Provisional text

JUDGMENT OF THE COURT (Grand Chamber)

2 October 2018 (*)

(Reference for a preliminary ruling — Electronic communications — Processing of personal data — Directive 2002/58/EC — Articles 1 and 3 — Scope — Confidentiality of electronic communications — Protection — Article 5 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Data processed in connection with the provision of electronic communications services — Access of national authorities to the data for the purposes of an investigation — Threshold of seriousness of an offence capable of justifying access to the data)

In Case C−207/16,

REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain), made by decision of 6 April 2016, received at the Court on 14 April 2016, in the proceedings brought by

Ministerio Fiscal,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Tizzano, Vice-President, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), J.L. da Cruz Vilaça, C.G. Fernlund and C. Vajda, Presidents of Chambers, E. Juhász, A. Borg Barthet, C. Toader, M. Safjan, D. Šváby, M. Berger, E. Jarašiūnas and E. Regan, Judges,

Advocate General: H. Saugmandsgaard Øe,

Registrar: L. Carrasco Marco, Administrator,

having regard to the written procedure and further to the hearing on 29 January 2018,

after considering the observations submitted on behalf of

– the Ministerio Fiscal, by E. Tejada de la Fuente,

– the Spanish Government, by M. Sampol Pucurull, acting as Agent,

– the Czech Government, by M. Smolek, J. Vláčil and A. Brabcová, acting as Agents,

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

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

– Ireland, by M. Browne, L. Williams, E. Creedon and A. Joyce, acting as Agents, and by E. Gibson, Barrister-at-Law,

– the French Government, by D. Colas, E. de Moustier and E. Armoet, acting as Agents,

– the Latvian Government, by I. Kucina and J. Davidoviča, acting as Agents,

– the Hungarian Government, by M. Fehér and G. Koós, acting as Agents,

– the Austrian Government, by C. Pesendorfer, acting as Agent,

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

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

– the European Commission, by I. Martínez del Peral, P. Costa de Oliveira, R. Troosters and D. Nardi, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 3 May 2018,

gives the following

Judgment

1 This request for a preliminary ruling concerns, in essence, 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 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings brought by the Ministerio Fiscal (Public Prosecutor's Office, Spain) against the decision of the Juzgado de Instrucción No 3 de Tarragona (Court of Preliminary Investigation No 3, Tarragona, Spain, 'the investigating magistrate') refusing to grant the police access to personal data retained by providers of electronic communications services.

Legal context

EU law

Directive 95/46

3 According to Article 2(b) of 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), 'processing of personal data' means 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

4 Article 3 of the directive, entitled 'Scope', provides as follows:

'1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

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

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

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

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

Directive 2002/58

5 Recitals 2, 11, 15 and 21 of Directive 2002/58 state:

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

...

(11) Like Directive [95/46], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by 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, 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.

...

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. ...

...

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.'

6 Article 1 of Directive 2002/58, entitled 'Scope and aim', provides:

'1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers

who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

7 Article 2 of Directive 2002/58, entitled 'Definitions', is worded as follows:

'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:

...

(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;

...'

8 Article 3 of Directive 2002/58, entitled 'Services concerned', provides:

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

9 Article 5 of Directive 2002/58, entitled 'Confidentiality of the communications', is worded as follows:

'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). …

...

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. …'

10 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.

...’

11 Article 15 of that directive, entitled ‘Application of certain provisions of Directive [95/46]’, provides, 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) of the Treaty on European Union.’

Spanish law

Law 25/2007

12 Article 1 of Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Law 25/2007 on the retention of data relating to electronic communications and to public communication networks) of 18 October 2007 (BOE No 251 of 19 October 2007, p. 42517) provides:

‘1. The purpose of this law is to regulate the obligation of operators to retain the data generated or processed in the context of the supply of electronic communications services or public communication networks, and the obligation to communicate those data to authorised agents whenever they are requested to do so by the necessary judicial authorisation, for the purposes of the detection, investigation and prosecution of serious offences provided for in the Criminal Code or in special criminal laws.

2. This law shall apply to traffic data and to location data concerning both natural and legal persons, and to related data necessary in order to identify the subscriber or registered user.

...’

The Criminal Code

13 Article 13(1) of Ley Orgánica 10/1995 del Código Penal (Criminal Code) of 23 November 1995 (BOE No 281 of 24 November 1995, p. 33987) is worded as follows:

‘Serious offences are those which the law punishes with a serious penalty.’

