Provisional text

OPINION OF ADVOCATE GENERAL
SAUGMANDSGAARD ØE
Delivered on 3 May 2018 (1)

**Case C-207/16**

**Ministerio Fiscal**

(Request for a preliminary ruling from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain))

(Reference for a preliminary ruling — Electronic communications — Processing of personal data — Right to private life and right to protection of personal data — Directive 2002/58/EC — Article 1 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7 and 8 and Article 52(1) — Data collected in the context of the provision of electronic communications services — Request for access by a police authority for the purposes of a criminal investigation — Principle of proportionality — Concept of 'serious crime' capable of justifying an interference with fundamental rights — Criteria of seriousness — Penalty incurred — Minimum threshold)

## I. Introduction

1. This reference for a preliminary ruling concerns, in essence, the interpretation of the concept of 'serious crime' (2) within the meaning of the case-law of the Court resulting from the judgment in *Digital Rights Ireland and Others* (3) ('the judgment in *Digital Rights*') and then from the judgment in *Tele2 Sverige and Watson and Others* (4) ('the judgment in *Tele2*'), where that concept was used as a criterion for the assessment of the lawfulness and proportionality of an interference with the rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter'), namely, respectively, the right to respect for private and family life and the right to protection of personal data.

2. This reference for a preliminary ruling was made in the context of an action brought against a judicial decision whereby the police authorities were denied the possibility of receiving communication of certain identification data held by mobile telephony operators for the purpose of identifying individuals in the context of a criminal investigation. The contested decision was based, in particular, on the consideration that the facts giving rise to that investigation did not constitute serious crime, contrary to the requirements of the applicable Spanish legislation.

3. The referring court asks the Court, in essence, about the way in which the threshold of seriousness of infringements must be fixed beyond which there may be justification, in the light of the case-law referred to above, for interfering with the fundamental rights protected by Articles 7 and 8 of the Charter when the competent national authorities have access to personal data retained by electronic communications service providers.

4. After having established that the Court has jurisdiction to rule on that request for a preliminary ruling, and that the request is admissible, I propose to show that access to personal data in circumstances such as those of the present case entails an interference with the abovementioned fundamental rights which does not correspond to situations in which only the fight against serious infringements is capable of justifying the breach of those rights, in accordance with the case-law cited above.

5. Since I consider that, having regard to the particular subject matter of the main proceedings, it will not be necessary for the Court to answer the questions as initially worded, it is only in the alternative that I shall provide indications as to the criteria that might make it possible to define the concept of 'serious crime' within the meaning of that case-law, in particular with regard to the criterion of the penalty incurred.

## II. Legal framework

### *A. European Union law*

6. 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), (5) as amended by Directive 2009/136/EC, (6) ('Directive 2002/58') states in its preamble:

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

…

(11) Like Directive 95/46/EC, [(7)] 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 ['the ECHR'], as interpreted by the rulings of the European Court of Human Rights ['the ECtHR']. 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 [ECHR]. [(8)]'

7. In the words of Article 1 of Directive 2002/58, entitled 'Scope and aim':

'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. …

…

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.'

8. Article 2 of that directive, 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) [(9)] shall apply.

The following definitions shall also apply:

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

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

(c) "location data" means any data processed in an electronic communications network, 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;

…'

9. Article 15 of Directive 2002/58, entitled 'Application of certain provisions of Directive [95/46]', provides, in paragraph 1, that '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'.

### *B. Spanish law*

#### *1. Law 25/2007*

10. La 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 (10) ('Law 25/2007') transposed Directive 2006/24, (11) which was declared invalid by the Court in the judgment in *Digital Rights*, into Spanish law.

11. In the words of Article 1 of Law 25/2007, in the version applicable to the facts of the main proceedings:

'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.

…'

12. Article 3 of that law lists the data which operators are required to retain. They include, in particular, pursuant to paragraph 1(a)(1)(ii) of that article, the data necessary in order to retrieve and identify the source of a communication, such as, in the case of mobile telephony, the name and address of the subscriber or the registered user.

### *2. The Criminal Code*

13. Under Article 13(1) of the Spanish Criminal Code, in the version applicable to the facts of the main proceedings, 'serious offences are those which the law punishes with a serious penalty'.

14. Article 33 of the Criminal Code is worded as follows:

'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.

…'

### *3. The Code of Criminal Procedure*

15. The Spanish 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 (12) ('Organic Law 13/2015').

16. That law, which entered into force on 6 December 2015, incorporates, in the Code of Criminal Procedure, the sphere of access to telephone and telematic communications data which have been retained by electronic communications services providers.

17. In the words of Article 579(1) of the Code of Criminal Procedure, in the version as amended by that law, '[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 that Code, entitled ‘Data available in the electronic archives of service providers’, states:

‘1. Electronic data retained by service providers or by persons who supply the communication in application of 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 procedure 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 electronic 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.’

## III. The main proceedings, the questions for a preliminary ruling and the procedure before the Court

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

20. By application of 27 February 2015, the police requested the Juzgado de Instrucción No 3 de Tarragona (Court of Preliminary Investigation No 3, Tarragona, Spain, ‘the Court of Preliminary Investigation’) to order the various telephone operators to communicate (i) the telephone numbers which had been activated, between 16 February and 27 February 2015, with the IMEI code (13) of the stolen mobile telephone and (ii) the personal data of the owners or users of all the telephone numbers corresponding to the SIM cards activated by that IMEI code. (14)

21. By order of 5 May 2015, the Court of Preliminary Investigation refused that request, on the grounds that the requested measure would not serve to identify the perpetrators of the offence and that, in any event, Law 25/2007 limited the communication of the data retained by the telephone operators to serious offences — namely, according to the Spanish Criminal Code, (15) to those punishable by a term of imprisonment of more than five years —, while the facts at issue did not constitute a serious offence.

22. The Ministerio Fiscal (Spanish Public Prosecutor’s Office), the only party to the proceedings, appealed against that order before the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain), claiming that communication of the data at issue ought to have been allowed by reason of the nature of the facts and a decision of the Tribunal Supremo (Supreme Court, Spain) relating to a similar case. (16)

23. By order of 9 February 2016, that court, by way of a provisional measure addressed to the telephone operators, ordered the extension of the period of retention of the data to which the request at issue related.

24. The order for reference from that court states that, after the adoption of the contested decision, the Spanish legislature introduced, in Organic Law 13/2015, (17) two 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. (18) The second is a formal normative criterion, based exclusively on the penalty prescribed for the offence in question. In fact, the threshold of three years’ imprisonment which that criterion envisages might encompass the great majority of criminal classifications. In addition, the referring court observes that the State’s interest in protecting citizens and repressing criminal conduct cannot confer legitimacy on a disproportionate interference with the fundamental rights of individuals.

25. In that context, by decision of 6 April 2016, received at the Court on 14 April 2016, the Audiencia Provincial de Tarragona (Provincial Court, Tarragona) decided to stay proceedings and to refer the following questions to the Court 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 [in *Digital Rights*] as standards for the strict review of the directive [declared invalid in that judgment], 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?’

26. The procedure before the Court was stayed, by decision of the President of 23 May 2016, pending delivery of the judgment of the Court in Joined Cases *Tele2 Sverige and Watson and Others*, C−203/15 and C−698/15.

27. Questioned by the Court following the delivery of that judgment, on 21 December 2016, (19) the referring court stated that it intended to maintain its request for a preliminary ruling. It claimed that the questions which it had submitted were still relevant, since that judgment admittedly gave examples of serious offences, (20) but did not define with sufficient clarity the substantive content of the concept of seriousness of the offence that could serve as a criterion for the assessment of the justification for a measure of interference. According to the referring court, that concept gives rise to the risk that the conditions governing retention of and access to the data will be determined, at national level, very broadly, which would not respect the fundamental rights referred to in the judgment in *Tele2*. Thus, when adopting Organic Law 13/2015, the Spanish legislature, in spite of the criteria laid down in the judgment in *Digital Rights*, (21) very significantly reduced, by comparison with the earlier rules laid down in Law 25/2007, the threshold of seriousness of the offences in respect of which the retention and communication of personal data are permitted.

28. Following that reply, the procedure before the Court was resumed on 16 February 2017. Written submissions were then lodged by the Spanish, Czech and Estonian Governments, Ireland, the French, Latvian, Hungarian, Austrian and United Kingdom Governments and the European Commission.

29. With a view to the hearing, the Court put a number of questions for a written answer to the Spanish Government, to which it replied on 9 January 2018, and also a number of questions for an oral answer to all of the interested parties referred to in Article 23 of the Statute of the Court of Justice of the European Union.

30. At the hearing, which was held on 29 January 2018, the Spanish Public Prosecutor’s Office, the Spanish, Czech, Danish and Estonian Governments, Ireland, the French, Latvian, Polish and United Kingdom Governments and the Commission submitted their oral observations.

## IV. Analysis

### *A. Introductory observations*

31. Before examining in detail the issues raised by the present request for a preliminary ruling, I consider it necessary to make a few observations concerning the specific subject matter of that request.

