn concerning a user's private

[1] Original language: English.

[2] Directive 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).

[3] See Article 5 of Directive 2002/58. The protection of confidentiality of electronic communications which Article 5(1) of Directive 2002/58 guarantees applies to measures taken by all persons other than users, whether public or private. Judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraph 36 and the case-law cited).

[4] Judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152; 'the judgment in *Prokuratuur*').

life, pursuant to measures adopted under Article 15(1) of Directive 2002/58, constitutes a serious interference with the fundamental rights and principles enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').[5] Such access may not be authorised for the purposes of the prevention, investigation, detection and prosecution of 'criminal offences in general'. It may be granted only in procedures and proceedings to combat 'serious crime'[6] and must be the subject of a prior review by a court or independent administrative body in order to ensure compliance with that requirement.[7] The Tribunale di Bolzano (District Court, Bolzano) asks the Court to clarify two aspects of the judgment in *Prokuratuur*: the concept of 'serious crime' and the scope of the prior review that a court must carry out under a provision of national law that requires it to authorise access to data retained by providers of electronic communications services.

II. Legal framework

A. European Union law

3. 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). …

…'

4. Article 6 of Directive 2002/58, entitled 'Traffic data', states:

'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).

…

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.

[5] Irrespective 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 that period.

[6] Or to prevent serious threats to public security. See the judgment in *Prokuratuur*, paragraphs 35, 39 and 45. See also judgments of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraph 56), 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 140).

[7] The judgment in *Prokuratuur*, paragraphs 48 to 52.

…’

5. Article 9 of Directive 2002/58, entitled ‘Location data other than traffic data’, provides:

‘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. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

…’

6. Article 15(1) of Directive 2002/58 is in the terms following:

‘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/EC[8]. 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) of the Treaty on European Union.’

B. National law

7. Article 132(3) of decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (Legislative Decree No 196, establishing the Personal Data Protection Code) of 30 June 2003,[9] as recently amended by Article 1 of decreto-legge 30 settembre 2021 n. 132 – Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP, convertito con modificazioni nella legge 23 novembre 2021 n. 178 (Decree-Law No 132 of 30 September 2021,[10] converted, with amendments, into Law No 178 of 23 November 2021)[11] (‘Article 132(3) of Legislative Decree No 196/2003’) provides:

‘3. Within the retention period laid down by law [that is, 24 months from the date of the communication], 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

[8] Directive 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).

[9] Ordinary Supplement No 123 to GURI No 174 of 29 July 2003, p. 11.

[10] GURI No 234 of 30 September 2021, p. 1.

[11] GURI No 284 of 29 November 2021, p. 1.

3 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 or disturbance is serious, the data are, if relevant to establishing the facts, acquired with the prior authorisation of the court, by way of reasoned order, at the request of the Public Prosecutor 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;

…

3c. No use may be made of data acquired in breach of the provisions of paragraph 3 or paragraph 3a.'

8. Under Article 4 of the Code of Criminal Procedure, entitled 'Rules for determining competence':

'The court's competence 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.'

9. According to the referring court, the Public Prosecutor may prosecute the offence of aggravated theft *ex officio*.[12] Under Article 625 of the Codice penale (Criminal Code), a person guilty of aggravated theft is liable to a special penalty of a term of imprisonment of two to six years and a fine of between EUR 927 and EUR 1 500. Article 624 of the Criminal Code provides that a person guilty of simple theft, which may be prosecuted on foot of a complaint by the injured party, is liable to a term of imprisonment of between six months and three years and a fine of between EUR 154 and EUR 516.

III. The disputes in the main proceedings and the question referred for a preliminary ruling

10. The Public Prosecutor (Bolzano) brought two sets of criminal proceedings against unknown perpetrators for the aggravated theft of a mobile phone pursuant to Articles 624 and 625 of the Criminal Code.[13] In order to trace the perpetrators, he applied to the referring court pursuant to Article 132(3) of Legislative Decree No 196/2003 for '… authorisation to obtain from all telephone companies all the data in their possession, with tracking and localisation methods (in particular, users and possible IMEI codes called/callers, sites visited/reached, times and durations of calls/connections and details of the cells and/or towers concerned, users and IMEIs 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'.

[12] Italian law classifies the thefts under investigation before the referring court as 'aggravated'.

[13] The first theft was committed on 27 October 2021 (reference number RGNR 9228/2021). The second took place on 20 November 2021 (reference number RGNR 9794/2021). The thefts of the mobile telephones occurred in Bolzano and the owners of the telephones reported them to the Carabinieri (Police).