14 Article 33 of the Criminal Code provides:

‘1. Depending on their nature and duration, penalties shall be classified as serious, less serious and light.

2. Serious penalties shall be:

(a) imprisonment for life, subject to review.

(b) imprisonment for a period of more than five years.

...’

Code of Criminal Procedure

15 After the facts in the main proceedings had taken place, the Ley de Enjuiciamiento Criminal (Code of Criminal Procedure) was amended by Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Organic Law 13/2015 amending the Code of Criminal Procedure in order to strengthen the procedural guarantees and regulate technological investigative measures) of 5 October 2015 (BOE No 239 of 6 October 2015, p. 90192).

16 The law entered into force on 6 December 2015. It brings the field of access to telephone and telematic communications data which have been retained by providers of electronic communications services within the purview of the Code of Criminal Procedure.

17 Article 579(1) of the Code of Criminal Procedure in the version as amended by Organic Law 13/2015 provides:

‘1. The court may authorise the interception of private postal and telegraphic correspondence, including fax, Burofax and international money orders, which the suspect sends or receives, and also the opening and analysis of such correspondence where there are grounds for thinking that that will permit the discovery or verification of a fact or a factor of relevance for the case, provided that the investigation relates to one of the following offences:

(1) Intentional offences punishable by a maximum penalty of at least three years’ imprisonment.

(2) Offences committed in the context of a criminal organisation.

(3) Terrorism offences.

...’

18 Article 588 *ter* j of the Code is worded as follows:

‘1. Electronic data retained by service providers or by persons who supply the communication pursuant to the legislation on the retention of electronic communications data, or on their own initiative for commercial or other reasons, and who are connected with communications processes, shall be communicated in order to be taken into account in the context of the proceedings only when authorised by the court.

2. Where knowledge of those data is essential for the investigation, application must be made to the competent court for authorisation to access the information in the automated archives of the service providers, in particular for the purpose of a cross search or a smart search of the data, provided that the nature of the data of which it is necessary to have knowledge and the reasons justifying the communication of those data are specified.’

The main proceedings and the questions referred for a preliminary ruling

19 Mr Hernandez Sierra lodged a complaint with the police for a robbery, which took place on 16 February 2015, during which he was injured and his wallet and mobile telephone were stolen.

20 On 27 February 2015, the police requested the investigating magistrate to order various providers of electronic communications services to provide (i) the telephone numbers that had been activated between 16 February and 27 February 2015 with the International Mobile Equipment Identity code ('the IMEI code') of the stolen mobile telephone and (ii) the personal data relating to the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code, such as their surnames, forenames and, if need be, addresses.

21 By order of 5 May 2015, the investigating magistrate refused that request. The latter held that the measure requested would not serve to identify the perpetrators of the offence. Moreover, it refused to grant the request on the ground that Law 25/2007 limited the communication of the data retained by the providers of electronic communications services to serious offences. Under the Criminal Code, serious offences are punishable by a term of imprisonment of more than five years, whereas the facts at issue in the main proceedings did not appear to constitute such an offence.

22 The Public Prosecutor's Office appealed against that order before the referring court, claiming that communication of the data at issue ought to have been allowed by reason of the nature of the facts and pursuant to a judgment of the Tribunal Supremo (Supreme Court, Spain) of 26 July 2010 relating to a similar case.

23 The referring court explains that, subsequent to that order, the Spanish legislature amended the Code of Criminal Procedure by adopting Organic Law 13/2015. That legislation, which is relevant to the resolution of the case in the main proceedings, introduced two new alternative criteria for determining the degree of seriousness of an offence. The first is a substantive criterion, relating to conduct which corresponds to criminal classifications the criminal nature of which is specific and serious, and which is particularly harmful to individual and collective legal interests. Moreover, the national legislature relied on a formal normative criterion, based on the penalty prescribed for the offence in question. The threshold of three years' imprisonment envisaged by that criterion does, however, cover the great majority of offences. In addition, the referring court considers that the State's interest in punishing criminal conduct cannot justify disproportionate interferences with the fundamental rights enshrined in the Charter.