32. *First*, in the light of the information set out in the order for reference and the additional information supplied by the Spanish Government, I observe that the *main proceedings* have a number of notable features that distinguish it, in particular, from the context of the cases that gave rise to the judgments in *Digital Rights* and *Tele2*. (22)

33. In fact, it is apparent that the police authorities' request at issue in this case seeks to obtain *only* data that would make it possible to identify the owners or users of the telephone numbers linked with the SIM cards that were inserted in the stolen mobile telephone. (23) In addition, it is common ground that that request concerns a clearly defined period of short duration, namely around 12 days. (24)

34. In such circumstances, the number of persons capable of being affected by the measure at issue is not unlimited, but restricted. In addition, those persons are not just any person in possession of a SIM card, but individuals with a very specific profile, namely those who have used the stolen telephone after it was taken, and indeed may still have it in their possession, and who may therefore be lawfully suspected either of themselves being the perpetrators of the offence or of being connected with those perpetrators.

35. What is more, the data referred to correspond not to every type of 'personal data' (25) held by the electronic communications services providers but only to those relating to the identity of the abovementioned individuals, namely their forenames, surnames and possibly their addresses, (26) data that can also be called 'contact data'. The other information relating to those individuals that might be found in the providers' archives (27) are in my view excluded from the main proceedings.

36. Furthermore, the aim pursued here is to my mind to gather information which does not relate either to a location or to communications as such, (28) but to natural persons who are sought for having used an electronic communications service by means of the stolen telephone, even if they did not make an actual telephone call. It follows from the explanations provided to the Court by the Spanish Public Prosecutor's Office that the personal data requested, which are derived from the connection between a specific SIM card and the IMEI number of the stolen device, can technically be obtained by means of a simple connection between the device and a mobile telephony terminal, even though no call has been made by the holder of the card by means of the telephone concerned, and therefore independently of any actual communication. (29) It will therefore be for the referring court to verify that factual assertion, which, however, seems to me to be sufficiently plausible for it to be reasonable to accept it as true.

37. Having regard to all of those factors, I would emphasise at the outset that the main proceedings concern personal data the transmission of which is sought not in a general and indiscriminate manner, but in a targeted manner as regards the persons concerned and one that is limited in duration. In addition, the requested data seem at first sight not to be of a particularly sensitive nature, although the fundamental rights enshrined in Articles 7 and 8 of the Charter are nonetheless capable of being affected by access to data of that type. (30)

38. *Second*, I note that it is apparent from the grounds of the order for reference that the questions submitted in the present case have the characteristic that they relate not to the conditions governing the *retention* of personal data in the electronic communications sector, but rather to the rules on *access* by the national authorities to such data which have been retained by the service providers operating in that sector. (31)

39. The referring court states, in particular, that under Article 588 *ter* j of the Code of Criminal Procedure, judicial authorisation is required in order for the electronic data archived by the service providers to be transmitted to the competent authorities for the purpose of being taken into account in the context of a procedure. Paragraph 1 of that article states that such data may have been retained by service providers either in application of the relevant legislation or on their own initiative for commercial or other reasons.

40. In this instance, it is apparent that the personal data to which the police authorities seek access, for the purposes of the investigation, may have been archived by the mobile telephone operators in order to

comply with an obligation resulting from Spanish law. (32) The referring court provides no information on that point, as its request for a preliminary ruling is focused on possible access to data which have already been retained and since that the conformity of the storage of the data with the requirements of EU law is not called into question in the main proceedings. (33) It is therefore appropriate in my view to take as a basis the premiss that the data at issue in the main proceedings were retained in accordance with the national legislation, in compliance with the conditions laid down in Article 15(1) of Directive 2002/58, which it is for the referring court alone to verify. (34)

41. I shall return, in the following developments, to the legal implications of the preliminary observations made here. (35)

### *B. The procedural objections raised by the Spanish Government*

42. The Spanish Government has raised two categories of procedural objections, one relating to the jurisdiction of the Court and the other to the admissibility of the request for a preliminary ruling, on which the Court will have to rule before adjudicating on the substance, if necessary.

#### *1. The Court's jurisdiction in the light of the scope of EU law*

43. First of all, I recall that it has consistently been held that the fundamental rights guaranteed in the legal order of the European Union, and in particular those enshrined in Articles 7 and 8 of the Charter, are applicable only if the situation in question is governed by EU law. (36) Furthermore, Article 51(1) of the Charter provides that the provisions of the Charter are addressed to the Member States only 'when they are implementing Union law, within the meaning of the case-law of the Court relating to that concept. (37) Accordingly, where a legal situation is not covered by the scope of EU law, the Court does not have jurisdiction to rule on it and any provisions of the Charter relied on cannot, of themselves, form the basis for such jurisdiction. (38)

44. In the present case, the questions submitted by the referring court refer only to Articles 7 and 8 of the Charter and to 'the fundamental principles of EU law applied by the Court in [the judgment in *Digital Rights*']. However, the referring court considers that the directives applicable in personal data protection matters, such as Directive 95/46 and Directive 2002/58, establish the link required, under Article 51(1) of the Charter, between the main proceedings and EU law.

45. In that regard, I observe, *in the first place*, that the Spanish Government maintains, primarily, that the Court does not have the requisite jurisdiction to adjudicate on this reference for a preliminary ruling, on the ground that the reference does not concern the application of EU law. It claims, in particular, that the main proceedings are *excluded from the scope of EU law*, since they concern access by the police to data which was the subject of a judicial decision in the context of an investigation, which constitutes an activity of the State in criminal matters (39) and therefore comes within the exceptions provided for in Article 1(3) of Directive 2002/58 and also in the first indent of Article 3(2) of Directive 95/46. (40) At the hearing, the United Kingdom Government stated that it shared the Spanish Government's viewpoint.

46. However, I consider that Directive 2002/58 is applicable with regard to national measures such as those at issue in the main proceedings. The Court has already held, in the judgment in *Tele2*, that national legislation relating to the retention of data for the purpose of combating crime are covered by the scope of that directive, not only in that they define the obligations borne in that respect by electronic communications service providers, but also in that they govern access by the national authorities to the data retained in that context. (41) Like the Commission, I am of the view that the considerations set out in that judgment can be applied by analogy to the national rules applicable in this case, namely to those resulting from Law 25/2007 read in conjunction with the Spanish Code of Criminal Procedure as amended by Organic Law 13/2015, (42) and can therefore be applied by analogy to the subject matter of the main proceedings.

47. I would add that the personal data processed *directly* in the context of the activities — of a sovereign nature (43) — of the State in a field governed by criminal law (44) must not be confused with the data processed in the context of the activities — of a commercial nature — of an electronic communications service provider which are *then* used by the competent State authorities. (45) Moreover, I note that a reference has recently been made to the Court concerning, in particular, the interpretation of Article 1(3) of Directive 2002/58 in connection with the use, by the Security and Intelligence Agencies of a Member State, of data that had to be transferred to those agencies in bulk by such providers, (46) a problem which, to my mind, will not need to be addressed in the present case. (47)

48. *In the second place*, I observe that other questions have been asked concerning the *scope of Directive 2002/58*, on which the Court's jurisdiction in the present case depends, with regard to the *type of data at issue in the main proceedings*.

49. As I have already indicated, (48) it is apparent from the material on the file that the request for access at issue seeks to obtain information about the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated by means of the stolen mobile telephone, in order to discover the persons who had that device, and not information about any calls that might have been made from the device.

50. In other words, even though a larger range of personal data might potentially have been concerned in the light of the Spanish legislation, (49) the present dispute in the main proceedings concerns data which relate only to the identity of 'users', within the meaning of Article 2(a) of Directive 2002/58, and not to any 'location', (50) within the meaning of Article 2(c) or 'communications' as such, within the meaning of Article 2(d) of that directive. (51)

51. According to the Spanish Public Prosecutor's Office, the Spanish and Danish Governments, Ireland, the Latvian and United Kingdom Governments and the Commission, information such as that at issue here, provided that it is taken into account in isolation, that is to say, independently of the communications made, where appropriate, should also not in principle be covered by the concept of 'traffic data' within the meaning of Article 2(b), which defines such data as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'. (52)

52. Admittedly, it seems that the identification data requested here by the police authorities do not concern the 'traffic' of communications in the strict sense, in so far as it appears that those data may be obtained notwithstanding the complete absence of telephone calls made with the stolen device, and therefore even if no interpersonal communication has been conveyed by a mobile telephone operator during the targeted period. (53)

53. Nonetheless, I consider that a dispute such as that in the main proceedings comes within the scope of Directive 2002/58, since the processing of the information associated with the SIM cards and their owners, referred to in the present case, is necessary, from a commercial viewpoint, for the provision of the electronic communications services, (54) at least for purposes of charging for the service provided (55) irrespective of the calls made or not made in the context of that provision of services.

