



Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 20 April 2023¹

Case C-548/21

CG

v

Bezirkshauptmannschaft Landeck

(Request for a preliminary ruling from the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria))

(Reference for a preliminary ruling – Telecommunications – Protection of personal data – Directive (EU) 2016/680 – Criminal proceedings – Attempt by public authorities to gain access to the data recorded on a mobile telephone without authorisation by a court or independent administrative authority)

1. This request for a preliminary ruling concerns, in essence, the requirements to be complied with by law-enforcement authorities in order to gain access to the data stored on the mobile telephone of a person subject to a criminal investigation.

2. As I shall try to explain, the reference for a preliminary ruling suffers from considerable defects in terms of admissibility. If the Court decides, nevertheless, to examine the substance, it will have to rule on the scope of Directive 2002/58/EC² and of Directive (EU) 2016/680 respectively.³

¹ Original language: Spanish.

² Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).

³ Directive of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

I. Legislative framework

A. *European Union law*

1. *Regulation (EU) 2016/679*⁴

3. Paragraph 2 of Article 2 ('Material scope') provides:

'This Regulation does not apply to the processing of personal data:

...

- (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

2. *Directive 2016/680*

4. Recital 2 states:

'The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should ... respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.'

5. Recital 46 reads:

'Any restriction of the rights of the data subject must comply with the Charter [of Fundamental Rights of the European Union ("the Charter")] and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights [⁵] respectively, and in particular respect the essence of those rights and freedoms.'

6. According to recital 49:

'Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise [of] the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.'

7. Article 1 ('Subject matter and objectives') provides:

'1. This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

⁴ Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR').

⁵ 'the ECtHR'.

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2. In accordance with this Directive, Member States shall:

- (a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

...

3. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.'

8. Paragraph 1 of Article 2 ('Scope') provides:

'This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).'

9. Article 3 ('Definitions') states:

'For the purposes of this Directive:

...

- (2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

...

(7) "competent authority" means:

- (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

....'

10. Paragraph 1 of Article 4 ('Principles relating to processing of personal data') requires that:

'Member States shall provide for personal data to be:

- (a) processed lawfully and fairly;
- (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

...

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'

11. Article 8 ('Lawfulness of processing') states:

'1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.

2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.'

12. Article 13 ('Information to be made available or given to the data subject') provides:

'1. Member States shall provide for the controller to make available to the data subject at least the following information:

...

(d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

...

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

....'

13. According to paragraph 1 of Article 15 ('Limitations to the right of access'):

'Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.'

14. Under Article 27 ('Data protection impact assessment'):

'1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.'

15. Article 28 ('Prior consultation of the supervisory authority') states:

'1. Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:

- (a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or
- (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

....'

16. Article 54 ('Right to an effective judicial remedy against a controller or processor') establishes that:

'Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.'

B. National law

17. Under Paragraph 18 of the Strafprozessordnung⁶ the police is assigned tasks in the service of the administration of criminal justice (subparagraph 1). Police investigations are to be the responsibility of the security authorities (subparagraph 2). The organs of the public security service shall provide the executive service of the police, consisting of investigating and prosecuting criminal offences (subparagraph 3).

18. Under Paragraph 99 of the StPO, the police conducts investigations on its own initiative or pursuant to a complaint and must comply with the orders of the Public Prosecutor's Office and of the courts (subparagraph 1). Where an investigation requires an order of the Public Prosecutor's Office, the police may exercise the corresponding power notwithstanding the absence of such an order in the event of imminent danger. In that situation, it must immediately seek that authorisation (subparagraph 2).

19. Under Paragraph 111(2) of the StPO, where data are to be gathered from information stored on data carriers, any person must allow access to that information and, on request, provide or allow the creation of an electronic data carrier in a commonly used file format. Any person must also allow a back-up copy to be made of the information stored on the data carriers.

II. Facts, dispute and questions referred for a preliminary ruling

20. CG is a German citizen who lives and works in Austria.

21. On 23 February 2021, while carrying out a narcotics check, officers of the customs office in Innsbruck (Austria) seized a package addressed to CG which contained 85 g of cannabis.