24 In that regard, the referring court considers that, in the main proceedings, Directives 95/46 and 2002/58 establish a link with the Charter. The national legislation at issue in the main proceedings therefore comes within its scope, in accordance with Article 51(1) of the Charter, despite the fact that 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) was annulled by the judgment of 8 April 2014, *Digital Rights Ireland and Others* (C−293/12 and C−594/12, EU:C:2014:238).

25 In that judgment, the Court recognised that the retention and communication of traffic data constitute particularly serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter and established criteria for the assessment of whether the principle of proportionality has been observed, including the seriousness of the offences warranting the retention of data and access thereto for the purposes of an investigation.

26 In those circumstances, the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Can the sufficient seriousness of offences, as a criterion which justifies interference with the fundamental rights recognised by Articles 7 and 8 of the [Charter], be determined taking into account only the sentence which may be imposed in respect of the offence investigated, or is it also necessary

to identify in the criminal conduct particular levels of harm to individual and/or collective legally protected interests?

(2) If it were in accordance with the constitutional principles of the European Union, used by the Court of Justice in its judgment [of 8 April 2014, *Digital Rights Ireland and Others*, C−293/12 and C−594/12, EU:C:2014:238] as standards for the strict review of [Directive 2002/58], to determine the seriousness of the offence solely on the basis of the sentence which may be imposed, what should the minimum threshold be? Would it be compatible with a general provision setting a minimum of three years' imprisonment?'

Procedure before the Court

27 By decision of the President of the Court of 23 May 2016, the proceedings before the Court were stayed pending delivery of the judgment in *Tele2 Sverige and Watson and Others*, C−203/15 and C−698/15 (judgment of 21 December 2016, EU:C:2016:970, hereinafter '*Tele2 Sverige and Watson and Others*'). Further to the delivery of that judgment, the referring court was asked whether it wished to maintain or withdraw its request for a preliminary ruling. In its response by letter of 30 January 2017, received at the Court on 14 February 2017, the referring court stated that, in its view, that judgment did not enable it to assess with a sufficient degree of certainty the national legislation at issue in the main proceedings in the light of EU law. Consequently, the proceedings before the Court were resumed on 16 February 2017.

Consideration of the questions referred

28 The Spanish Government claims that, first, the Court lacks jurisdiction to reply to the request for a preliminary ruling and, secondly, the request is inadmissible.

The jurisdiction of the Court

29 In its written observations submitted to the Court, the Spanish Government expressed the view, endorsed by the United Kingdom Government during the hearing, that the Court does not have jurisdiction to answer the question referred for a preliminary ruling, on the ground that, in accordance with the first indent of Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58, the case in the main proceedings is excluded from the scope of those two directives. Therefore, the case does not fall within the scope of EU law, with the result that the Charter, in accordance with Article 51(1) thereof, is not applicable.

30 According to the Spanish Government, the Court did, admittedly, rule in *Tele2 Sverige and Watson and Others* that a legislative measure governing national authorities' access to data retained by providers of electronic communications services comes within the scope of Directive 2002/58. However, the present case concerns a request for access made by a public authority, by virtue of a judicial decision in connection with a criminal investigation, to personal data retained by providers of electronic communications services. The Spanish Government infers that the request for access is part of national authorities' exercise of *jus puniendi*, as a result of which it constitutes an activity of the State in areas of criminal law falling under the exception provided for in the first indent of Article 3(2) of Directive 95/46 and Article 1(3) of Directive 2002/58.

31 In order to assess the claim that the Court does not have jurisdiction, it must be observed that Article 1(1) of Directive 2002/58 states that the directive provides for the harmonisation of the national provisions required, inter alia, to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector. In accordance with Article 1(2) thereof, the directive particularises and complements Directive 95/46 for the purposes set out in Article 1(1).

32 Article 1(3) of Directive 2002/58 excludes from its scope ‘activities of the State’ in specified fields, including the activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters (*Tele2 Sverige and Watson and Others*, paragraph 69 and the case-law cited). The activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (see, by analogy, in respect of the first indent of Article 3(2) of Directive 95/46, judgment of 10 July 2018, *Jehovan Todistajat*, C−25/17, EU:C:2018:551, paragraph 38 and the case-law cited).

33 Article 3 of Directive 2002/58 states that the directive is to apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the European Union, including public communications networks supporting data collection and identification devices (‘electronic communications services’). Consequently, that directive must be regarded as regulating the activities of the providers of such services (*Tele2 Sverige and Watson and Others*, paragraph 70).