54. In fact, having regard to Article 1(1) and Article 3 of Directive 2002/58, (56) I share the opinion expressed, in particular, by the Commission, that that directive is intended to govern, in a comprehensive manner, the processing of personal data carried out in the context of the provision of electronic communications services, so that its scope includes data relating to the identity of users of such services, like those involved here, and not only the data associated with a specific communication. Having regard, also, to the objectives of protection referred to in that directive, which consist mainly in safeguarding fundamental rights guaranteed by the Charter, (57) I therefore consider that the concept of 'communication', within the meaning of that measure, must be understood broadly and that the principle of confidentiality of communications laid down in that measure (58) is indeed at stake in the present case.

55. I am also of the view that that interpretation is corroborated by an earlier judgment of the Court, in which the Court accepted that the scope of Directive 2002/58 covered a dispute concerning the conveyance of the names and addresses of users of an electronic communications service. (59) I would add that Article 12 of that directive, which concerns directories of subscribers, in my view certainly covers data of that nature (60) and that recital 15 also reflects a flexible conception of 'communication', including, in particular, 'addressing information provided by the sender of a communication'. (61)

56. In addition, such an approach is consistent with the case-law of the ECtHR on data protection, (62) it being noted that the preamble to Directive 2002/58 makes clear that that directive is intended to guarantee the confidentiality of communications and the right of users to private life in accordance with the ECHR as interpreted by that Court, (63) even though the ECHR is not formally integrated in the legal order of the European Union. (64)

57. Consequently, I consider that a dispute such as that in the main proceedings comes within the material scope of Directive 2002/58 and that the objection of lack of jurisdiction raised by the Spanish Government must therefore be rejected.

58. In the interest of completeness, I would point out, however, that, if Directive 2002/58 should not be recognised as applicable in such a situation, Directive 95/46, on which both the referring court and the Spanish Government rely, could not constitute a basis for the Court's jurisdiction to adjudicate in the present case.

59. In fact, as the Commission submits, Directive 95/46 does indeed constitute the instrument of general application as regards the processing of personal data, (65) but the questions raised by the referring court would in my view be devoid of relevance if they were examined from that aspect alone, since their object is to determine the threshold beyond which offences may be classified as 'serious' within the meaning of the case-law resulting from the judgments in *Digital Rights* and *Tele2*, which did not concern the interpretation of that directive. (66)

### *2. The admissibility of the request for a preliminary ruling*

60. The Spanish Government claims, in the alternative, that if the Court should decide that it has jurisdiction to answer the questions referred to it, the request for a preliminary ruling should be declared inadmissible, for two reasons.

61. *In the first place*, the Spanish Government claims that the referring court *does not clearly define the EU normative framework* on which the Court should rule.

62. On that point, it refers to the consistent case-law according to which, in the context of the cooperation established by Article 267 TFEU, the Court can refuse to give a ruling on questions referred for a preliminary ruling, which enjoy a presumption of relevance, only where it is quite obvious that the interpretation, or the determination of validity, of a rule 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. (67)

63. However, I consider that in this instance the Spanish Government's complaint is not well founded. In the light of the information provided by the referring court, I consider that that court has sufficiently identified the provisions of EU law which in its view are relevant. I recall that the questions submitted refer in particular to Articles 7 and 8 of the Charter and that the referring court explains that Directives 95/46 and 2002/58 constitute the necessary link between the national legislation applicable in the main proceedings and EU law (68) and, last, that Directive 2002/58 seeks, as stated in recital 2, to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter. (69)

64. I would add that it is immaterial that one of the pieces of Spanish legislation mentioned in the order for reference, namely Law 25/2007, was intended to transpose Directive 2006/24, which was repealed after being declared invalid in the judgment in *Digital Rights*. (70) As the referring court rightly observes, it would be wrong to consider that the questions referred to the Court for a preliminary ruling in this case are irrelevant because that directive was declared invalid. On that point, it is sufficient to state that the matter to which those questions relate, namely the protection of personal data, comes within the competence of the European Union and that the main proceedings are covered by the scope of an act of EU law, namely 2002/58, (71) which Directive 2006/24, which was declared invalid, was intended to amend.

65. It may also be observed that by far the majority of the parties who submitted observations to the Court proceed from the principle that the present request for a preliminary ruling must be examined in the light of Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, and on the basis of the lessons learned from the judgments in *Digital Rights* and *Tele2*. That is also my view, it being noted that the expression 'criminal offences', and not 'serious offences' appears in 2002/58, only in Article 15(1). (72)

66. *In the second place*, the Spanish Government maintains that *Article 7of the Charter*, which is the central element of the present request for a preliminary ruling, *is not relevant*, on the ground that the measure of investigation sought in the main proceedings does not concern the interception of communications and cannot therefore affect the confidentiality of the communications, so that the questions submitted are hypothetical.

67. For my part, I consider that Article 7 of the Charter is indeed relevant in the present case and that the request for a preliminary ruling is therefore not hypothetical in nature. While it is true that, in this case, there is no risk of a breach of the right to the secrecy of communications, having regard to the object of the measure at issue in the main proceedings, (73) the fact nonetheless remains that a measure of that type is apt to constitute an interference with the right to respect for private life guaranteed by that provision, albeit in my view a minor interference. (74)

68. In fact, as the Court has already consistently held, the communication of personal data to a third party, such a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, irrespective of the use to which the information communicated is subsequently put. The same applies to the retention of personal data, in particular by electronic communications service providers, and to access to those data with a view to their being used by the public authorities. (75)

69. Accordingly, I am of the view that the plea of inadmissibility raised by the Spanish Government must be rejected and that it is therefore necessary to give a ruling on the substance of the request for a preliminary ruling.

### *C. The factors required in order to characterise the sufficient seriousness of an offence justifying an interference with the fundamental rights in question (first question)*

70. By its first question, the referring court asks the Court, in essence, about the factors that must be taken into account for the purpose of establishing that the criminal offences are of sufficient seriousness to justify an interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter, in the context of the retention of and access to personal data, in accordance with the case-law resulting from the judgment in *Digital Rights*, followed by the judgment in *Tele2*.

71. On that topic, I recall that the concept of '*infractions graves*' ('serious crime') was used by the Court in the judgment in *Digital Rights*, (76) sometimes in conjunction with the concept of '*criminalité grave*' ('serious crime'), (77) as a criterion for verifying the purpose and the proportionality of the interference with the abovementioned fundamental rights entailed by provisions of EU law relating to personal data, namely the provisions of Directive 2006/24. I would point out that that concept, which does not appear in Directive 2002/58, (78) was used in Directive 2006/24, (79) which was declared invalid in that judgment. The Court then used those two concepts in the judgment in *Tele2*, (80) as the same criterion

of assessment, but relating this time to the consistency with EU law (81) of provisions adopted by Member States.

72. More specifically, the first question asks the Court to rule on whether, for the purposes of assessing the existence of a 'serious offence' capable of justifying an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter with regard to personal data, only the penalty incurred for the offence at issue must be taken into consideration or whether, in addition, the particularly harmful nature of the criminal conduct with regard to the individual or collective legal interests involved, must also be taken into consideration.

73. However, like the Commission, I consider that, before ruling on that question, it is appropriate to consider whether the interference at issue in a dispute such as that in the main proceedings presents a sufficiently high degree of seriousness for it to be necessary, under EU law, for that interference to be justified by the fight against serious crime in order to be permitted. In fact, it seems to me that if that is not the case, the Court should interpret the relevant provisions of EU law, not by adhering to what is sought by the referring court, but after having reformulated the first question (82) as much as necessary in the light of the circumstances of the main proceedings. (83)

### *1. The taking into account of the absence of seriousness of the interference at issue*

74. *First of all*, it is appropriate to establish that operations such as those at issue in the main proceedings are indeed capable of constituting a breach of the fundamental rights guaranteed by Articles 7 and 8 of the Charter, and therefore of *constituting an interference* with those rights, within the meaning of the case-law deriving from the judgments in *Digital Rights* and *Tele2*.

75. Admittedly, as the Spanish and Danish Governments submitted in their oral pleadings, (84) and as I have already stated, (85) the data to which the authorities responsible for the criminal investigation in question wish to have access seem to be less sensitive than certain other categories of personal data (86) as the request at issue appears to relate only to the surnames, forenames and possibly the addresses of the individuals targeted by the investigation, as users of telephone numbers activated from the mobile telephone forming the subject matter of the investigation.