11. The referring court doubts whether Article 132(3) of Legislative Decree No 196/2003 is compatible with Article 15(1) of Directive 2002/58 as interpreted in the judgment in *Prokuratuur*. It observes that, on 7 September 2021, the Corte suprema di cassazione (Supreme Court of Cassation, Italy) [14] held that since national courts enjoy a margin of discretion in determining what offences constitute 'serious threats to national security and serious crime', the judgment in *Prokuratuur* was not directly applicable by national courts. In the wake of the judgment of the Corte suprema di cassazione (Supreme Court of Cassation), the Italian legislature adopted Decree-Law No 132 of 30 September 2021, Article 132(3) of which classifies serious criminal offences for the purposes of obtaining telephone records as, inter alia, offences punishable by law for 'a maximum term of imprisonment of at least three years …'.

12. According to the referring court, the threshold for the classification of serious criminal offences under Article 132(3) of Legislative Decree No 196/2003 brings within its ambit offences that cause limited social disturbance and which may be prosecuted only pursuant to a complaint by an individual. [15] Access to telephone records may thus be obtained pursuant to that provision for the theft of an item of minimal value, such as a mobile telephone or a bicycle. The threshold laid down in Article 132(3) of Legislative Decree No 196/2003 accordingly fails to respect the principle of proportionality in accordance with Article 52(1) of the Charter, which requires that, in every case, the seriousness of the offence under investigation must be weighed against a limitation of the enjoyment of a fundamental right. The prosecution of such minor offences does not justify placing limits on the enjoyment of the fundamental rights to respect for private life, the protection of personal data and freedom of expression and information. [16]

13. The referring court explains that Italian courts have a very limited margin of discretion to refuse to authorise access to telephone records, since authorisation must be granted where there is 'sufficient evidence of the commission of an offence' and such authorisation is 'relevant to establishing [the facts]'. The courts have, in particular, no jurisdiction to evaluate the seriousness of the offence under investigation. The legislature carried out that assessment when it provided, in general terms and without differentiating between various types of offences, that access to telephone records must be granted in respect, inter alia, of the investigation of all offences punishable by a maximum term of imprisonment of at least three years.

14. In those circumstances, the Tribunale di Bolzano (District Court, Bolzano) decided to stay the proceedings and to refer the following question to the Court 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:

"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 or disturbance is serious, the data may, if relevant to

[14] Cass. Pen. Sez. II, n. 33116, ud. 7.9.2021, est. Pellegrino.

[15] According to the referring court 'that is the case, for example, with the offence of violation of the home, punishable under Article 614 of the Criminal Code with a term of imprisonment of between one and four years. Other offences, the maximum legal penalties for which are such as not to preclude the obtaining of telephone records, but which are [prosecuted] only if the interested party brings a complaint, because they do not greatly alarm society, are those referred to in Article 633 of the Criminal Code (invasion of land or buildings: a term of imprisonment of between one and three years and a fine of between EUR 103 and EUR 1 032) and in Article 640 of that code (simple fraud: imprisonment for a term of between six months and three years and a fine of between EUR 51 and EUR 1 032).'

[16] See Articles 7, 8 and 11 of the Charter.

establishing the facts, be acquired with the prior authorisation of the court, by way of reasoned order, at the request of the Public Prosecutor 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"?'

IV. The procedure before the Court

15. The Czech and Estonian Governments, Ireland, the French, Italian, Cypriot, Hungarian, Netherlands, Austrian and Polish Governments and the European Commission submitted written observations.

16. Those interested parties and the Public Prosecutor (Bolzano) presented oral argument and replied to questions put by the Court at the hearing on 21 March 2023.

V. Assessment

A. Admissibility

17. The Italian Government and Ireland submit that part of the request for a preliminary ruling is inadmissible. According to the facts in the order for reference, the request for access was made in the context of investigations into aggravated thefts of mobile telephones. Ireland emphasises that the Public Prosecutor may prosecute that offence *ex officio*. That power reflects the view that the nature and effects of the offence affect society generally. The request for a preliminary ruling is thus hypothetical to the extent that it also refers to criminal offences that may be prosecuted only on foot of a complaint by an individual. The Italian Government observes that the referring court refers to a series of offences that are irrelevant to the cases pending before it. The Italian Government and the Commission submit that, contrary to the reference in the request to 'a maximum term of imprisonment of at least three years', pursuant to Article 625 of the Criminal Code, the offence of aggravated theft is punishable by a term of imprisonment of two to six years. The Commission therefore proposes that the Court reformulate the question. The French Government also requests the Court to reformulate the question. It considers that while the Court may interpret provisions of EU law, it is not competent to assess the compatibility of provisions of national law with EU law.