34 As regards Article 15(1) of Directive 2002/58, the Court has previously held that the legislative measures that are referred to in that provision come within the scope of that directive, even if they concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active, and even if the objectives that such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of Directive 2002/58. Article 15(1) necessarily presupposes that the national measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraphs 72 to 74).

35 The Court concluded that Article 15(1), read in conjunction with Article 3 of Directive 2002/58, must be interpreted as meaning that the scope of the directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic and location data, but also to a legislative measure relating to the access of the national authorities to the data retained by those providers (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraphs 75 and 76).

36 The protection of the confidentiality of electronic communications and related traffic data, guaranteed by Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including ‘any data related to such communications’, in order to protect the confidentiality of electronic communications (*Tele2 Sverige and Watson and Others*, paragraph 77).

37 It should also be noted that legislative measures requiring providers of electronic communications services to retain personal data or to grant competent national authorities access to those data necessarily involve the processing, by those providers, of the data (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraphs 75 and 78). Such measures, to the extent that they regulate the activities of such providers, cannot be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58.

38 In the present case, as stated in the order for reference, the request at issue in the main proceedings, by which the police seeks judicial authorisation to access personal data retained by providers of electronic communications services, is based on Law 25/2007, read in conjunction with the Code of Criminal Procedure in the version applicable to the facts in the main proceedings, which governs the access of public authorities to such data. That legislation permits the police, in the event that the judicial authorisation applied for on the basis of that legislation is granted, to require providers of electronic communications services to make personal data available to it and, in so doing, in the light of the definition in Article 2(b) of Directive 95/46, which is applicable in connection with Directive 2002/58 pursuant to the first paragraph of Article 2 of the latter directive, to ‘process’ those data within the meaning of the two

directives. That legislation therefore governs the activities of providers of electronic communications services and, as a result, falls within the scope of Directive 2002/58.

39 In those circumstances, the fact, noted by the Spanish Government, that the request for access was made in connection with a criminal investigation does not make Directive 2002/58 inapplicable to the case in the main proceedings by virtue of Article 1(3) of the directive.

40 It is also irrelevant in that regard that the request for access at issue in the main proceedings relates, as is apparent from the Spanish Government's written answer to a question raised by the Court and confirmed by both that government and the Public Prosecutor's Office during the hearing, to the granting of access to only the telephone numbers corresponding to the SIM cards activated with the IMEI code of the stolen mobile telephone and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses, not to the data relating to the communications carried out with those SIM cards and the location data concerning the stolen mobile telephone.

41 As observed by the Advocate General in point 54 of his Opinion, Directive 2002/58, pursuant to Article 1(1) and Article 3 thereof, governs all processing of personal data in connection with the provision of electronic communications services. In addition, in accordance with subparagraph (b) of the second paragraph of Article 2 of the directive, the notion of 'traffic data' covers 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.

42 In that connection, as regards, more specifically, data relating to the identity of owners of SIM cards, it is apparent from recital 15 of Directive 2002/58 that traffic data may include, inter alia, the name and address of the person sending a communication or using a connection to carry out a communication. Data relating to the identity of owners of SIM cards can also prove necessary in order to bill for the electronic communications services provided and therefore form part of traffic data as defined in subparagraph (b) of the second paragraph of Article 2 of the directive. Consequently, those data fall within the scope of Directive 2002/58.

43 The Court therefore has jurisdiction to reply to the question raised by the referring court.

Admissibility

44 The Spanish Government argues that the request for a preliminary ruling is inadmissible on the ground that it does not clearly identify the provisions of EU law on which the Court is asked to give a preliminary ruling. What is more, the police request at issue in the main proceedings does not concern the interception of communications made by means of the SIM cards activated with the IMEI code of the stolen mobile telephone, but rather the establishment of a link between the cards and their owners, in such a way that the confidentiality of the communications is not affected. Article 7 of the Charter, referred to in the questions referred for a preliminary ruling, is therefore irrelevant to the present case.

45 The Court has consistently held that it is solely for the national court before which the 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 put by national courts concern the interpretation of a provision of EU law, the Court is, in principle, bound to give a ruling. 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 10 July 2018, *Jehovan Todistajat*, C−25/17, EU:C:2018:551, paragraph 31 and the case-law cited).