22. On 6 March 2021, two police officers questioned CG about the consignor of the package and searched his home. During that search, his mobile telephone (which included a SIM card and an SD card) was seized and he was given the report of seizure.

23. Asked to provide access to the connection data on his mobile telephone, CG refused, and also refused to disclose the telephone's PIN code.

24. Officers at district police headquarters in Landeck (Austria) were unable to unlock the mobile telephone. It was sent to the Bundeskriminalamt (Criminal Police Office) in Vienna (Austria), where another, unsuccessful, attempt was made to unlock it and extract the stored data.

⁶ Austrian Code of Criminal Procedure ('StPO') (BGBl No 631/1975, in the version applicable at the material time (BGBl I No 24/2020)).

25. At the time those measures were taken by the police, they were not covered by an order of the Public Prosecutor's Office or a court order.

26. On 31 March 2021, CG lodged an appeal before the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria) against the coercive measure imposed on him, challenging the seizure of his mobile telephone. The telephone was returned to him on 20 April 2021.

27. CG was not advised that attempts had been made to process data stored on the mobile telephone; he became aware of them because the police officer who had seized and subsequently initiated the data processing was questioned under oath. Nor were those attempts documented in the file compiled by the police.

28. Against that background, the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol) referred the following questions to the Court of Justice for a preliminary ruling:

- '(1) Is Article 15(1) (possibly read in combination with Article 5) of Directive [2002/58], as amended by Directive 2009/136/EC [of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ 2009 L 337, p. 11)], read in the light of Articles 7 and 8 of the [Charter], to be interpreted as meaning that public authorities' access to data stored on mobile telephones entails interference with fundamental rights enshrined in those articles of the Charter which is sufficiently serious to entail that access being limited, in areas of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime?
- (2) Is Article 15(1) of Directive [2002/58], as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the [Charter], to be interpreted as meaning that it precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation without the authorisation of a court or independent administrative body?
- (3) Is Article 47 of the [Charter], possibly read in combination with Articles 41 and 52 thereof, to be interpreted, from the point of view of equality of arms and from the point of view of an effective remedy, as meaning that it precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows data processing of a mobile telephone without advising the data subject before or, at the very least, after the measure is taken?'

III. Procedure before the Court

29. The request for a preliminary ruling was registered at the Court on 6 September 2021.

30. On 20 October 2021, the Court asked the referring court to express an opinion on whether Directive 2016/680 could be relevant to the case.

31. On 11 November 2021, the referring court responded that Directive 2016/680 must be applied in the main proceedings.

32. Written observations were submitted by the German, Austrian, Cypriot, Danish, Estonian, French, Hungarian, Irish, Netherlands, Norwegian, Polish and Swedish Governments and by the European Commission.

33. The parties that had submitted written observations, with the exception of the German, Hungarian and Polish Governments, appeared at the hearing held on 16 January 2023, as did the Finnish Government. The Court invited them all to focus their arguments on Directive 2016/680 and to reply orally to certain questions about it.

IV. Analysis

A. *Inadmissibility*

34. The referring court initially worded its questions as seeking interpretation only of Directive 2002/58. However, practically all those that have participated in the proceedings agree that Directive 2002/58 does not apply to this case and that, in consequence, its interpretation is not necessary in order to resolve the dispute.

35. Article 3 of Directive 2002/58 states that it governs ‘the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the [European Union], including public communications networks supporting data collection and identification devices’.

36. The Court has held that ‘where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, subject to the application of [Directive 2016/680]’.⁷

37. In the present case, the attempt to gain access to the data was made directly by law-enforcement authorities in the course of a criminal investigation. The electronic communications service providers were not involved and were not asked to communicate personal data. Directive 2002/58 therefore does not enter the equation.

38. The EU law measure governing the situation at issue is Directive 2016/680, which applies, by virtue of Article 2(1) thereof, to the processing of personal data by competent authorities for the ‘purposes of the ... investigation ... of criminal offences’.

39. The foregoing is sufficient to suggest that the reference for a preliminary ruling, as worded by the national court, is inadmissible, since the EU law measure whose interpretation it was seeking did not apply to the case.

⁷ Judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, ‘the judgment in *La Quadrature du Net*’, paragraph 103).