18. The referring court's question literally asks the Court to rule on the compatibility of a provision of national law with EU law. That is, in itself, no obstacle to providing the referring court with an interpretation of EU law, in this instance, Article 15(1) of Directive 2002/58, that will enable it to rule on the compatibility with that provision of any national rule at issue in the proceedings before it. [17]

19. It is clear from the request for a preliminary ruling that the Public Prosecutor (Bolzano) sought access to data, inter alia, to investigate and to prosecute two incidents of the offence of aggravated theft of a mobile telephone pursuant to Article 625 of the Criminal Code. In those circumstances, the references that the request makes to other offences, including Article 624 of

[17] See, by analogy, judgment of 17 March 2021, *Consulmarketing* (C-652/19, EU:C:2021:208, paragraph 33). It is settled case-law that, pursuant to Article 267 TFEU, it is for the Court to provide a national court with an answer that will enable the latter to determine the case before it. To that end, the Court may reformulate the questions referred. Judgment of 25 July 2018, *Dyson* (C-632/16, EU:C:2018:599, paragraph 47 and the case-law cited).

the Criminal Code (simple theft),[18] are irrelevant to the determination of the applications pending before the referring court.[19] In so far as the question referred addresses the request from the Public Prosecutor (Bolzano) to access data in order to investigate the commission of offences of aggravated theft, it is not hypothetical. I shall accordingly confine my assessment of the application of Article 132(3) of Legislative Decree No 196/2003 to such facts as the referring court describes that pertain to the aggravated thefts of mobile telephones.

B. Substance

1. Preliminary observations

20. The present reference derives from a request from the Public Prosecutor (Bolzano) to access data retained by providers of electronic communications services. It does not concern the retention of those data or the lawfulness thereof pursuant, inter alia, to Article 15(1) of Directive 2002/58.[20] The data consists of details of incoming and outgoing communications[21] carried out with the stolen mobile telephones and location data.[22] Although the data do not include the contents of communications, they enable precise conclusions to be drawn as to the private lives of the persons whose data are concerned, access to which appears to amount to a 'serious' interference with their fundamental rights.[23] The interference that access to such data entails may be justified by the objective,[24] to which the first sentence of Article 15(1) of Directive 2002/58 refers, of preventing, investigating, detecting and prosecuting 'serious criminal offences', but not criminal offences in general. In interpreting Article 15(1) of Directive 2002/58, the Court links the seriousness of the interference with a person's fundamental rights to the seriousness of the criminal offence under investigation.[25]

[18] A person who commits the offence of simple theft is liable to a term of imprisonment ranging from six months to three years and therefore falls within the scope of Article 132(3) of Legislative Decree No 196/2003.

[19] In so far as those references indicate that Article 132(3) of Legislative Decree No 196/2003 may be relied upon in the investigation of offences that are not serious crimes, see points 35 to 39 of the present Opinion.

[20] The request for a preliminary ruling is thus based on the premiss that the retention of the data sought is lawful. The retention of and access to data covered by Directive 2002/58 constitute separate interferences with the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter and require a separate justification pursuant to Article 52(1) thereof. See, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 47). Paragraphs 29 to 33 of the judgment in *Prokuratuur* provide an overview of the rules governing the retention of such data.

[21] Article 2(d) of Directive 2002/58 provides that 'communication' means 'any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. …'

[22] Article 2(c) of Directive 2002/58 provides that 'location data' means 'any data … indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.

[23] The judgment in *Prokuratuur*, paragraphs 34 and 35. See, by analogy, judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraphs 59 to 62). It is for the national court to assess whether access to the data at issue constitutes a 'serious' interference with the fundamental rights of the persons concerned by such data. The present Opinion is based on the premiss that the interference entailed by access to the data described in point 10 of the present Opinion is serious.

[24] The list of objectives in Article 15(1) of Directive 2002/58 is exhaustive. Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 90).

[25] See, to that effect, Opinion of Advocate General Saugmandsgaard Øe in *Ministerio Fiscal* (C-207/16, EU:C:2018:300, points 79 to 82 and the case-law cited). In relation to the objective of fighting crime, access can, as a general rule, be granted 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 that crime. Judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 105).

2. Member States' competence to define 'serious criminal offences'

21. Directive 2002/58 regulates the activities of providers of electronic communications services in relation to the processing of personal data.[26] Article 1(3) expressly excludes from the scope of Directive 2002/58 activities of the State in specified fields such as public security, defence, State security and criminal law. The activities to which Article 15(1) of Directive 2002/58 refers overlap substantially with those described in Article 1(3) thereof and include State activities in the field of criminal law that are expressly excluded from the scope of Directive 2002/58.[27] There is thus a clear link between the State activities that Article 1(3) of Directive 2002/58 excludes from the scope of that directive and the legislative measures Member States may adopt pursuant to Article 15(1) thereof.[28]