76. However, I consider that for the purpose of determining whether personal data must be covered by the protection provided for in EU law, and in particular by Directive 2002/58, (87) it is immaterial whether the information referred to by the request for retention or communication is particularly sensitive or not. In fact, as was observed in the context of the first legislative work dealing with the matter, 'depending on the use to which it is put, any item of data relating to an individual, harmless though it may seem, may be sensitive (e.g. a mere postal address)'. (88) In addition, the Court has already held that, for the purposes of characterising *the existence of an interference* with the fundamental right enshrined in Article 7 of the Charter, 'it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way'. (89)

77. Furthermore, I recall that the communication of personal data to a third party, even a public authority such as the police, constitutes an interference with the fundamental right guaranteed in Article 7 of the Charter, (90) including where that information is conveyed for the purposes of a criminal investigation, a situation, moreover, which is expressly referred to in Article 15(1) of Directive 2002/58. (91) I would add that an operation of that type may also constitute a breach of the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter, since it involves the processing of personal data. (92)

78. Therefore, I consider that it must be held that a measure such as that at issue in the main proceedings constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

79. *However*, I consider that, in the circumstances of the present case, an essential element identified by the Court in order to require, at the stage of providing justification for such an interference, that there is a

'serious offence' — a concept the definition of which is requested by the referring court — for the purposes of being able to derogate from the principle of confidentiality of electronic communications, is missing. The element which in my view is *missing* in the present case, in order to provide an answer to the first question in the terms used by that court, is the *seriousness of the interference at issue*, a factor which, if it were present, would give rise to the need for enhanced justification.

80. In that regard, I observe that, in the judgment in *Digital Rights*, the Court highlighted the great breadth and the particularly serious nature of the interference produced by the legislation at issue, observing in particular that 'Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime'. (93)

81. Likewise, in the judgment in *Tele2*, the Court ruled that 'Article 15(1) of Directive 2002/58 … preclude[es] national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication'. (94) A link was also made in that judgment between, on the one hand, the particular 'seriousness of the interference' and, on the other, the need to justify a breach of such magnitude vis-à-vis the fundamental rights guaranteed by Articles 7 and 8 of the Charter, in reliance on a ground of general interest as basic as the 'fight against serous crime'. (95)

82. That establishment of a link between the seriousness of the interference found and the seriousness of the reason that could justify the interference was made in line with the principle of proportionality. (96) In addition, it seems to me that the ECtHR, in its case-law relating to Article 8 of the ECHR, (97) has established a link equivalent to that which in my view emerges from the judgments in *Digital Rights* and *Tele2*.

83. As I stated above (98) and as, more especially, the French and United Kingdom Governments and the Commission have emphasised, the nature of the interference at issue in the main proceedings is in several respects distinct from those envisaged by the Court in those two judgments. The examination of the conformity with EU law of a measure such as that concerned here must therefore take a different course.

84. In the present case, the measure in question is not one that relates to a general and undifferentiated obligation to retain traffic and location data of every subscriber or registered user that would concern all means of electronic communication, but a targeted measure intended to allow access, by competent authorities and for the needs of a criminal investigation, to data held for commercial purposes by service providers and relating solely to the identity (surnames, forenames and possibly addresses) of a restricted category of subscribers or users of a specific means of communication, namely those whose telephone numbers were activated from the mobile telephone the theft of which forms the subject matter of the investigation, during a limited period, namely around 12 days. (99)

85. I would add that the potentially harmful effects for the persons concerned by the request for access in question are both slight and circumscribed. As they are intended to be used in the sole context of a measure of investigation, the requested data are not intended to be disclosed to the public at large. (100) In addition, the right of access given to the police authorities is accompanied by procedural guarantees under Spanish law, since it is subject to review by a court, which, moreover, resulted in the rejection of the police request in the main proceedings.

86. The interference with the abovementioned fundamental rights entailed by the communication of those data relating to civil identity is not in my view particularly serious, (101) since data of such a type and such a limited scope do not in themselves make it possible to obtain varied and/or specific information about the persons concerned (102) and therefore do not directly and seriously affect their right to a private life in those particular circumstances. (103)

87. *Accordingly*, like the Commission, I consider that, in order to provide the referring court with the relevant information to settle the dispute before it, it is necessary to *reformulate* the first question so that

the Court's forthcoming answer relates to the interpretation of Article 15(1) of Directive 2002/58 in the light of circumstances such as those of the present case, namely where there is an interference with the abovementioned fundamental rights which is not particularly serious and which is based on the fight against a type of criminal offences the seriousness of which is open to question.

88. In that regard, I recall that, since the objectives capable of justifying national legislation derogating from the principle of confidentiality of electronic communications are listed exhaustively in Article 15(1) of Directive 2002/58, access to the retained data must correspond effectively and strictly to one of those objectives. (104) Those objectives include the general-interest objective of 'the prevention, investigation, detection and prosecution of *criminal offences*', (105) without further detail as to the nature of those offences.

89. It is apparent from the terminology thus used that it is not essential that the offences conferring legitimacy on the restrictive measure at issue, under Article 15(1), may be classified as 'serious' within the meaning of the case-law resulting from the judgments in *Digital Rights* and *Tele2*. In my view, it is only where the interference is particularly serious, as in the cases that gave rise to those judgments, that the offences capable of justifying such an interference must themselves be particularly serious. On the other hand, in the case of a non-serious interference, it is necessary to go back to the basic principle that emerges from the wording of that provision, namely that any type of 'criminal offence' is capable of justifying such an interference.

90. To my mind, it is necessary not to adopt too broad a conception of the requirements laid down by the Court in those two judgments, in order not to impede, or in any event not to do so excessively, the possibility for Member States to derogate from the regime established by Directive 2002/58, which is granted to them by Article 15(1) of that directive, in cases where the intrusions into private life in question have both a legitimate purpose and a limited scope, such as those that could be entailed in the present case by the police request. More specifically, I am of the view that EU law does not preclude the competent authorities from having access to identification data, held by electronic communications services providers, that make it possible to find the presumed perpetrators of a criminal offence that is not of a serious nature.

91. Consequently, I recommend that the Court's *answer to the question for a preliminary ruling, as reformulated*, should be that Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and of Article 52(1) of the Charter, must be interpreted as meaning that a measure allowing the competent national authorities to have access, for purposes associated with combating criminal offences, to the identification data of users of telephone numbers activated from a specific mobile telephone during a limited period, in circumstances such as those at issue in the main proceedings, entails an interference with the fundamental rights guaranteed by that directive and by the Charter which does not attain a sufficient level of seriousness for such access to be confined to cases in which the offence concerned is of a serious nature.

92. Having regard to the answer thus proposed, all of the following observations will be submitted purely in the *alternative*, in the interest of being comprehensive.

### *2. The possible determination of the criteria for characterising the sufficient seriousness of an offence*

93. In case the Court should decide, contrary to my recommendation, that it is appropriate, notwithstanding the very particular circumstances of the main proceedings, to determine, in the present case, what must be understood by a 'serious offence' within the meaning of the case-law resulting from the judgments in *Digital Rights* and *Tele2*, (106) it would still be appropriate to examine, *in the first place*, whether that classification does indeed constitute an *autonomous concept* of EU law, which it would therefore be for the Court to define. In accordance with the answer primarily proposed by the French Government, I am not convinced that that is so, for the following reasons.

94. First of all, I observe that Directive 2006/24, from which the use of the concept of 'serious crime' comes, (107) did not contain a definition of that concept, but referred in that respect to the legal orders of

the Member States. (108) I would add that the relevant considerations in the judgments in *Digital Rights* and *Tele2* must not in my view be understood as tending to harmonise the legal rules in force in the Member States as regards the content of that concept.

95. In that regard, I recall 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. (109) In the words of Article 83(2) TFEU, it is only if the approximation of the criminal law of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures that the Union may adopt directives to establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. As EU law currently stands, there is no provision of general application that would provide a harmonised definition of the concept of 'serious crime'. (110)

96. It seems to me that the power to determine what constitutes 'serious crime' belongs, in principle, to the competent authorities of the Member States. Nonetheless, because of the references for a preliminary ruling which the Member States may submit to it, the Court is responsible for ensuring compliance with all the requirements resulting from EU law, and in particular for ensuring the consistent application of the protection afforded by the provisions of the Charter.

97. I would observe that the legal classification in question may not only vary from one Member State to another, depending on the traditions followed and the priorities defined by each of them, but also fluctuate over time, according to the course taken by criminal policy, towards greater or indeed lesser severity, in order to take account of developments in crime (111) and also, more generally, changes in society and needs existing, in particular in terms of criminal law enforcement, at national level.

98. In addition, I would emphasise that, given that there are significant differences between the scales of penalties traditionally applicable in the various Member States, (112) the seriousness of an offence does not relate solely to the magnitude of the associated penalty. Whether an offence is a serious offence is very relative, in that it depends on the scale of penalties generally applied in the Member State concerned. Thus, the fact that a Member State lays down a short term of imprisonment, or even an alternative penalty to imprisonment, does not prejudge the intrinsic seriousness of the type of offence concerned. (113)

99. It is necessary, in my view, to respect the specific characteristics of the criminal law system of each of the Member States, in so far as EU law does not set out obligations which are strictly binding on the Member States, by analogy with what the Court has held as regards the protection of public security, (114) a concept which to my mind is similar to the concept of the fight against serious crime, in particular having regard to the wording of the first sentence of Article 15(1) of Directive 2002/58.