40. However, Article 267 TFEU allows the Court of Justice to reformulate the questions referred to it for a preliminary ruling or identify other provisions of EU law that may be relevant, in order to provide the referring court with an answer which will be of use to it.⁸

41. The Court approached the referring court for its opinion on whether Directive 2016/680 could be applicable. It therefore gave that court an opportunity itself to supplement or reformulate its questions. Instead of doing so, the referring court merely stated that ‘the requirements of [Directive 2016/680] are in any case to be complied with in the present case’, but did not identify the provisions of that directive about which it is uncertain or expand upon other substantive considerations.⁹

42. The Court has repeatedly held that ‘it is essential, as is stated in Article 94(c) of the Rules of Procedure that the request for a preliminary ruling itself contain a statement of the reasons which prompted the referring court or tribunal to inquire about the interpretation or validity of certain provisions of EU law, and the relationship between those provisions and the national legislation applicable to the main proceedings’.¹⁰

43. It is therefore clear that, as a result of the factors set out above, the requirements of Article 94 of the Rules of Procedure have not been complied with in this reference. Even though the Court of Justice enjoys a degree of flexibility in that respect, the cooperation with the referring court must be reciprocal: where, without good cause, the referring court fails to collaborate in order to set out its uncertainties on the interpretation of the EU law it considers applicable (in this case, Directive 2016/680) it stands to reason, to my mind, that the request for a preliminary ruling should be dismissed as inadmissible.¹¹

44. In addition, the following should be noted.

- The referring court has not specified the nature of either the processing attempted by the law-enforcement authorities or the specific personal data being sought. Initially, it seemed to be indicating that it was confined to connection data (that is to say, traffic and location data), but later did not rule out that unlocking the telephone might afford access to ‘all digital data stored [on it]’¹² and even to the content of the communications and the electronic mail exchanged using the telephone.¹³
- It also refers to both the seizure of the telephone and access, or attempted access, to the data contained in it and to their subsequent ‘exploitation’ (*Auswertung*), that is to say, to the processing and interpretation of those data. That exploitation, it adds, ‘entails full and uncontrolled access to all the data subject’s digital communications’, which makes it possible to ‘reconstruct a detailed and in-depth picture of almost all areas of his private life’.

⁸ For example, judgment of 28 April 2016, *Oniors Bio* (C-233/15, EU:C:2016:305, paragraph 30).

⁹ The Court found it necessary to invite the parties to indicate ‘what, in your opinion, are the relevant provisions of Directive 2016/680 in the light of which the Court should, if applicable, reformulate the three questions raised by the referring court for a preliminary ruling’ (fourth of the questions sent to be answered orally at the hearing).

¹⁰ Judgment of 6 October 2021, *Consorzio Italian Management and Catania Multiservizi* (C-561/19, EU:C:2021:799, paragraph 69).

¹¹ I share that view with the French Government (paragraphs 36 to 41 of its written observations).

¹² In the words of the second question referred.

¹³ The referring court stated that ‘communications data allow almost all contacts to be reconstructed in terms of the frequency, time and duration of communications, as well as of the content of communications via text messages and other messenger services, and processing of photographs and browser history gives a very close insight into the data subject’s private life’.

45. In those circumstances, more than *reformulating* the referring court's questions, the Court of Justice would be veritably *reconstructing* the reference for a preliminary ruling, partly on the basis, moreover, of hypothetical considerations instead of established facts. It would also be doing so, I repeat, after giving the court an opportunity itself to supplement or reformulate its questions.

46. I therefore propose that the reference for a preliminary ruling should be dismissed as inadmissible, as a number of the participating States have suggested.

47. A dismissal on grounds of inadmissibility should likewise flow from the fact, to which attention was drawn at the hearing, that there is now no genuine dispute before the referring court that requires the interpretation of provisions of EU law.

48. Indeed, the Austrian Government (under whose jurisdiction the law-enforcement authorities involved in the investigation fall) acknowledges that those authorities acted unlawfully and infringed the rights of the data subject. Since, according to the order for reference, the complainant's claim before the administrative court challenged precisely the law-enforcement measures that the defendant administration considers to be unlawful, the dispute brought before the referring court has ceased to exist.