22. Notwithstanding that clear link, the Court has consistently held that since Article 15(1) of Directive 2002/58 expressly authorises Member States to adopt the national legislative measures described therein, such measures fall within the scope of that directive. It follows from that case-law that the concept of 'activities', including the 'activities of the State in areas of criminal law' in Article 1(3) of Directive 2002/58, does not include the legislative measures to which Article 15(1) thereof refers.[29]

23. Neither Article 2 of Directive 2002/58, which contains a number of definitions for the purposes of the application of that directive, nor any other provision of Directive 2002/58, including Article 15(1), defines the term 'criminal offences'. Directive 2002/58 does not contain a list of 'criminal offences'.[30] Moreover, the case-law interpreting Article 15(1) of Directive 2002/58 does not define that term.[31]

[26] See, to that effect, Article 3 of Directive 2002/58, which states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services. See also judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraphs 70 and 74) and, by analogy, Opinion of Advocate General Szpunar in *La Quadrature du Net and Others (Personal data and action to combat counterfeiting*) (C-470/21, EU:C:2022:838, point 38).

[27] 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 97).

[28] For the purposes of safeguarding national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences and the unauthorised use of the electronic communications system.

[29] Judgments of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 98), and of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790, paragraph 38 and the case-law cited).

[30] See, by contrast, Article 2(2) of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ 2002 L 190, p. 1), as amended by Council Framework Decision 2009/299/JHA of 26 February 2009 (OJ 2009 L 81, p. 24), which lists the criminal offences that give rise to surrender pursuant to a European arrest warrant, and Annex II to Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132), which lists the 'serious crimes' defined by Article 3(9) of that directive.

[31] Directive 2002/58 does not refer to 'general criminal offences', 'serious criminal offences' or 'crime(s)'. The Court refers to those terms in its case-law without defining them or furnishing any criteria as to how national legislatures might do so. See, for example, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraphs 115 and 125), and of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraphs 54, 56 and 63). See also, in that regard, paragraph 45 of the judgment in *Prokuratuur*.

24. Despite the absence of any such definitions, Directive 2002/58 does not provide that each Member State defines 'criminal offences' in accordance with its national law. [32] According to the Court's settled case-law, the need for a uniform application of EU law and the principle of equality require that a provision of EU law that does not refer expressly to the law of the Member States in order to determine its meaning and scope is normally given an independent and uniform interpretation throughout the European Union. In the context of interpreting Article 15(1) of Directive 2002/58, the term 'criminal offences' may, at least in principle, be regarded as an autonomous concept of EU law which falls to be interpreted in a uniform manner throughout the Member States. [33]

25. The 10 Member States that submitted observations to the Court and the Commission are, however, of the unanimous view that it is for each Member State to define 'criminal offences', including serious offences, to which Article 15(1) of Directive 2002/58 refers by reference to their national laws.

26. I agree with those submissions for the following reasons.

27. First, the Court has previously stated that, in the context of Article 15(1) of Directive 2002/58, it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security. [34] While it did not expressly so hold, the Court thus appears to have taken the view that the term 'national security' in Article 15(1) of Directive 2002/58 is not an autonomous concept of EU law despite the absence of a definition of that term or any express reference to the law of the Member States. [35] I see no reason why that same approach ought not to apply to Member States' powers to define 'criminal offences' or 'serious criminal offences' for the purposes of Article 15(1) of Directive 2002/58. The terms 'criminal offences', 'public security' and 'national security' in that provision may be considered *noscitur a sociis* as it appears that the EU legislature intended that each of them be treated in a similar manner, including as regards the manner of their definition. [36]

28. Second, Article 4(2) TEU requires the European Union to respect the national identities of the Member States inherent in their fundamental political and constitutional structures. The preamble to the Charter also acknowledges that, while the Union contributes to the preservation and to the development of common values, it respects, inter alia, the diversity of the cultures and

[32] See, by contrast, Article 1(1) of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 (OJ 2006 L 105, p. 54) which provided that 'this Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, *as defined by each Member State in its national law*' (emphasis added). By judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238), the Court declared Directive 2006/24 invalid.

[33] See, by analogy, judgment of 7 September 2022, *Staatssecretaris van Justitie en Veiligheid (Nature of the right of residence under Article 20 TFEU)* (C-624/20, EU:C:2022:639, paragraphs 19 and 20).

[34] 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 99 and 136).

[35] In addition, Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That a national measure is adopted for the purpose of protecting national security does not render EU law inapplicable and exempt the Member States from any obligation to comply therewith. 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 99 and 135).