100. Consequently, I am of the view, in the alternative, that the concept of 'serious crime' within the meaning of the case-law of the Court resulting from the judgments in *Digital Rights* and *Tele2* is not an autonomous concept of EU law the content of which must be defined by the Court, although the fact nonetheless remains that the derogation provided for in Article 15(1) of Directive 2002/58 must be implemented by the Member States in accordance with the fundamental rights guaranteed by the Charter, and that such implementation must be subject to review by the Court.

101. On this last point, I note that it follows from the case-law of the Court, in particular, that Article 15(1), in that it allows the Member States to restrict the scope of certain rights and obligations provided for in that directive, must be interpreted strictly and cannot therefore result in the derogation from those rights and obligations of principle becoming the rule. (115) Accordingly, the scope of the concept of 'serious crime' cannot be understood in an excessively broad fashion by the Member States.

102. *In the second place*, and very much in the alternative, *if the Court should consider that that concept is autonomous*, it would then have to answer the question as formulated by the referring court and therefore have to rule on the determination of the criteria on which it may be assessed, at EU level, whether a

criminal offence is sufficiently serious to justify an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

103. More specifically, the Court would have to determine whether, in order to establish the existence of 'serious crime' within the meaning of that case-law, it is sufficient to rely on the penalty prescribed for the alleged offence or whether, in addition, the unlawful conduct must have been particularly harmful to the individual or collective legal interests involved. In that regard, it would be appropriate, in my view and also according to the Danish, Spanish, French, Hungarian, Austrian, Polish and United Kingdom Governments, to opt not for the first part of that alternative, but for the second part in essence, preferring a definition based on *a number of criteria of assessment*. (116)

104. As regards the seriousness of the offence that is capable of justifying access to the data, in my view it would be impossible, having regard to the principle of proportionality, to determine the seriousness of the offences by taking into account only the penalty that might be imposed. In fact, in the light of the significant differences which still exist between the criminal systems of the Member States, I consider that the penalty incurred cannot be considered to be capable in itself of reflecting, whether from the qualitative aspect of the type of penalty and/or from the quantitative aspect of the level of the penalty, the particular seriousness of a criminal offence.

105. Even though the penalty assumes considerable importance, other objective factors must also be taken into account, on a case-by-case basis, in that respect. These are, more especially, first, the context of which the alleged offence forms part — in that the unlawful conduct is intentional, is accompanied by aggravating circumstances, was a second or subsequent offence —, second, the importance of the interests of society that were harmed by the offender and also the nature and/or degree of the harm sustained by the victim of the offence (117) and, last, the scale of penalties generally applicable in the Member State concerned. (118) It is on the basis of that alternative and non-exhaustive body of criteria of assessment that a criminal offence might be classified as 'serious' within the meaning of the relevant case-law of the Court.

106. I would add that the interpretation thus proposed is consistent with the approach which seems to me to have been adopted by the ECtHR in its case-law on the 'prevention of criminal offences', as an objective which can justify an interference with the right to private life enshrined in Article 8 of the ECHR, provided that other conditions are also satisfied. (119) In my view it follows from that case-law that the fight against certain categories of infringements may validly be relied on in that context, by the States Parties to the ECHR, (120) having regard not only to the penalty incurred, but rather to various factors of assessment, among which appear, high on the list, the nature of the offences in question and the public and private interests affected by them. (121)

107. Consequently, I am of the view that if the concept of 'serious crime' within the meaning of the case-law that follows from the judgments in *Digital Rights* and *Tele2* were considered by the Court to constitute an autonomous concept of EU law, it would have to be interpreted as meaning that the seriousness of an infringement, capable of justifying access by the competent national authorities to personal data under Article 15(1) of Directive 2002/58, must be gauged not by taking account solely of the penalty that might be imposed, but by taking account also of a body of other objective criteria of assessment, such as those mentioned above.

### *D. The alternative definition of the minimum level of penalty required in order to characterise the sufficient seriousness of an offence justifying an interference with the fundamental rights in question (second question)*

108. By its second question, the referring court, in essence, asks the Court to identify the minimum level which the penalty incurred should attain in order for a criminal offence to be characterised as 'serious' within the meaning of the case-law resulting from the judgments in *Digital Rights* and *Tele2*, and to state whether a threshold of three years' imprisonment, as provided for in the Spanish Code of Criminal Procedures since the 2015 reform, (122) is consistent with the requirements of EU law.

109. Those questions are submitted solely in the alternative, in the event that the Court should rule, in answer to the first question, that the seriousness of a criminal offence, a factor that may justify an interference with fundamental rights in accordance with that case-law, must be determined by taking account solely of the custodial sentence that might be imposed.

110. Having regard to the answer which I propose should be given to the first question, there will in my view by no need for the Court to give a ruling on the second question. Nonetheless, I propose to make some observations on the subject, in the interest of being exhaustive.

111. As regards the *first part of the second question*, I consider, as do, in particular, the Czech and Estonian Governments, that the *level of the penalty incurred* which in itself allows an offence to be characterised as 'serious' cannot be determined in a uniform manner for the whole of the territory of the European Union, having regard to the considerations set out above in answer to the first question submitted by the referring court. (123)

112. Furthermore, that variation is the definition of what is to be meant by 'serious crime', and more particularly as regards the threshold of the penalty beyond which that characterisation must apply, is also present in the acts of EU law. In fact, it may be stated that the acts of the European Union adopted on the basis of Article 83(1) TFEU lay down penalties of imprisonment established at different levels for offences which nonetheless are considered to be a 'particularly serious crime, (124) as may be seen, by way of illustration, from Article 3 of Directive 2011/92/EU (125) and Article 15 of Directive (EU) 2017/541, (126) measures relating, respectively, to the fight against the sexual abuse of children and the fight against terrorism. Thus, the EU legislature itself did not opt for a uniform definition of the concept of 'serious crime' from the aspect of a specific quantum of penalty incurred.

113. I recall that the freedom left to the Member States to decide on the minimum level of penalty required in order for criminal offences to be termed 'serious' is limited by the standards set out in the relevant provisions of EU law, and also by the principle that an exception cannot confer such a broad degree that it becomes de facto the general rule. (127)

114. In the present case, 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 fix that threshold at such a low level, having regard to the normal level of penalties applicable in that State, (128) 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, as Ireland has correctly observed.

115. In addition, it is common ground that the interferences with the rights guaranteed by Articles 7 and 8 of the Charter that might be authorised by the Member States pursuant to Article 15(1) always continue to be subject to compliance with the general requirements flowing from the principle of proportionality, as set out in Article 52(1) of the Charter. (129)

116. As regards the *last part of the second question*, the Estonian Government and the Commission state that a threshold based exclusively on a penalty of at least *three years' imprisonment* appears, in absolute terms, to be sufficient for an offence to be classified as 'serious', within the meaning of the case-law of the Court relating to access to personal data resulting from the judgment in *Digital Rights*, and, furthermore, that such a threshold is not manifestly incompatible with EU law in general (130) and, more particularly, with Article 15(1) of Directive 2002/58.

117. However, to my mind it would be desirable that the Court should refrain from adopting a position in favour of a precise quantum of penalty incurred, since what is appropriate for certain Member States will not necessarily be appropriate for others, and what applies today for a type of offence will not necessarily apply irrevocably in the future, as I have already mentioned. (131) Since a determination of the threshold in question requires a complex and potentially evolving evaluation, it is appropriate in my view to remain prudent on that point and to reserve that operation for the assessment of the EU legislature, in the field of

the powers conferred on it, or for the assessment of the legislature of each Member State, within the limits of the requirements resulting from EU law.

118. In the latter regard, I observe that, in the present case, the referring court mentions a risk of inversion of the general rule and the derogations provided for in Directive 2002/58, a risk referred to above, (132) where it states that 'the threshold of three years' imprisonment [introduced by the Spanish legislature in 2015 (133)] covers a significant majority of criminal offences'. In other words, according to the referring court, the current list of offences capable of justifying, in Spain, restrictions of the rights protected under Articles 7 and 8 of the Charter, which was established by the reform of the Code of Criminal Procedure, would lead in practice to the majority of offences provided for in the Criminal Code being included in that list.

119. On the assumption that the interference at issue in the main proceedings should be considered to be serious by the Court, and on the assumption that the result thus referred to by the referring court should transpire, that result would in my view not comply with the obligation of proportionality to which such restrictions are subject. (134) That is the case, to my mind, notwithstanding the existence of judicial review, to which the Spanish Government refers, since the exercise of such review makes it possible only to prevent the implementation of measures deemed, on a case-by-case basis, to be arbitrary or too intrusive, and not generally to restrict the use of measures of that type and their development.