46 In the present case, the order for reference contains sufficient factual and legal information required both for the definition of the provisions of EU law referred to in the questions referred for a preliminary ruling and for the understanding of the scope of those questions. More specifically, it is apparent from the order for reference that the questions referred for a preliminary ruling are intended to enable the referring court to assess whether, and to what extent, the national legislation, on which the police request at issue in the main proceedings is based, pursues an objective which is capable of justifying infringement of the fundamental rights enshrined in Articles 7 and 8 of the Charter. According to the statements of the referring court, that national legislation falls within the scope of Directive 2002/58, with the result that the Charter is applicable to the case in the main proceedings. The questions referred for a preliminary ruling are thus directly related to the subject matter of the main proceedings and cannot therefore be regarded as hypothetical.

47 In those circumstances, the questions referred for a preliminary ruling are admissible.

Substance

48 By its two questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that public authorities' access to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners of the SIM cards, entails interference with their fundamental rights, enshrined in those articles of the Charter, which is sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime and, if so, by reference to which criteria the seriousness of the offence at issue must be assessed.

49 In that regard, it is apparent from the order for reference that, as observed in essence by the Advocate General in point 38 of his Opinion, the request for a preliminary ruling does not seek to determine whether the personal data at issue in the main proceedings have been retained by providers of electronic communications services in a manner consistent with the requirements laid down in Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter. As stated in paragraph 46 of this judgment, the request concerns only whether, and to what extent, the objective pursued by the legislation at issue in the main proceedings is capable of justifying the access of public authorities, such as the police, to such data, without the other conditions for access deriving from Article 15(1) forming part of the subject matter of the request.

50 More specifically, the referring court is uncertain as to the factors that should be taken into consideration in order to assess whether the offences in respect of which the police may be authorised, for the purposes of an investigation, to have access to personal data retained by providers of electronic communications services are sufficiently serious to warrant the interference entailed by such access with the fundamental rights enshrined in Articles 7 and 8 of the Charter, as interpreted by the Court in its judgment of 8 April 2014, *Digital Rights Ireland and Others* (C−293/12 and C−594/12, EU:C:2014:238), and in *Tele2 Sverige and Watson and Others*.

51 As to the existence of an interference with those fundamental rights, it should be borne in mind, as observed by the Advocate General in points 76 and 77 of his Opinion, that the access of public authorities to such data constitutes an interference with the fundamental right to respect for private life, enshrined in Article 7 of the Charter, even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. Such access also constitutes interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter, as it constitutes processing of personal data (see, to that effect, *Opinion 1/15 (EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, points 124 and 126 and the case-law cited).

52 As regards the objectives that are capable of justifying national legislation, such as that at issue in the main proceedings, governing the access of public authorities to data retained by providers of electronic communications services and thereby derogating from the principle of confidentiality of electronic communications, it must be borne in mind that the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, as a result of which that access must correspond, genuinely and strictly, to one of those objectives (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraphs 90 and 115).

53 As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, it should be noted that the wording of the first sentence of Article 15(1) of Directive 2002/58 does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally.

54 In that regard, the Court has admittedly held that, in areas of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraph 99).

55 However, the Court explained its interpretation by reference to the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraph 115).

56 In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'.

57 By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally.

58 It should therefore, first of all, be determined whether, in the present case, in the light of the facts of the case, the interference with fundamental rights enshrined in Articles 7 and 8 of the Charter that police access to the data in question in the main proceedings would entail must be regarded as 'serious'.

59 In that regard, the sole purpose of the request at issue in the main proceedings, by which the police seeks, for the purposes of a criminal investigation, a court authorisation to access personal data retained by providers of electronic communications services, is to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone. As noted in paragraph 40 of the present judgment, that request seeks access to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern, as confirmed by both the Spanish Government and the Public Prosecutor's Office during the hearing, the communications carried out with the stolen mobile telephone or its location.

60 It is therefore apparent that the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.

61 In those circumstances, access to only the data referred to in the request at issue in the main proceedings cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned.

62 As stated in paragraphs 53 to 57 of this judgment, the interference that access to such data entails is therefore capable of being justified by the objective, to which the first sentence of Article 15(1) of Directive 2002/58 refers, of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious'.

63 In the light of the foregoing considerations, the answer to the questions referred is that Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.

Costs

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

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

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 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter of Fundamental Rights, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.

[Signatures]

---

* Language of the case: Spanish.