[36] Although the importance of the objective of safeguarding national security supersedes that of combating serious crime and is thus capable of justifying more serious interferences with fundamental rights, that objective does not impinge on Member States' right to define 'criminal offences' or 'serious criminal offences'. 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 136).

traditions of the peoples of Europe. The definition of criminal offences and penalties [37] reflects national sensitivities and traditions that vary considerably not only as between Member States but also over time in tandem with societal change. [38]

29. It may be observed in that context that, when defining criminal offences and penalties, Member States take a variety of different factors into account to varying degrees. A Member State's assessment of the 'seriousness' of a particular offence is often, if not invariably, reflected in the gravity of the penalty imposed. The length of a custodial sentence may reflect an analysis of a number of factors, including the perceived intrinsic 'seriousness' of an offence and its relative 'seriousness' as compared to other offences. No reasons have been advanced as to why Member States ought not to exercise that power or, indeed, why a different approach ought to apply to the definition of 'criminal offences', 'serious criminal offences' or 'criminal offences in general' in the particular context under consideration.

30. Member States' competence in the field of criminal law is without prejudice to that which the European Union enjoys, in certain instances, to establish, for example, minimum rules defining criminal offences and sanctions as regards particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. [39] The EU legislature did not, however, establish rules governing the definition of criminal offences in Article 15(1) of Directive 2002/58. [40] Indeed, as previously indicated, [41] it is evident from the text of Article 1(3) of Directive 2002/58 that, by enacting that directive, the EU legislature did not intend to exercise any competence in the field of criminal law.

31. Those two reasons suffice to explain why, notwithstanding that national legislative measures adopted pursuant to Article 15(1) of Directive 2002/58 for the investigation and prosecution of criminal offences fall within the scope of that measure, Member States retain the power to define 'criminal offences', including 'serious criminal offences', and to set penalties for engaging in such conduct. [42]

[37] And that of attenuating and aggravating circumstances.

[38] Advocate General Saugmandsgaard Øe considered that criminal legislation and the rules of criminal procedure fall within the competence of the Member States, although their legal orders may nevertheless be affected by the provisions of EU law adopted in that field on the basis, inter alia, of Article 83(2) TFEU. There is thus no provision of general application that would provide a harmonised definition of the concept of 'serious crime'. Opinion in *Ministerio Fiscal* (C-207/16, EU:C:2018:300, point 95). Advocate General Pitruzzella stated that the definition of 'serious crime' should be left to the discretion of the Member States. Depending on the national legal system, the same offence may be penalised more or less severely. What constitute aggravating circumstances may also vary between the Member States. Opinion in *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2020:18, points 91 and 92). By contrast, Advocate General Szpunar considered that 'the concept of "serious crime" must … be given an autonomous interpretation. It cannot depend on the individual approach taken by each Member State as that would allow the requirements of Article 15(1) of Directive 2002/58 to be circumvented depending on whether or not Member States construe action to combat serious crime broadly.' Opinion in *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (C-470/21, EU:C:2022:838, point 74).

[39] The first subparagraph of Article 83(1) TFEU. See also judgment of 21 October 2021, *Okrazhna prokuratura – Varna* (C-845/19 and C-863/19, EU:C:2021:864, paragraph 32).

[40] See, by analogy, the judgment in *Prokuratuur*, paragraphs 41 and 42. The Court stated that in the absence of EU rules on the matter and in accordance with the principle of procedural autonomy, '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'. The legal basis of Directive 2002/58 is Article 114 TFEU (formerly Article 95 TEC) and not, for example, the first subparagraph of Article 83(1) TFEU. By contrast, the legal bases of Directive 2016/681 are point (d) of the second subparagraph of Article 82(1) TFEU (judicial cooperation in criminal matters) and point (a) of Article 87(2) TFEU (police cooperation).

[41] See point 21 of the present Opinion.

[42] See, by analogy, judgment of 23 October 2007, *Commission* v *Council* (C-440/05, EU:C:2007:625, paragraphs 66, 70 and 71 and the case-law cited). See also judgment of 28 April 2011, *El Dridi* (C-61/11 PPU, EU:C:2011:268, paragraph 53).

3. The standard of review of the exercise of the option in Article 15(1) of Directive 2002/58 to derogate from the principle of confidentiality

32. The Court has emphasised that the option to derogate [43] from, inter alia, the principle of confidentiality prescribed in Article 5(1) of Directive 2002/58, must be interpreted strictly in order for it not to become the general rule, thereby rendering the principle meaningless. [44] The exercise of that option must thus respect, inter alia, the principles of equivalence [45] and effectiveness. [46] It must also comply with the general principles of EU law, including the principle of proportionality, [47] and Articles 7, 8 and 11 [48] and Article 52(1) of the Charter. [49] The objective of combating serious crime must always be reconciled with the enjoyment of the fundamental rights thus affected. The rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute and their exercise must be considered in relation to their function in society. [50] Article 52(1) of the Charter thus provides that limitations on the exercise of those rights, as are provided for by law, must respect the essence of those rights and, in compliance with the principle of proportionality, must be necessary and must genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. National legislative measures adopted pursuant to Article 15(1) of Directive 2002/58 must thus correspond genuinely and strictly to one of the objectives outlined in that provision. They must be based on objective criteria, be legally binding and lay down clear and precise rules that indicate the substantive and procedural conditions under which providers of electronic communications services must grant competent national authorities access to data. [51]

33. In order to ensure full respect for those conditions in practice, access by competent national authorities to retained data must, in principle, [52] be subject to prior review by a court or by an independent administrative body [53] following a reasoned request by those authorities and the

[43] Article 15(1) of Directive 2002/58 provides that the Member States 'may adopt' legislative measures that restrict certain rights and obligations for which that directive provides.