49. In any event, in case the Court does not share my view, I shall address below, in the alternative, the substantive issues underlying the questions referred.

50. Before I do so, however, I believe it is necessary to rule out another ground of inadmissibility outlined by a number of the participants in the proceedings.¹⁴ In their view, since Directive 2016/680 seeks to protect natural persons in so far as concerns the *processing* of their data, it does not govern situations such as the present one, in which there has not been any processing but merely an *attempt to gain access* to data that ultimately could not be obtained.

51. According to the Commission, in contrast, the need to ensure the effectiveness of Directive 2016/680 means that its subject matter should be interpreted so that it is not limited to data processing in the strict sense, but also encompasses matters directly linked to that processing. An attempt to gain access to data in order to process them is, in the Commission's view, one of those matters.¹⁵

52. To my mind, the application of Directive 2016/680 to this situation is justified, with no need to strain the bounds of its scope,¹⁶ not because the mobile telephone was seized¹⁷ but as a result of the subsequent actions by the law-enforcement authorities aimed at obtaining certain personal data of the data subject from it, which is why they tried to unlock it and make its content available.

¹⁴ I am referring specifically to the Austrian, French, Netherlands and Norwegian Governments.

¹⁵ According to the Commission, 'it is irrelevant whether or not the attempts were successful. The emergence of technical difficulties that thwart the attempts to gain access is a circumstance that cannot be known in advance and does not influence the data protection risks'.

¹⁶ In particular, I believe it is unnecessary to resort to Articles 27 and 28 of Directive 2016/680, as the Commission suggested in its written observations. The 'data protection impact assessment' provided for in Article 27 refers generically to 'a type of processing' rather than to individual or specific processing operations. This can be seen from recital 58 of Directive 2016/680: 'impact assessments should cover relevant systems and processes of processing operations, *but not individual cases*' (emphasis added). At the hearing, the Commission qualified its reference to both those articles, stating that it had cited them only in order to highlight the fact that Directive 2016/680 also envisages situations prior to the data processing in the true sense.

¹⁷ Directive 2016/680 does not govern the seizure of a telephone as evidence in the context of a criminal investigation.

53. The operations that Article 3(2) of Directive 2016/680 defines as ‘processing’ include ‘otherwise making [personal data] available’ in the course of a criminal investigation. In my understanding, when a law-enforcement authority seizes a telephone on which personal data are stored and manipulates it to extract those data, it is beginning a processing ‘operation’, even if it is frustrated by technical factors relating to security encryption.

54. An unsuccessful attempt to gain access to the personal data stored on a mobile telephone, in a criminal investigation, is governed by Directive 2016/680 for reasons similar to those that led the Court to find that Directive 2002/58 applied to a – likewise unsuccessful – *attempt* to obtain court authorisation for access to certain data belonging to the person under investigation where those data were in the possession of an electronic communications operator.¹⁸

55. In that context, if the referring court was required to rule on whether the law-enforcement actions were unlawful (as the Austrian Government has acknowledged they were, as already described), it could base its assessment on the lawfulness of the aim it was thereby sought to achieve, both where the measure was successful and where its implementation had merely begun and been of no avail.

B. Substance

1. The first question referred

56. The referring court wishes to know whether, under Article 15(1) (possibly read in combination with Article 5) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, ‘public authorities’ access to data stored on mobile telephones entails interference with fundamental rights enshrined in those articles of the Charter which is sufficiently serious to entail that access being limited, in areas of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime’.

57. Because Directive 2002/58 does not apply, if the reference for a preliminary ruling is admissible it would be necessary to reformulate the first question so that the Court’s answer provides an interpretation of Directive 2016/680.

58. That answer would need to clarify, first, whether it is possible to speak of interference in cases such as this and, next, if there is interference, whether Directive 2016/680 requires access to data to be limited to situations concerning the combating of serious crime.

59. Data processing operations are, by definition, capable of undermining the rights to respect for private life (Article 7 of the Charter) and to the protection of personal data (Article 8 of the Charter). In order to justify intruding upon the exercise of those fundamental rights, public authorities must therefore comply with the conditions laid down in Article 52(1) of the Charter.