120. Last, I would emphasise that the approach proposed throughout this section is in my view consistent with the approach taken by the ECtHR in its case-law on personal data protection. Admittedly, as Ireland and the Commission submit, that court has held that national legislation defining 'serious' offences, capable of justifying an interference with private life, was sufficiently clear, referring to a potential penalty equal to or greater than three years' imprisonment. (135) Nonetheless, I consider that the ECtHR has not established that figure as an absolute and fixed criterion for the purposes of that definition, as its case-law seems to me to be focused on the requirement of sufficient foreseeability and clarity for citizens with regard not so much to the penalty incurred, but rather to the nature of the offences that permit such an interference. (136) Furthermore, although the ECtHR recognises that the States have a certain latitude to assess the existence of and the need for such an interference, it nonetheless makes that margin of appreciation subject to review at European level. (137) In particular, it takes care to prevent the risks of abuse induced by legislation referring to such a wide range of offences that they mean that most offences justify intrusive measures. (138)

121. In conclusion, I consider that, if the Court should hold — contrary to my recommendation — that only the penalty incurred should be taken into account for the purpose of classifying a criminal offence as 'serious' within the meaning of the case-law resulting from the judgment in *Digital Rights*, the answer to the second question should therefore be that the Member States are free to set the minimum level of the penalty relevant for that purpose, provided that they comply with the requirements resulting from EU law, and in particular the requirements that interferences with the fundamental rights guaranteed in Articles 7 and 8 of the Charter must remain exceptional and respect the principle of proportionality.

## V. Conclusion

122. In the light of the foregoing considerations, I propose that the Court answer the questions for a preliminary ruling submitted by the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain) 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, read in the light of Articles 7 and 8 and also of Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a measure allowing the competent national authorities to have access, for purposes associated

with combating criminal offences, to the identification data of users of telephone numbers activated from a specific mobile telephone during a limited period, in circumstances such as those at issue in the main proceedings, entails an interference with the fundamental rights guaranteed by that directive and by the Charter which does not attain a sufficient level of seriousness for such access to be confined to cases in which the offence concerned is of a serious nature.

---

1 Original language: French.

---

2 This footnote is not relevant to the English translation.

---

3 Judgment of 8 April 2014 (C−293/12 and C−594/12, EU:C:2014:238), in which the Court declared 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/EC (OJ 2006 L 105, p. 54) invalid on the ground that 'by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter' (paragraph 69).

---

4 Judgment of 21 December 2016 (C−203/15 and C−698/15, EU:C:2016:970), in which the Court held that EU law, *first*, 'preclud[es] national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication' and, *second*, 'preclud[es] national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union' (operative parts 1 and 2).

---

5 OJ 2002 L 201, p. 37.

---

6 Directive of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).

---

7 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).

---

8 In particular, in compliance with Article 8 of the ECHR, according to which:
'1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

---

9 OJ 2002 L 108, p. 33.

---

10 BOE No 251 of 19 October 2007, p. 42517.

---

11 That follows both from the preamble to that law and from its essential provisions, the wording of which is similar to that of the corresponding provisions of Directive 2006/24.

---

12 BOE No 239 of 6 October 2015, p. 90192.

---

13 IMEI is the abbreviation of the expression ‘International Mobile Equipment Identity’ The IMEI is a unique identification code, consisting of around 15 digits, which is generally found inside the battery compartment of the mobile telephone and also on the box and the invoice issued when the device is purchased.

---

14 The Spanish Government states that that request related to four telephone companies and specified that where the IMEI used the telephone network of one of those companies while the management of that network belonged to a virtual mobile network operator, the abovementioned data received by that operator must also be provided.

---

15 See the provisions reproduced in points 13 and 14 of this Opinion.

---

16 See judgment of the Sala de lo Penal (Criminal Chamber) of 26 July 2010 (No 745/2010, ES:TS:2010:4200), available at the following internet address: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference= 5697924&links=&optimize= 20100812&publicinterface=true.

---

17 See point 15 et seq. of this Opinion. According to the referring court, that reform is clearly relevant for the request for a preliminary ruling. At the hearing, the Spanish Government stated that the new legislation was applicable in the present case.

---

18 Namely, terrorism offences and offences committed in the context of a criminal organisation.

---

19 See footnote 4 of this Opinion.

---

20 See paragraph 103 of the judgment in *Tele2*, which refers to ‘organised crime and terrorism’. I note that the same twofold illustration may also be found in paragraphs 24 and 51 of the judgment in *Digital Rights*, with apparent reference to recitals 7 to 10 of Directive 2006/24, which was declared invalid by that judgment.

---

21 The referring court mentions, in particular, paragraph 60 of the judgment in *Digital Rights*, where the Court observed that ‘Directive 2006/24 … fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law’.

---

22 On that topic, see, in particular, footnotes 3 and 4 of this Opinion.

---

23 To my mind, the ‘owners or users’ referred to in that request are necessarily persons who are subscribers, are registered or at least are identifiable (see also footnote 25 of this Opinion), and not persons who have bought a SIM card without leaving any traces.

---

24 See point 20 of this Opinion.

---

25 In accordance with the definition provided in Article 2(a) of Directive 95/46, to which Article 2 of Directive 2002/58 refers, the concept of ‘personal data’ covers ‘any information relating to an identified or identifiable natural person’, it being specified that ‘an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’. The Court has already observed that ‘the right to respect for private life with regard to the processing of personal data concerns any information corresponding to that definition’ (see, in particular, judgment of 17 October 2013, *Schwarz*, C−291/12, EU:C:2013:670, paragraph 26) and that the scope of that definition is very wide (see, in particular, judgment of 20 December 2017, *Nowak*, C−434/16, EU:C:2017:994, paragraph 33).

---

26 According to the Spanish Government, the addresses of the persons concerned were not explicitly requested.

---

27 Information such as, for example, an individual’s marital status, the number of his national identity card, his bank details or any telephone subscription.

---

28 Information that might relate to the numbers associated with incoming or outgoing calls, or again the date, duration or frequency, or indeed the content, of communications. The Spanish Government states that, in this case, the police expressly indicated that their request was not intended to obtain data protected by the secrecy of communications.

---

29 In other words, those data might be obtained by the mere activation of the mobile device in question, whether or not it is subsequently used by its owner or keeper in a specific interpersonal communication process.

---

30 See point 74 et seq. of this Opinion.

---

31 I would observe that access to personal data, in absolute terms, does not in my view present fewer risks for the fundamental rights enshrined in Articles 7 and 8 of the Charter than the retention of such data. The danger might even be considered to be greater, in that access to retained data gives concrete form to the potentially harmful use that might be made of the data.

---

32 The Spanish Government states that the forename, name and possibly the address of the owner of a SIM card may be lawfully retained in Spain. In my view, it follows from Article 1 and Article 3(1)(a) of Law 25/2007 (see point 10 et seq. of this Opinion) that mobile telephone operators are required to deep the data generated or processed in the context of their supply of services, in particular the name and address or the subscriber or registered user, in so far as those data may be necessary in order to retrieve and identify the source of a communication. I would recall that equivalent requirements are to be found in Article 3 and Article 5(1)(a)(1)(ii) of Directive 2006/24, which was transposed by that law.

---

33 A circumstance that had already been noted by the Court in the judgment of 29 January 2008, *Promusicae* (C−275/06, EU:C:2008:54, paragraph 45 *in fine*).

---

34 To that effect, judgment of 19 April 2012, *Bonnier Audio and Others* (C−461/10, EU:C:2012:219, paragraph 37).

---

35 In particular, as regards the jurisdiction of the Court and the answer to the first question, see point 43 et seq. and point 70 et seq., respectively, of this Opinion.

---

36 See, in particular, judgment of 16 May 2017, *Berlioz Investment Fund* (C−682/15, EU:C:2017:373, paragraph 49 and the case-law cited).

---

37 See, in particular, judgment of 6 October 2016, *Paoletti and Others* (C−218/15, EU:C:2016:748, paragraph 14 et seq.).

---

38 See, in particular, judgment of 1 December 2016, *Daouidi* (C−395/15, EU:C:2016:917, paragraph 63).

---

39 According to the Spanish Government, this constitutes the exercise of the right to punish (*ius puniendi*) by the State authorities. On that point, see the Opinion of Advocate General Sánchez-Bordona in *Breyer* (C−582/14, EU:C:2016:339, points 86 to 92).

---

40 The principles set out in those provisions are also mentioned in recital 11 of Directive 2002/58, which refers to Article 15(1) of that directive (see points 6 and 7 of this Opinion).

---

41 See paragraphs 72 to 81 of the judgment in *Tele2*. In that regard, see also my Opinion in Joined Cases *Tele2 Sverige and Others* (C−203/15 and C−698/15, EU:C:2016:572, paragraphs 88 to 97 and 124).

---

42 See, in particular, Article 1(1) of Law 25/2007 and Article 579(1) of the Code of Criminal Procedure, reproduced in points 11 and 17 of this Opinion, and also, on the legal obligation borne by those suppliers, point 40 of this Opinion.

---

43 It being understood that what are known as the 'sovereign' activities of the State relate to the functions reserved for the State or its divisions, which it cannot delegate to private entities, and, in particular, the activities connected with justice, the police and the army.

---

44 Such as those processed by the police or judicial authorities in order to seek the perpetrators of offences (for example, the data collected and analysed in the course of the interception of telephone conversations by police officers at the request of an investigating judge).