[44] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 89). Advocate General Saugmandsgaard Øe considered that 'although each Member State has the power to assess what is the appropriate penalty threshold for the purpose of characterising a serious offence, it is nevertheless under a duty not to set that threshold at such a low level, having regard to the normal level of penalties applicable in that State, that the exceptions to the prohibition on the storage and use of personal data laid down in Article 15(1) would be transformed into principles …' Opinion in *Ministerio Fiscal* (C-207/16, EU:C:2018:300, point 114).

[45] There is nothing to indicate that the Italian law at issue does not comply with this principle.

[46] Judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 127).

[47] See also recital 11 of Directive 2002/58.

[48] See also recital 2 of Directive 2002/58.

[49] Judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 89), and of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 111 to 113). See also Opinion of Advocate General Saugmandsgaard Øe in *Ministerio Fiscal* (C-207/16, EU:C:2018:300, points 116 to 120). In the judgment of 8 March 2022, *Bezirkshauptmannschaft Hartberg-Fürstenfeld (Direct effect)* (C-205/20, EU:C:2022:168, paragraph 31), the Court recalled that the principle of proportionality binds Member States when they implement EU law. In that context, Member States must comply with Article 49(3) of the Charter when they adopt criminal penalties, even in the absence of EU legislation harmonising those sanctions.

[50] Article 52(1) of the Charter. 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 120).

[51] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraphs 117 to 119). See also 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 110 and 129 to 133).

[52] For example, Article 132(3a) of Legislative Decree No 196/2003 establishes special rules to access data in urgent cases. In his Opinion in *La Quadrature du Net and Others (Personal data and action to combat counterfeiting)* (C-470/21, EU:C:2022:838, points 99 to 105), Advocate General Szpunar considered that prior review is necessary only where there is a serious interference with the private lives of users of electronic communications services. Prior review is necessary since the interference in the present proceedings is serious due to the nature of the data to which the Public Prosecutor seeks access.

[53] The case-law of the Court, not Directive 2002/58, established the prior review requirement: judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraphs 120 and 121 and the case-law cited).

notification of the persons concerned.[54] It is settled case-law that, in conducting that prior review, a court or independent administrative body must reconcile the various interests and rights at issue in order to strike a fair balance between the requirements of the investigation and the need to safeguard the fundamental rights to privacy and protection of personal data of the persons concerned.[55]

34. In the present case, Article 132(3) of Legislative Decree No 196/2003 establishes the conditions pursuant to which a national court must order providers of electronic communications services to grant the Public Prosecutor access to data at the latter's request. It is not disputed[56] that Article 132(3) of Legislative Decree No 196/2003 sets out in clear and precise terms the circumstances and the conditions under which a national court can order the providers of electronic communications services to grant such access. The referring court is, however, of the view that the penalty of 'a maximum term of imprisonment of at least three years' is excessively broad as it brings within its scope offences such as simple theft that cause little social disturbance.

35. While Article 132(3) of Legislative Decree No 196/2003 potentially covers a wide range of criminal offences, there is nothing before the Court by way of evidence in the present proceedings that it encompasses such a large number of offences as to render access to data thereunder the rule rather than the exception.[57] The threshold of a maximum term of imprisonment of at least three years in that provision does not appear to be excessively low.[58] By way of analogy, Article 3(9) of Directive 2016/681[59] defines 'serious crime' as 'the offences listed in Annex II that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.'[60] The Court, however, stated that since Article 3(9) of Directive 2016/681 refers to the maximum penalty applicable rather than the minimum, it cannot be ruled out that the relevant 'data may be processed for the purposes of combating offences which, although meeting the criterion laid down by that provision relating to the threshold of severity, amount to ordinary crime rather than serious crime, having regard to the particular features of the domestic criminal justice system'.[61]

54 Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraphs 120 and 121).

55 The judgment in *Prokuratuur*, paragraph 52.

56 Subject to verification by the referring court.

57 See the analysis in the Opinion of Advocate General Saugmandsgaard Øe in *Ministerio Fiscal* (C-207/16, EU:C:2018:300, points 116 to 120). This is ultimately a matter for the referring court to assess.