60. The intrusion upon the rights protected by Articles 7 and 8 of the Charter will be all the greater where, through that intrusion: (a) access is sought to sensitive data ordinarily recorded on mobile phones, knowledge of which may reveal aspects of their owners’ lives that should be kept from being known by third parties; and (b) access is afforded to the content of communications.

¹⁸ Judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788).

61. In general terms and having regard to its terms, Directive 2016/680 cannot be interpreted as meaning that the data processing to which it refers is confined solely to situations concerning the combating of serious crime.

62. Directive 2016/680 covers any personal data processing operation¹⁹ by competent authorities for the prevention, investigation, detection or prosecution of *all kinds* of criminal offences.

63. Neither the principles that Directive 2016/680 lays down in respect of the processing of personal data for that purpose (Article 4) nor the requirements in order for the processing of data to be lawful (Article 8) suggest that, as a rule, there is scope for data processing only in situations involving serious crime.

64. Nor can any basis for a limitation that confines processing to situations concerning the combating of serious crime be found simply by extrapolating the Court's case-law on Directive 2002/58²⁰ to situations such as that in the present case.

65. That is so, in my view, because, without prejudice to what I shall set out below, that case-law relates to the systematic general and indiscriminate retention, by providers of electronic communications services, of personal data of an undefined generic group. The extent of the interference that such retention entails for society as a whole explains why the Court has been particularly rigorous in barring it and establishing the exceptions to that prohibition.

66. The same is not true where the access sought concerns not the entire population or large groups of it (that is to say, the personal data of an undefined generic group) but instead the information stored on an individual mobile telephone, in the course of a likewise individual criminal investigation which is governed, specifically, by Directive 2016/680.

67. The subject matter of Directive 2016/680 is precisely the processing of data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences – of all manner of criminal offences, not only serious offences.

68. Furthermore, as a number of the participants in the reference for a preliminary ruling have highlighted, since there is no indication of the severity of the criminal offences in Directive 2016/680, the directive might not be applied uniformly in the Member States, as there are appreciable differences in how national law assesses the degree of seriousness of an unlawful act.²¹

69. In short, Directive 2016/680 does not require that the personal data processing it regulates, in order to be lawful, may only be carried out for the purpose of combating serious crime.

70. Notwithstanding the foregoing, applying the principle of proportionality and on a case-by-case basis, the data processing that competent authorities intend to carry out under Directive 2016/680 must be tailored to: (a) the nature of the criminal offences being prosecuted; and (b) the type of personal data it is intended to process.

¹⁹ The category of the 'operations' included in Article 3(2) of Directive 2016/680 is very broad. See that article reproduced in point 9 of this Opinion.

²⁰ The judgment in *La Quadrature du Net* and judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970; 'the judgment in *Tele2 Sverige and Watson*'); of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788); of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790); and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152; 'the judgment in *Prokuratuur*').

²¹ The French Government gives the example of drug possession and trafficking offences, whose seriousness differs in Austrian and French criminal law. The Swedish Government expresses the same view.

71. In that respect I concur with some of the assertions of the German Government on limiting access to data on seized telephones, where they make it possible to establish a complete profile of the personality of the owners, in the light of the data stored on them. To the German Government, that access should be limited to the data necessary as evidence in a specific situation and may be inappropriate where, for example, ‘the offence being investigated is a minor offence or the data it is sought to obtain have little evidential value’.²²

72. In *theory*, therefore, Directive 2016/680 does not mean that access to the personal data stored on a mobile telephone is by default unlawful where its purpose is to facilitate the investigation of conduct that can be defined as ordinary or common crime. In *practice*, on the other hand, whether that access is appropriate will be a matter for the corresponding authority to assess on each occasion, having regard to whether it is necessary and to the criterion of proportionality to which I referred above.

73. In my view, the foregoing follows from the provisions of Directive 2016/680 that lay down the requirements for the processing of personal data to be valid in the context of combating crime.

- Article 4(1)(a), according to which the data must be ‘processed lawfully and fairly’.
- Article 8(1), which emphasises that the processing must be *necessary* and based on EU or Member State law.