---

45 Such as the data relating to the particulars of the users of a telephone service which are used on the occasion of a criminal investigation, as in the main proceedings.

---

46 See the order for reference relating to pending case *Privacy International* (C−623/17), which refers, in particular, to the judgments of 30 May 2006, *Parliament* v *Council and Commission* (C−317/04 and C−318/04), EU:C:2006:346, paragraphs 56 to 59), and of 10 February 2009, *Ireland* v *Parliament and Council* (C−301/06, EU:C:2009:68, paragraphs 88 and 91), from which it is apparent that the processing of data relating to air passengers forming the subject matter of the first judgment was necessary not for a supply of services, but for safeguarding public security, and therefore fell outside the scope of Directive 95/46.

47 Given that, first, the dispute in the main proceedings here relates to the transfer not of bulk data but of targeted data and, second, the views adopted by the Court in the judgment in *Tele2* may, to my mind, be transposed to the present case, as I have indicated in point 46 of this Opinion.

48 See point 33 et seq. of this Opinion.

49 See, in particular, Article 1(2) of Law 25/2007 and Article 579(1) of the Code of Criminal Procedure.

50 In fact, the police authorities' request seeks to ascertain not the geographic position of the stolen device or of the persons who held them, but only the identity of those persons.

51 Provisions of Article 2 reproduced in point 8 of this Opinion.

52 Traffic data, which are governed by Article 6 of Directive 2002/58.

53 See point 36 of this Opinion.

54 Electronic communications service, defined in Article 2(c) of Directive 2002/21 (which establishes the applicable regulatory framework) as 'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks …'.

55 The fact that the processing of data may be necessary for the purpose of the billing of the service, especially in the case of subscribers, is referred to in several provisions of Directive 2002/58 (in particular, recitals 26, 27 and 29; subparagraph g of the second paragraph of Article 2 and Article 6(2) and (5)). On that subject, see also paragraph 86 of the judgment in *Tele2* and the case-law cited in that paragraph.

56 Provisions referring, respectively, generally, to 'the processing of personal data in the electronic communication sector' and the 'processing of personal data in connection with the provision of … electronic communications services'.

57 See recitals 2, 7 and 11 and also Article 1(1) and Article 15(3) of Directive 2002/58.

58 See recital 21 and also Article 1(1) and Article 5, which specifically governs the confidentiality of the communications, of Directive 2002/58.

59 See judgment of 29 January 2008, *Promusicae* (C−275/06, EU:C:2008:54, paragraphs 29 to 31 and 45).

60 On the interpretation of Article 12, see, in particular, judgment of 15 March 2017, *Tele2 (Netherlands) and Others* (C−536/15, EU:C:2017:214, paragraph 33 et seq. and also the case-law cited).

61 According to recital 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 …'.

62 The concept of data relating to the private life of a person within the meaning of Article 8 of the ECHR (reproduced in footnote 8 of this Opinion) is given a broad interpretation by the ECtHR (see, in particular, ECtHR, 13 February 2018, *Ivashchenko v. Russia*, CE:ECHR:2018:0213JUD006106410, § 63 et seq.), as has already been observed (see judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C−92/09 and C−93/09, EU:C:2010:662, paragraph 59 and the case-law of the ECtHR cited).

63 See recitals 3, 11 and 24 of Directive 2002/58.

64 See, in particular, the judgment in *Tele2* (paragraph 120, where an analogy is drawn with the case-law of the ECtHR, and also paragraph 126 et seq., referring to the situation of the European Union vis-à-vis that of the ECHR).

65 While Directive 2002/58 governs the particular sector of electronic communications (see, in particular, recitals 4 and 10 and Article 1(1) and (2) of that directive).

66 I recall that the concept of 'serious crime' was introduced, as a criterion restricting the action of Member States, by Directive 2006/24 on the retention of data, which was declared invalid by the judgment in *Digital Rights*, and then used by the Court in the judgment in *Tele2*, in order to interpret the provisions of Directive 2002/58, in the context of national legislation on the retention of an access to data (see also footnotes 3 and 4of this Opinion). It follows, in my view, that if Directive 2002/58 were declared inapplicable in this case, there would be no need to provide an interpretation of that concept, which is requested by the referring court.

67 See, in particular, judgments of 16 June 2015, *Gauweiler and Others* (C−62/14, EU:C:2015:400, paragraphs 24 and 25), and of 22 February 2018, *Porras Guisado* (C−103/16, EU:C:2018:99, paragraph 34).

68 See also point 44 of this Opinion.

69 See also judgment in *Tele2* (paragraph 82).

70 See also point 10 of this Opinion. I note that the situation was similar in one of the cases that gave rise to the judgment in *Tele2* (see paragraphs 15 and 63).

71 In the latter regard, see point 45 et seq. of this Opinion.

72 See also point 71 of this Opinion.

---

73 See points 36 and 52 of this Opinion

---

74 On the absence of seriousness of the interference caused in the present case, see point 74 et seq. of this Opinion.

---

75 See, in particular, judgment in *Digital Rights* (paragraph 26 et seq.) and also Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, paragraph 124 and the case-law cited).

---

76 See paragraphs 24, 41, 49 and 57 to 61 of the judgment in *Digital Rights*.

---

77 See paragraphs 41, 42, 51 and 59 of the judgment in *Digital Rights*.

---

78 It being borne in mind that only the expression 'criminal offences' appears in Directive 2002/58, in the first sentence of Article 15(1).

---

79 The expression is used, in essence, in recital 9 of Directive 2006/24 and also, literally, in recital 21 and Article 1(1) of that directive.

---

80 See, as regards the concept of 'infractions graves', paragraphs 105, 106 and 119 and, as regards the concept of 'criminalité grave', paragraphs 102, 103, 108, 110, 111, 114, 115, 118, 125 and 134 of the judgment in *Tele2*.

---

81 Namely, Article 15(1) of Directive 2002/58, under which Member States may adopt a measure derogating from the principle of confidentiality of traffic data and related data where it is necessary, appropriate and proportionate within a democratic society, having regard to the objectives stated in that provision.

---

82 It being observed that the second question is submitted only in the alternative.

---

83 It has consistently been held that it is settled case-law that in order to provide the referring court with an answer which will be of use to it and enable it to determine the case before it, the Court may have to reformulate the questions referred to it (see, in particular, judgment of 22 February 2018, *SAKSA*, C−185/17, EU:C:2018:108, paragraph 28).

---

84 The Spanish Government emphasised that the data forming the subject matter of the main proceedings do not make it possible to establish, for example, the profile of the person concerned.

---

85 See points 35 to 37 of this Opinion.

---

86 I recall that Directive 95/46 lays down, in Article 8, specific rules for the processing of 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership,

and the processing of data concerning health or sex life'. On the concept of sensitive data and the processing of such data, see *Handbook on European data protection law*, prepared under the aegis of the European Union Agency for Fundamental Rights and the Council of Europe; the updated version is available at the following internet address: https://www.coe.int/en/web/data-protection/home, p. 46 et seq. and p. 93 et seq.

---

87 The sensitive nature of certain data is mentioned only in recital 25 of Directive 2002/58, and it cannot be inferred that this a general requirement.

---

88 See Commission Communication of 13 September 1990 on the protection of individuals in relation to the processing of personal data in the Community and information security (COM(90) 314 final, p. 20).

---

89 See Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, paragraph 124 and the case-law cited). The ECtHR has also made a determination to that effect (see ECtHR, 16 February 2000, *Amann v. Switzerland*, CE:ECHR:2000:0216JUD002779895, §§ 68 to 70).

---

90 See point 8 of this Opinion. See also ECtHR, 8 February 2018, *Ben Faiza v. France* (CE:ECHR:2018:0208JUD003144612, §§ 66 to 68), concerning a judicial request for the communication of information relating to the use of a telephone.

---

91 In the following terms: for 'the prevention, investigation, detection and prosecution of criminal offences'.

---

92 See, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, paragraph 126 and the case-law cited).

---

93 Paragraph 57 of the judgment in *Digital Rights*. On the particular seriousness of the interference in question, see also paragraphs 37, 39, 47, 48, 60 and 65 of that judgment.

---

94 Operative part 1 of the judgment in *Tele2*.

---

95 In the words of paragraph 102 of the judgment in *Tele2*, 'in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the *retention* of traffic and location data, *only the objective of fighting serious crime is capable of justifying such a measure* (see, by analogy, in relation to Directive 2006/24, [the judgment in *Digital Rights*], paragraph 60 [in which the expression "*in view of the extent and seriousness of the interference*" appeared])' (emphasis added). Paragraph 115 of the judgment in *Tele2* applies that reasoning to *access* to such data. On the particular seriousness of the interference in question, see also paragraphs 97 and 100 of that judgment.

---

96 Thus, paragraph 115 of the judgment in *Tele2* emphasises that '*since the objective pursued by [national legislation derogating from the principle of confidentiality of electronic communications] must be proportionate to the seriousness of the interference* in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, *only the objective of fighting serious crime is capable of justifying such access* to the retained data' (emphasis added).