58 The fact that the definition of offences and the system of penalties in one Member State differ from those in another cannot itself affect the proportionality of the legislation. See by analogy judgment of 8 July 2010, *Sjöberg and Gerdin* (C-447/08 and C-448/08, EU:C:2010:415, paragraph 38).

59 Directive 2016/681 concerns the transfer and processing of passenger data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

60 The Court held that the requirements flowing from that provision, which relate to the nature and severity of the applicable penalty, are, in principle, such as to limit the application of the system established by Directive 2016/681 to offences that have the requisite level of seriousness to justify the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Judgment of 21 June 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, paragraph 150).

61 The Court thus held that the Member States must ensure that the system established by Directive 2016/681 is limited to combating serious, not ordinary, crime. Judgment of 21 June 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, paragraphs 151 and 152). The subject matter and scope of Directive 2016/681 which provide, inter alia, for the exchange of PNR data between Member States, do not overlap with those of Directive 2002/58. It follows that the provisions of these directives are to be assessed separately and on their own merits. In that regard, and contrary to the position as regards Article 15(1) of Directive 2002/58, the concept of 'serious crime' in Directive 2016/681 is an autonomous concept of EU law. See also, in that regard, recital 12 and Article 3(9) of and Annex II to Directive 2016/681.

36. The three-year penalty in Article 132(3) of Legislative Decree No 196/2003 refers to the maximum penalty applicable and could thus apply to offences such as simple theft.[62] It is therefore necessary to examine how Article 132(3) of Legislative Decree No 196/2003 is applied in practice. Subject to verification by the referring court, Article 132(3) of Legislative Decree No 196/2003 appears to establish two different standards of prior review by a national court depending on the nature of the offences under investigation.

37. The first of these standards of review requires[63] national courts to authorise the Public Prosecutor to access data retained by providers of electronic communications services if such data are relevant for the purpose of establishing the facts and there is sufficient evidence of the commission of an offence of threatening and harassing or disturbing persons by means of the telephone, where the threat or disturbance is serious. The national court must therefore carry out an individual assessment of the seriousness of the offence in question and verify whether the investigation and prosecution of that offence merits a limitation of the general rights enshrined in Articles 7, 8 and 11 of the Charter and the specific rights contained in Articles 5, 6 and 9 of Directive 2002/58. That standard requires an individual assessment, in a given case, as to whether the interference with those rights is proportionate, as compared with the public interest objective of combating crime.

38. By contrast, the second standard of review, which is relevant in the context of the present proceedings, requires[64] national courts to authorise the Public Prosecutor to access data retained by providers of electronic communications services if such data are relevant for the purpose of establishing the facts and there is sufficient evidence of the commission of an offence liable to punishment by, inter alia, a maximum term of imprisonment of at least three years. In that case, the role of the national court is limited to verifying whether those objective requirements are met without having any possibility to carry out an individual assessment of the interests in the case at hand.[65] The review the national court carries out pursuant to Article 132(3) of Legislative Decree No 196/2003 is thus detached from any real connection with the specific circumstances of the case before it.

39. While national courts may not have jurisdiction to review the definition, by the legislature, of offences or to review the legislature's decision as to the seriousness of such offences,[66] those courts must nonetheless have jurisdiction to carry out an individual assessment as to whether the grant of access, pursuant to legislative measures adopted under Article 15(1) of Directive 2002/58, to sensitive data enabling precise conclusions to be drawn concerning a user's private life – which thus constitutes a serious interference with the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter – is proportionate.

[62] See, by analogy, judgment of 21 June 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, paragraph 151).

[63] The original language text uses the terms 'i dati sono acquisiti'.

[64] Subject to verification by the referring court, the use of the indicative in Article 132(3) of Legislative Decree No 196/2003 ('i dati sono acquisiti') implies that access to the data in question shall be granted by the national court provided the objective conditions imposed by that provision are fulfilled.

[65] At the hearing, the views of the Public Prosecutor (Bolzano) and the Italian Government on the role of the national court and the scope of prior review pursuant to Article 132(3) of Legislative Decree No 196/2003 differed. While the Public Prosecutor (Bolzano) claimed that, prior to granting access to such data, the national court must carry out an individual assessment of the proportionality of granting that access, the Italian Government emphasised that the national court is bound, in accordance with Article 101 of the Costituzione della Repubblica Italiana (Constitution of the Italian Republic) and Article 1 of the Criminal Code, by the principle of legality and therefore cannot adopt what it described as a creative interpretation of the law. It is for the referring court to interpret the applicable provisions of national law.

[66] Unless national law so permits and subject to compliance with, inter alia, Article 49 of the Charter.