2. *The second question referred*

74. By its second question, the referring court inquires whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, ‘precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation without the authorisation of a court or independent administrative body’.

75. The question is worded somewhat ambiguously.

- The referring court acknowledges that according to Paragraph 110(2) of the StPO, the seizure of property, in principle, requires the authorisation of the Public Prosecutor’s Office. The law-enforcement authority may only seize property without such authorisation in the extraordinary circumstances provided for in Paragraph 110(3) (which appear not to be present here).
- It further states, nevertheless, that the processing of the information stored on mobile telephones ‘is not regulated exclusively [in the StPO]’ and that the security authorities can gain that access on their own initiative, without prior authorisation.

²² Written observations of the German Government, paragraph 20.

76. The Austrian Government presents a version of the national legislation at variance with that set out in the order for reference. In particular, it states that, according to national law, both the seizure of a telephone (unless there is urgency) and the processing of the data stored on it are only possible with authorisation by the Public Prosecutor's Office.²³ Without an order from the Public Prosecutor's Office, exploitation of the data stored on such a telephone is unlawful.

77. It is for the referring court to examine the terms of the domestic legislation. In the context of the procedure under Article 267 TFEU, the Court does not have jurisdiction to interpret national law and it is for the referring court alone to determine the exact scope of national laws, regulations or administrative provisions.²⁴

78. Without wishing to mediate in the controversy concerning the interpretation of Austrian law, I find it difficult, solely from the provisions identified by the referring court (Paragraph 18 of the StPO read in combination with Paragraph 99(1) thereof), to draw the same conclusion as that court. However, once again, that is a matter that only the referring court can determine.

79. Be that as it may, the referring court is of the view that the judgment in *Prokuratuur* case-law²⁵ on the prior review of access to retained data by a judicial authority or an independent administrative authority can be transposed to a situation such as that in the present case.

80. In the view of the Netherlands Government, in contrast, that case-law must be understood in the context of national legislation which permitted *general* access of the competent authorities to *all* retained traffic and location data. That explains the requirement for judicial authorisation which may, however, not be warranted in relation to access to the data on a single mobile telephone.

81. In the same vein, the Norwegian Government argues that the many and varied safeguards that Directive 2016/680 establishes²⁶ do not explicitly include the need for prior authorisation by a judicial authority or an independent administrative authority.

82. The Commission, on the premiss that the provisions of Directive 2016/680 must be interpreted in the light of the Charter, argues that the obligation imposed on the Member States in Article 8(1) of that directive (requirements in order for the processing to be lawful) includes the need to uphold the fundamental rights guaranteed by Articles 7 and 8 of the Charter.

83. I concur with the Commission that, in accordance with those provisions of the Charter, the national legislatures must define the rules necessary to ensure that access to data is justified in each case and is limited to what is strictly necessary and proportionate.

²³ Paragraph 19 of the written observations of the Austrian Government. It cites the decision of 13 October 2020 of the Oberster Gerichtshof (Supreme Court, Austria) (Case 11 Os 56/20z), according to which the processing by the police of the data on a mobile telephone without the authorisation of the Public Prosecutor's Office is unlawful because it infringes the subjective rights of the person concerned.

²⁴ For example, judgment of 28 April 2022, *SeGEC and Others* (C-277/21, EU:C:2022:318, paragraph 21).

²⁵ Judgment in *Prokuratuur*, paragraph 51: 'it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.'

²⁶ In addition to Articles 4 and 8, those in Chapters III ('Rights of the data subject'), IV ('Controller and processor'), VI ('Independent supervisory authorities') and VIII ('Remedies, liability and penalties').

84. However, those national rules do not have to be rules specific to access to personal data contained, as here, on a mobile telephone, but may be the general rules laid down in domestic law for the obtaining of evidence.