---

97 In fact, the ECtHR has repeatedly emphasised the need to *weigh up*, on the one hand, the interest of a State in protecting *national security* by means of measures affecting personal data and, on the other, the *seriousness of the interference* with the right of an individual to respect for his private life, two factors on which the State's margin of appreciation depend, in particular where it means to prevent or prosecute *serious criminal offences* (see ECtHR, 26 March 1987, *Leander v. Sweden*, CE:ECHR:1987:0326JUD000924881, § 59;ECtHR, 26 June 2006, *Weber and Saravia v. Germany*, CE:ECHR:2006:0629DEC005493400, §§ 106, 125 and 126; and ECtHR, 4 December 2015, *RomanZakharov v. Russia*, CE:ECHR:2015:1204JUD004714306, §§ 232 and 244).

---

98 See point 32 et seq. of this Opinion.

---

99 In note that, in Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, in particular paragraphs 194 and 207 to 209), the Court also evaluated the necessity of the interferences entailed by the proposed agreement by examining the procedures for the use and retention of data envisaged in that agreement, especially, from the aspect of the particular context of those measures, their specification and their duration.

---

100 As might be the case, for example, of the identity of individuals that would be published in a press article or on an internet site.

---

101 To that effect, see the Convention on Cybercrime held under the aegis of the Council of Europe in Budapest on 23 November 2001, and signed by all the Member States of the European Union (available at the following internet address: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?_coeconventions_WAR_coeconventionsportlet_languageId=en_EN), Article 18 of which requires the adoption of legislative measures allowing the competent authorities to order a service provider to submit subscriber information such as the subscriber's 'identity, … address [and] telephone number' in the service provider's possession.

---

102 Thus, the Danish Government rightly observed that when the police obtain, as in the present case, information concerning the name and address of the owner of a SIM card used in the context of an offence, that is not fundamentally different, for example, from obtaining information about the owner of a motor vehicle used in the commission of an offence.

---

103 Unlike particularly intrusive information, in particular as regards the tracing of communications and the profile of the persons concerned, which were at issue in the cases that gave rise to the judgment in *Digital Rights* (see paragraphs 26 to 29 and 37) and to the judgment in *Tele2* (see paragraphs 97 to 100).

---

104 See, in particular, Paragraphs 90 and 115 of the judgment in *Tele2*.

---

105 Emphasis added.

---

106 Namely if the Court were to consider that the interference at issue in the main proceedings is sufficiently serious for the first question as submitted by the referring court to be answered, or that it is immaterial in that respect that the interference is not serious.

---

107 See point 71 of this Opinion.

---

108 Article 1(1) of Directive 2006/24 stated that that directive aimed ‘to harmonise Member States’ provisions concerning the obligations of the providers of … communications services …, 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). See also recital 21 of that directive.

---

109 See, in particular, judgments of 15 September 2011, *Dickinger and Ömer* (C−347/09, EU:C:2011:582, paragraph 31), and of 6 December 2011, *Achughbabian* (C−329/11, EU:C:2011:807, paragraph 33).

---

110 On that subject, see also point 112 of this Opinion.

---

111 On the evolving nature of serious crime, see also my Opinion in Joined Cases *Tele2 Sverige and Others* (C−203/15 and C−698/15, EU:C:2016:572, point 214).

---

112 By way of illustration, as regards the fight against organised crime, a Report from the Commission to the European Parliament and the Council dated 7 July 2016 indicates that the penalties laid down by Member States vary considerably between Member States (between three months and 17 years’ imprisonment) for the serious offence of participation in a criminal organisation (see Report to the European Parliament and the Council based on Article 10 of Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, COM(2016) 448 final, p. 7, point 2.1.4.1).

---

113 As the Danish Government has pointed out, less onerous penalties, by comparison with other Member States, are applied in Denmark, although that does not mean that the offence is regarded as not particularly serious. For example, the penalty for possession of child pornography is one year’s imprisonment, while it may be as much as 10 years’ imprisonment, for the same offences, in other Member States, but that does not alter the fact that the offence is particularly serious in nature.

---

114 See, in particular, judgment of 22 May 2012, *I* (C−348/09, EU:C:2012:300, paragraphs 21 to 23), according to which ‘European Union law does not impose on Member States a uniform scale of values as regards the assessment of conduct which may be considered to be contrary to public security’ and ‘Member States essentially retain the freedom to determine the requirements of public policy and public security in accordance with their national needs, which can vary from one Member State to another and from one era to another, particular as justification for a derogation from the fundamental principle of free movement of persons’, but ‘those requirements must nevertheless be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the institutions of the European Union’.

---

115 See, to that effect, paragraph 89 et seq. of the judgment in *Tele2*, concerning the general obligation to ensure the confidentiality of communications and of the related traffic data.

---

116 I would point out that the Czech and Estonian Governments propose that the answer should be, in essence, that it is possible to determine the sufficient seriousness of offences, as a criterion justifying a breach of the fundamental rights recognised in Articles 7 and 8 of the Charter, on the sole basis of the penalty incurred, but that those Governments nonetheless consider that each Member State should be free also to take into consideration other objective criteria reflecting the specific nature of its legal order, if it considers it necessary to do so.

---

117 I share the French Government's view that it is self-evident that breaches of the fundamental interests of the nation, the institutions or the integrity of the national territory come by their nature within the sphere of 'serious crime', but that other types of offences should also come within that sphere, such as offences against the life, physical or mental integrity of persons, and also offences against assets entailing significant financial harm for the victim, or again offences forming part of a serial phenomenon which constitute a repeated breach of public order. On the latter point, the Hungarian Government also refers to the possibility that an exceptionally high incidence of certain offences in crime at national level may be taken into account.

---

118 In that latter regard, see also point 98 of this Opinion.

---

119 In accordance with paragraph 2 of Article 8 of the ECHR, such an interference can be justified only if it is in accordance with the law, pursues one or more of the legitimate aims set out in that paragraph and is necessary in a democratic society in order to attain that aim or those aims.

---

120 The ECtHR has held that the relevant offences must be readily identifiable by citizens, although that condition of foreseeability does not require States to set out exhaustively the offences that may give rise to such a measure (see, in particular, ECtHR, 4 December 2015, *Roman Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306, § 244).

---

121 See, in particular, ECtHR, 26 June 2006, *Weber and Saravia v. Germany* (CE:ECHR:2006:0629DEC005493400, §§ 106 and 115); ECtHR, 4 December 2008, *Marper v. United Kingdom* (CE:ECHR:2008:1204JUD003056204, §§ 104 and 119); and ECtHR, 30 May 2017, *Trabajo Rueda v. Spain* (CE:ECHR:2017:0530JUD003260012, §§ 39 and 40).

---

122 See point 15 et seq. of this Opinion.

---

123 See point 93 et seq. of this Opinion.

---

124 It will be recalled that Article 83(1) TFEU permits the adoption of 'minimum rules concerning the definition of criminal offences in the areas of particularly serious crime with a cross-border dimension' listed in that provision.

---

125 Directive of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1), Article 3 of which lays down penalties of between at least one year's and at least 10 years' imprisonment for the various types of 'offences concerning sexual abuse' referred to in that article.

---

126 Directive of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ 2017 L 88, p. 6), Article 15(3) of which lays down custodial penalties that are not to be less than eight or 15 years depending on the various types of 'offences linked to a terrorist group' referred to in Article 4 of that directive.

---

127 See also point 101 of this Opinion.

---

128 On that subject, see point 98 of this Opinion.

---

129 See, in particular, recital 11 and Article 15(1) of Directive 2002/58, and paragraphs 94 to 96 of the judgment in *Tele2*.

---

130 See, in particular, in addition to the provisions referred to in footnotes 125 and 126 of this Opinion, 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), Article 3(9) of which defines ‘serious crime’ as referring to ‘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 laws of a Member State’.

---

131 See point 97 of this Opinion.

---

132 See point 101 of this Opinion.

---

133 The reform mentioned in point 15 et seq. of this Opinion.

---

134 See also point 115 of this Opinion.

---

135 See, to that effect, ECtHR, 18 May 2010, *Kennedy v. United Kingdom* (CE:ECHR:2010:0518JUD002683905, §§ 34 and 159), and ECtHR, 4 December 2015, *Roman Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306, § 244).

---

136 See point 106 of this Opinion.

---

137 See, in particular, ECtHR, 6 September 1978, *Klass and others v. Germany* (CE:ECHR:1978:0906JUD000502971, § 49), and ECtHR, 18 May 2010, *Kennedy v. United Kingdom* (CE:ECHR:2010:0518JUD002683905, §§ 153 and 154).

---

138 See ECtHR, 10 February 2009, *Iordachi and others v. Moldova* (CE:ECHR:2009:0210JUD002519802, § 44), where the Moldovan legislation was considered to be lacking in clarity, in particular, on the ground that more than one half of the offences provided for in the Criminal Code fell within the category of offences eligible for telephone interception warrants. See also ECtHR, 4 December 2015, *Roman Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306, § 248).