40. It follows that, pursuant to the measures adopted under Article 15(1) of Directive 2002/58, access to sensitive data may not be granted unless (i) the offence in question attains the threshold of seriousness determined in advance by the national legislature, and (ii) a court or other independent administrative body considers, following an individual assessment or review, that the interference with fundamental rights entailed by the grant of such access is proportionate, in view of the public interest objective of combating crime in a particular case. In certain cases, however, access to such data may not be granted, even where the offence reaches the threshold of seriousness under national law.

41. The offence of aggravated theft in the present case is considered to be 'serious' under national law as it is subject to a penalty of, inter alia, a term of imprisonment of two to six years, thereby complying with the threshold of seriousness in Article 132(3) of Legislative Decree No 196/2003.[67] When applying measures adopted pursuant to Article 15(1) of Directive 2002/58, the Italian courts do not appear to have jurisdiction to call into question the classification of aggravated theft as a 'serious offence' under national law. Where the threshold set by national law has not been met, the referring court thus may not grant access to the data sought.[68]

42. Where the threshold set by the national legislature is met, the referring court must, pursuant to Article 15(1) of Directive 2002/58, review whether, in the light of all the circumstances pertaining to the specific case at hand, the interference with fundamental rights entailed by facilitating access to sensitive data is proportionate to the public interest objective of combating that offence. The referring court must, in that regard, take into account and weigh all relevant rights and interests including, inter alia, the damage caused to the property rights of victims protected under Article 17 of the Charter and the fact that mobile telephones may contain highly sensitive information relating to their owners' private, professional and financial lives.[69] Access to the data in question may be the only effective means available to investigate and to prosecute the offences in question and to ensure that their, as yet unknown, perpetrators do not act with impunity. The rights of third parties[70] are also to be taken into account.

43. As regards the rights of third parties, it appears[71] from the referring court's files that the Public Prosecutor (Bolzano) sought access to data concerning communications from the stolen mobile telephones from 29 October 2021 in respect of the first theft committed on 27 October 2021[72] and from 20 November 2021 in respect of the second theft committed on that date.[73] These dates show that the requests for access impinge, to a very limited extent, on the rights of the victims guaranteed, inter alia, by Articles 7, 8 and 11 of the Charter.[74] The Italian Government also stated in its written observations that the national proceedings relate solely to data that would help to identify the perpetrator(s) of the thefts in question. In the event of the identification of calls to or from third parties unconnected to the theft, those data would be

67 A penalty of a maximum term of imprisonment of at least three years.

68 Article 52(1) of the Charter provides that the law must provide for any limitation on the exercise of a right recognised by the Charter. This implies that national courts are, in principle, bound by national legislation that contains such limitations.

69 Mobile telephones may contain photographs, health data, bank statements, passwords, etc. The theft of a mobile telephone may therefore compromise the digital identity of its owner and its effects may considerably outweigh the loss of its monetary value. The referring court should therefore also take into account and weigh any potential damage to the victims' rights pursuant, inter alia, to Articles 7, 8 and 17 of the Charter.

70 Such as the victims of the alleged offence.

71 Subject to verification by the referring court.

72 Reference number RGNR 9228/2021.

73 Reference number RGNR 9794/2021.

74 Although the data may relate to communications made to the victim after the date of the theft, it does not relate, in reality, to communications made by the victim or his or her location data.

destroyed, in accordance with Article 269 of the Code of Criminal Procedure.[75] Finally, Article 132(3c) of Legislative Decree No 196/2003 provides that data acquired in breach of paragraph 3 or 3a thereof may not be used.[76]

VI. Conclusion

44. In the light of the above considerations, I propose that the Court answer the question referred for a preliminary ruling by the Tribunale di Bolzano (District Court, Bolzano, Italy) as follows:

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 and Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union

must be interpreted as not precluding national legislation that requires a court to authorise access, by the Public Prosecutor, to data lawfully retained by the providers of electronic communications services and enabling precise conclusions to be drawn concerning a user's private life if such data are relevant for the purpose of establishing the facts and there is sufficient evidence of the commission of a serious crime as defined by national law which is liable to a maximum term of imprisonment of at least three years. Prior to granting access, the national court must carry out an individual assessment as to whether the interference with fundamental rights entailed by the grant of such access is proportionate in the light, inter alia, of the seriousness of the specific crime and the facts of the case.

[75] According to the Italian Government, the applicable version of Article 269(2) of the Code of Criminal Procedure provided that '… the recordings shall be kept until final judgment is delivered. However, in order to protect confidentiality, the interested parties may request the judge who authorised or validated the interception to destroy the recordings that have not been included in the file' (as they are irrelevant). While access to data relating to innocent third parties is unlimited, the use of those data appears, subject to verification by the referring court, to be circumscribed by national law.

[76] The reference for a preliminary ruling neither explains the exact meaning of this provision nor its application in practice.