85. In that respect, I have already reproduced paragraph 103 of the judgment in *La Quadrature du Net* as regards Member State measures that affect the confidentiality of electronic communications without imposing processing obligations on the providers of those telecommunication services.²⁷

86. It is therefore not necessary to infer from Directive 2016/680 any *specific* procedural rules to ensure that access to the data stored on a mobile telephone is lawful,²⁸ and the national rules governing the exercise of search and seizure powers in the course of criminal investigations will apply.²⁹

87. Referring to the provisions of domestic law in order to ensure that access is lawful in accordance with Directive 2016/680 is, moreover, consistent with the case-law of the ECtHR. In a situation relating precisely to the Republic of Austria concerning Article 8 ECHR (the right to respect for private and family life and for home and correspondence), the ECtHR found that the Austrian legislation on the seizure of objects and, in particular, of documents, applies to the search and seizure of data stored on electronic media.³⁰

88. If, as the Austrian Government maintains, citing the case-law of the Oberster Gerichtshof (Supreme Court, Austria), the law-enforcement authorities are not entitled to have access to the data kept on a particular mobile telephone without the authorisation of the Public Prosecutor's Office, the second question referred becomes to a large extent meaningless.

89. In any event, the answer to that question cannot ensure that access to the personal data on the seized telephone does not lead to 'reconstruct[ion of] a detailed and in-depth picture of almost all areas of [the] private life' of the data subject.³¹ On that basis, the law-enforcement authorities cannot dispense with the prior authorisation referred to in the judgment in *Prokuratuur*.

90. At first glance that assertion appears to be at odds with the fact that, as I have argued above, Directive 2002/58 (which the judgment in *Prokuratuur* interprets) does not apply to the present case. I nevertheless believe that the rationale on which that judgment is based supports the same thesis.

²⁷ Point 36 of this Opinion.

²⁸ The difficulty of that undertaking is well illustrated by the Commission's efforts in paragraphs 34 to 39 of its written observations to help define clear and precise rules for configuring the limits and appropriate safeguards in relation to accessing data on mobile telephones.

²⁹ Rules which, as the Danish and Irish Governments, for example, recall, fall outside the scope of EU law but may serve to satisfy a requirement resulting from that law.

³⁰ Judgment of the ECtHR of 16 October 2007, *Wieser and Bicos Beteiligungen v. Austria* (CE:ECHR:2007:1016JUD007433601), § 54: 'the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data'.

³¹ See the referring court's assertions in point 44 of this Opinion.

91. In the dispute that gave rise to the judgment in *Prokuratuur*, although the access was gained by obtaining data (metadata) from the electronic communications service providers, the matter concerned, as here, an individual criminal investigation against a particular person. The data being gathered were ‘data concerning several telephone numbers of ... and various IMEI codes of hers’.³²

92. To my mind, the judgment in *Prokuratuur* works on two levels: (a) the questioning of a Member State’s ordinary rules on the general and indiscriminate retention of and subsequent access to data in the possession of service providers; and (b) the prior review, in an individual case, of access to those metadata where they make it possible to construct a precise profile of a person’s private life.

93. The fact that, in the present case, the data that reveal the complainant’s private life were not in the possession of service providers and were obtained (or an attempt was made to obtain them) from a single seized telephone is in my view of secondary importance compared with the rationale underlying the prior review requirement advocated in the judgment in *Prokuratuur*.

94. That prior review is based ultimately on the protection guaranteed by Articles 7 and 8 of the Charter. The authority that carries out the review must be ‘able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access’.³³

3. *The third question referred*

95. By its third question, the referring court wishes to ascertain whether Article 47 (possibly read in combination with Articles 41 and 52) of the Charter precludes legislation such as the Austrian legislation,³⁴ which ‘allows data processing of a mobile telephone without advising the data subject before or, at the very least, after the measure is taken’.

96. In my view, the question thus worded may not be necessary in order to resolve the dispute, because the person concerned was able to exercise the right enshrined in Article 47 of the Charter by applying to the referring court to annul the law-enforcement action relating to the seized telephone, which included the subsequent (unsuccessful) exploitation of the data stored on it.

97. It is necessary to draw a distinction between those two stages of the law-enforcement action.

- As regards the seizure of the telephone itself, the information in the case file shows that the person concerned was aware of the seizure and that he refused to provide the law-enforcement authorities with the unlocking code at the time of the seizure.
- As regards the attempted data processing, all indications are that the data controller did not inform the person concerned of that operation, although the Austrian Government has stated

³² Judgment in *Prokuratuur*, paragraph 17.

³³ Judgment in *Prokuratuur*, paragraph 52.

³⁴ Once again, this relates to Paragraph 18, in conjunction with Paragraph 99, of the StPO.

that he was cognizant of a report which referred to the police activity in relation to the telephone.³⁵

98. A number of ambiguities remain, therefore, concerning the exploitation of the data and whether the person concerned was aware of it, which, as I have already observed, should have been clarified by the referring court in the order for reference and which prevent an answer of use to that court being given to the third question referred.

99. In any event, in case the Court finds it to be admissible, I shall express a view on that question. Should it be found to be admissible, and since Directive 2002/58 does not apply, the question would need to be reformulated in the light of Directive 2016/680, Articles 13, 15 and 54 of which provide the guidance necessary to give an answer.

100. According to Directive 2016/680, the information with which data subjects must be provided about the processing of their data is the information necessary, *inter alia*: (a) to lodge a complaint with a supervisory authority (Article 13(1)(d)); and (b) to obtain an effective remedy from the courts where rights guaranteed by Directive 2016/680 have been infringed, without prejudice to any available administrative or non-judicial remedy (Article 54).

101. It should nevertheless be borne in mind that both Article 13(3) and Article 15(1) of Directive 2016/680 authorise the Member States to adopt legislative measures which:

- delay, restrict or omit the provision of the information to the data subject pursuant to Article 13(2);
- restrict, wholly or partly, the data subject’s right of access to data processed, for as long as such restriction constitutes a necessary and proportionate measure in order, *inter alia*, to avoid obstructing official or legal investigations or procedures or prejudicing the investigation of criminal offences.³⁶

102. In any event, the lawfulness of the data processing does not depend on whether the competent authorities complied with their (subsequent) duties under Article 13 of Directive 2016/680, but on whether the purpose that justified the processing was lawful; that is to say, on whether those administrative authorities were entitled to process the personal data.

103. From that perspective, the fact that the person concerned has been informed of the attempts to access the data stored on the telephone seized from him is, in itself, unrelated to the lawfulness on substantive grounds of the law-enforcement action. Any conduct by the data controller in breach of its duties under Article 13 of Directive 2016/680 may have other consequences but does not, I would reiterate, in itself influence the lawfulness or otherwise of the processing of those data.

104. It is for the referring court to determine whether the national legislation enables the person concerned effectively to exercise those rights.

³⁵ Paragraph 37 of its written observations.

³⁶ To that effect, see the judgment in *Tele2 Sverige and Watson*, paragraph 121. The case-law established in that case on Directive 2002/58 can be transposed to Directive 2016/680 in the context of ensuring judicial protection of the rights of the owners of data undergoing processing.

V. Conclusion

105. In the light of the foregoing, I propose that the Court should dismiss as inadmissible the request for a preliminary ruling from the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria).

In the alternative, I suggest that the request should be answered as follows:

- (1) Article 4(1)(a) and Article 8(1) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, in conjunction with Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union,

must be interpreted as meaning that in the course of a criminal investigation, access by the public authorities to personal data stored on a mobile telephone, with a view to the processing of those data, is not limited to situations concerning the combating of serious crime.

Such access must be justified in each case and must be limited to what is strictly necessary and proportionate according to the nature of the criminal offences under investigation and of the personal data to which access is sought.

Law-enforcement authorities cannot, without prior authorisation by a court, grant themselves full and uncontrolled access to all the data stored on a mobile telephone in the course of a criminal investigation where those data make it possible to obtain a detailed picture of a person's private life.

- (2) Articles 13, 15 and 54 of Directive 2016/680, in conjunction with Articles 47 and 52 of the Charter,

must be interpreted as meaning that, without prejudice to the limitations authorised by Article 15(1) of Directive 2016/680 or to any other available administrative or non-judicial remedy, the owner of a mobile telephone must be informed of any processing of the personal data stored on that telephone carried out by the corresponding authorities, at the time and in the manner necessary to ensure the effective exercise of his or her right to seek a judicial remedy in the event of any infringement of the rights under Directive 2016/680.